Cyber Vulnerabilities of Energy Systems

Alexis Pengfei Zhao, Shuangqi Li, Chenghong Gu, Xiaohe Yan, Paul Jen-Hwa Hu, Zhaoyu Wang, *Senior Member, IEEE*, Da Xie, *Senior Member, IEEE*, Zhidong Cao, Xinlei Chen, *Member, IEEE*, Chenye Wu, *Senior Member, IEEE*, Tianyi Luo, Zikang Wang, and Ignacio Hernando-Gil

***Abstract*—In an era characterized by extensive use of and reliance on information and communications technology (ICT), cyber–physical power systems (CPPSs) have emerged as a critical integral of modern power infrastructures, providing vital energy sources to consumers, communities, and industries worldwide. The integration of ICT in these systems, while beneficial, introduces a rapidly evolving range of cybersecurity challenges that significantly threaten their confidentiality, integrity, and availability. To address this, our article offers a comprehensive and timely survey of the current landscape of cyber vulnerabilities in CPPS, reflecting the latest developments in the field up to the present. This includes an in-depth analysis of the diverse types of cyber threats to CPPS and their potential consequences, underscoring the necessity for a broad, multidisciplinary approach. Our review is distinguished by its thoroughness and timeliness, covering recent research to offer one of the most current overviews of cybersecurity in CPPSs. We adopt a holistic perspective, integrating technical, societal, environmental, and policy implications, thereby providing a more comprehensive understanding of cybersecurity in CPPSs. We delve into the complexities of cyberattacks, exploring sophisticated, targeted attacks alongside common threats, and emphasize the dynamic nature of cyber threats, providing insights into their evolution and future trends. Additionally, our review highlights critical yet often overlooked challenges, such as system visibility and standardization in security protocols, arguing their significance in enhancing CPPS resilience. Furthermore, our work gives special attention to the aspects of restoration and recovery postcyberattack, an area less emphasized in the existing literature. Through this comprehensive overview of the current state and evolving challenges of CPPS security, our article serves as an indispensable resource for research, practice, and policymaking dedicated to safeguarding the safety, reliability, and resilience of ICT-empowered energy systems.**

***Index Terms*—Cyberattack, cyber–physical systems, energy systems, literature review.**

I. Introduction

CYBER–PHYSICAL power systems, also referred to as CPPSs, are intricate networks that combine cyber and physical elements to orchestrate the generation, transmission, distribution, and consumption of power [1], [2], [3]. These systems leverage digital technology to optimize energy management, thus revolutionizing the traditional energy sector [4]. However, the integration of information and communication technologies (ICTs) in the energy sector has precipitated the emergence of novel security challenges [5], [6]. The proliferation of CPPS has resulted in a commensurate increase in the susceptibility of these systems to cyberattacks [7]. These intrusions can result in debilitating disruptions to energy delivery, with the potential to cause cascading failures across the infrastructure [8].

Real-world instances of cyberattacks targeting critical infrastructure in the energy sector, such as CPPS, are becoming increasingly prevalent and sophisticated. The Stuxnet attack on Iran's nuclear program in 2010 was a targeted intrusion that disrupted the country's critical energy infrastructure, destroying nearly 20% of its nuclear centrifuges and causing over $10 billion in economic losses [9], [10]. This sophisticated attack served as a wake-up call for organizations around the world to prioritize the protection of their control and energy systems against potential cyber threats, with the global cost estimated to reach $11.5 billion by 2022. The increasing interconnectedness of energy systems and the reliance on technology have made it crucial for organizations to adopt proactive security measures [11], [12], [13].

The Ukraine Blackout of December 2015 was the first documented case of a successful cyberattack leading to a power outage, affecting over 225 000 citizens for several hours [14].

Manuscript received 25 February 2023; revised 3 July 2023, 19 December 2023, 2 April 2024, and 19 June 2024; accepted 22 July 2024. Date of publication 30 July 2024; date of current version 14 October 2024. *(Corresponding author: Zhidong Cao.)*

Alexis Pengfei Zhao, Zhidong Cao, Tianyi Luo, and Zikang Wang are with the Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China (e-mail: P.zhao0308@gmail.com; Zhidong.Cao@ia.ac.cn; luotianyi2017@ia.ac.cn; wangzikang2016@ia.ac.cn).

Shuangqi Li is with the Department of Electrical Engineering, The Hong Kong Polytechnic University, Hong Kong (e-mail: shuangqi.li@connect.polyu.hk).

Chenghong Gu is with the Department of Electronic & Electrical Engineering, University of Bath, BA2 7AY Bath, U.K. (e-mail: C.Gu@bath.ac.uk).

Xiaohe Yan is with the State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources (North China Electric Power University), Beijing 102206, China (e-mail: x.yan@ncepu.edu.cn).

Paul Jen-Hwa Hu is with the David Eccles School of Business, University of Utah, Salt Lake City, UT 84112 USA (e-mail: paul.hu@eccles.utah.edu).

Zhaoyu Wang is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: wzy@iastate.edu).

Da Xie is with the Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: xieda@sjtu.edu.cn).

Xinlei Chen is with the Tsinghua Shenzhen International Graduate School, Shenzhen 518055, China (e-mail: chen.xinlei@sz.tsinghua.edu.cn).

Chenye Wu is with the School of Science and Engineering, the Chinese University of Hong Kong, Shenzhen, Shenzhen, Guangdong 518172, China, and also with the Shenzhen Institute of Artificial Intelligence and Robotics for Society, Shenzhen, Guangdong 518129, China (e-mail: chenyewu@yeah.net).

Ignacio Hernando-Gil is with the ESTIA Institute of Technology, University of Bordeaux, F-64210 Bidart, France, and also with the Institute for Systems and Computer Engineering, Technology and Science (INESC TEC), 4200-465 Porto, Portugal (e-mail: i.hernandogil@estia.fr).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JESTIE.2024.3434350.

Digital Object Identifier 10.1109/JESTIE.2024.3434350

The outage lasted for approximately 6 h before power was fully restored [15]. The incident resulted in severe financial losses, estimated at around 10 million dollars, highlighting the pressing need for stronger security measures in energy systems [16]. This event prompted increased investments in technology and security strategies by organizations and governments around the world, as they strive to secure their energy infrastructure and protect against potential future cyberattacks. The Triton attack targeted an oil and gas facility in the Middle East with sophisticated malware [17]. The malware could have caused catastrophic consequences if the attackers had intended to harm safety systems [18]. The incident highlights the threat to energy systems and the need for robust cybersecurity measures.

Rostami et al. [19] offer a comprehensive and insightful approach to assessing the reliability of CPPSs, integrating predicted cyber vulnerabilities. The uniqueness of this reference lies in its integration of predictive analytics with real-world cyber threat data, offering a realistic assessment of system vulnerabilities. Chen et al. [20] critically explore the vulnerabilities in machine-learning-based inertia forecasting in smart grids, specifically under cost-oriented data integrity attacks. Their analysis of potential risks associated with data manipulation and the subsequent destabilization of the grid is both in-depth and insightful. The reference is commendable for delving into the intersection of machine learning and cybersecurity, a crucial area in smart grid research. Zhang and Li [21] offer an in-depth cyber-vulnerability analysis for real-time power market operations, addressing a critical aspect of power system security. The combination of advanced cyber threat modeling with real-time market dynamics provides a comprehensive view of potential vulnerabilities. Zheng et al. [22] conduct a thorough examination of the vulnerabilities in deep reinforcement learning models for power system topology optimization. Their analysis highlights the susceptibility of these models to targeted cyberattacks, which could lead to compromised system configurations.

The detection of cyberattacks on CPPSs is a crucial aspect of ensuring the security, reliability, and resilience of modern energy systems [23]. Given the growing dependence on digital technologies and interconnected systems in the energy sector, it is increasingly important to have effective measures in place to detect and respond to cyberattacks [13], [24]. The significance of cyberattack detection in CPPS lies in the far-reaching and potentially catastrophic effects that such intrusions can have. Cyberattacks on CPPS can disrupt energy delivery, compromise energy management systems, and lead to system failures and widespread blackouts [25]. Additionally, cyberattacks on CPPS can have a significant impact on public safety, national security, and economic stability. To detect cyberattacks on CPPS, various techniques and tools are employed. These techniques range from network-based detection methods, such as static and dynamic state estimation [26]. Additionally, advanced techniques, such as machine-learning and artificial intelligence algorithms, are being developed to detect anomalies and suspicious activities in CPPS [27]. The implementation of these techniques is crucial to detecting cyberattacks in real time and mitigating their impacts on the CPPSs [28].

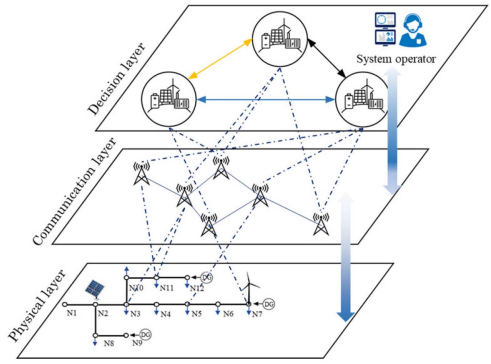

Fig. 1. Typical CPPS containing decision, communication, and physical layers.

Upon the detection of a cyberattack on a CPPS, it is imperative to implement remedial measures and effectuate emergency response protocols with alacrity to mitigate the damage inflicted [29], [30]. Such protocols typically entail a synergistic blend of techniques, such as the adjustment of energy generation and distribution plan, backup resources, load shedding, and demand-side management. Beyond these prompt response efforts, organizations can fortify their overall security posture, thereby reducing their susceptibility to future attacks [31]. This may encompass the deployment of technical safeguards, such as firewalls, access control systems, encryption, and other security measures, as well as the formulation of comprehensive incident response plans and the frequent testing and rehearsal of such plans to ensure preparedness [32]. By undertaking these proactive measures, organizations can enhance their capability to competently respond to cyber threats and minimize the ramifications of attacks on their CPPS [33].

The present article offers a comprehensive review of the various methods used for detecting, planning, and mitigating cyberattacks that target CPPSs while also addressing the challenges associated with these methods. Given the increasing dependence on CPPSs for managing critical infrastructures, it has become crucial to develop effective strategies for safeguarding these systems against malicious cyberattacks. The study presents an overarching framework for conducting cyberattack research on CPPSs. A typical CPPS is depicted in Fig. 1. We begin by introducing the types and impacts of cyberattacks on CPPSs, such as disruptions to operations, compromised system integrity, and potential harm to human safety.

We then employ attack detection techniques to diagnose and identify cyberattacks. Once detected, we propose a range of planning and mitigation mechanisms to ensure the safe and uninterrupted operation of CPPSs. Furthermore, we explore the challenges associated with implementing these defense mechanisms, such as the high cost of deployment and the need for regular updates and maintenance. In summary, the present study offers a comprehensive overview of the detection, planning, and mitigation methods for CPPSs while also highlighting the challenges associated with these methods. By providing a deep understanding of the characteristics of cyberattacks and the vulnerabilities of CPPSs, our study aims to contribute to the

TABLE I
COMPARATIVE ANALYSIS OF CYBER VULNERABILITIES IN POWER SYSTEMS WITH EXISTING LITERATURE

Reference	[33]	[34]	[35]	[36]	The proposed review
Main focus	Modeling, simulation, and cybersecurity applications in CPPS, with research status and recommendations.	Vulnerability analysis of CPPS using a game-theoretic approach, focusing on cascading failures and optimal responses.	Resilience measures and optimization methods in CPPS, emphasizing recovery and critical node protection.	Summarizes research on attack modeling, security evaluation, detection, and defense in CPPS.	Provides a comprehensive and timely survey on cyber vulnerabilities in CPPS, including types of cyber threats, consequences, and a broad, multidisciplinary approach to resilience.
Methodology	Review of modeling and simulation methods, cybersecurity measures in CPPS.	Game-theoretic modeling for vulnerability analysis and optimal load curtailment.	Review of quantitative resilience measures and optimization methods, including component recovery sequencing.	Review of attack modeling, security evaluation methods, and existing defense mechanisms in CPPS.	Employs a thorough literature review and in-depth analysis, focusing on system visibility, standardization in security protocols, and emphasizing a dynamic approach to cyber threats.
Key contributions	Analysis of the status quo in CPPS modeling and simulation with a focus on cybersecurity applications.	Novel approach to analyzing CPPS vulnerabilities using game theory; emphasis on system resilience under attacks.	Comprehensive overview of system resilience measures and optimization methods, with practical implications for CPPS.	Comprehensive analysis of cyber-attack and defense research, proposing solutions to existing challenges.	Emphasizes a holistic perspective that integrates technical, societal, environmental, and policy implications, filling a critical gap left by previous reviews and underscoring the significance of system restoration and recovery post-cyberattack.
Research gaps	Suggests a need for updated and comprehensive research in CPPS modeling and cybersecurity measures.	Identifies the necessity for more dynamic and adaptable vulnerability analysis methods in CPPS.	Points out the lack of comprehensive solutions for enhancing CPPS resilience at a system level.	Calls for innovative defense mechanisms and more effective detection methods to combat evolving cyber threats in CPPS.	Highlights the necessity for a multidisciplinary approach to address cyber vulnerabilities in CPPS, moving beyond the technical focus of prior studies to include broader societal and policy considerations.

development of effective defense strategies for protecting these critical systems against cyber threats.

The major contributors can be summarized as follows.

Comprehensive Overview of CPPS Cybersecurity: Our survey presents an extensive and up-to-date exploration of cybersecurity in CPPS. We offer a detailed analysis that not only encompasses the most current research but also anticipates future trends and challenges in cyber threats. This ensures our review remains relevant and useful for both current and future developments in the field.

Integrated Analysis of Cybersecurity Challenges: We provide a holistic view of the cybersecurity landscape in CPPS, blending technical insights with considerations of societal, environmental, and policy implications. Our work delves into the complexities of various types of cyberattacks, highlighting the nuanced challenges faced in securing CPPS against both common and sophisticated threats.

Emphasis on System Resilience and Recovery Strategies: Our survey underscores the importance of resilience in CPPS cybersecurity, focusing on robust recovery strategies and the critical need for standardized security protocols. We bring to light the importance of system restoration and the broader aspects of cybersecurity that extend beyond prevention and immediate mitigation. A detailed comparison in Table I is shown to juxtapose our findings and methodologies with the existing papers [34], [35], [36], [37] on similar topics, illustrating the comprehensive nature and multidisciplinary approach of our research on cyber vulnerabilities of power systems.

The sections of this article have been meticulously structured to offer a broad review of the latest research on cyberattacks, including detection and defensive strategies within ICT-enriched CPPSs (see Table II). The rest of this article

TABLE II
STRUCTURE OF THIS ARTICLE

Section	Subsection	Description
Introduction	1. CPPS Introduction	Brief introduction to CPPSs.
	2. Importance and Vulnerabilities	Discussion on the importance of CPPS and vulnerabilities due to ICT integration.
	3. Objectives and Structure	Outline of the article's objectives and structural overview.
Background and Related Work	1. Transition to ICT-enriched CPPSs	Exploration of the transition from traditional energy systems to ICT-enriched CPPSs.
	2. Motivations and Challenges	Examination of the motivations behind and challenges of integrating ICT into energy systems.
Cyber Vulnerabilities in CPPS	1. Types of Cyberattacks	Detailed description of various cyberattack types targeting CPPS.
	2. Cyberattack Detection	Overview of model-based and learning-based cyberattack detection methods.
	3. Cyberattack Mitigation	Discussion on strategies for cyberattack mitigation, including preventive, adaptive, and restoration.
Challenges in Securing CPPS	1. Interdependencies	Analysis of the interdependencies among system components.
	2. Lack of Standards	Investigation into the lack of standardized security protocols.
	3. Evolution of Cyberattacks	Examination of how cyberattacks on CPPS are evolving.
	4. Privacy Concerns	Discussion on privacy concerns within CPPS.
Proposed Solutions	1. Comprehensive Interdependency Solution	Proposed solutions for addressing system component interdependencies.
	2. Standardization Establishment	Strategies for the establishment of security standardization.
	3. Measures Against Cyberattack Evolution	Proactive measures to counter the evolution of cyberattacks.
	4. Privacy Concern Mitigation	Approaches to mitigating privacy concerns in CPPS.
Conclusion		Summary of key findings, the importance of adaptive strategies, and a call for further research.

is organized as follows. Section II discusses advancements in CPPSs, detailing their architecture, components, and functionalities. Section III analyzes a range of cyber threats to CPPSs, from common attacks, such as malware, to sophisticated threats, such as advanced persistent threat (APTs). Section IV reviews advanced techniques for detecting cyberattacks on CPPSs, including various methodologies and principles. Section V focuses on emergency responses, covering incident management, containment tactics, and recovery strategies. Section VI outlines research challenges and areas needing further study for enhancing CPPSs' resilience. Section VII presents solutions for cybersecurity issues, emphasizing AI, security standardization, and stakeholder collaboration. Finally, Section VIII concludes this article.

II. Transitioning From Traditional Energy Systems to ICT-Enriched CPPSs

The transition from traditional energy systems to modern CPPS has been a gradual and ongoing process that has taken place over several decades [38]. The integration of ICTs into the energy sector has been a driving force behind this transformation [39] and has helped to improve the efficiency, reliability, and sustainability of energy systems [40], [41]. Smart grids use advanced sensors, control systems, and communication networks to monitor and control the flow of electricity in real time [42]. This has allowed for the integration of renewable energy sources into the grid and has improved the efficiency of energy transmission and distribution [43]. Over time, more sophisticated systems, such as distributed energy resources, energy storage systems, and microgrids, have been added to the energy mix.

The pros of modern CPPS include improved energy efficiency and reliability, increased integration of renewable energy sources [44], and the ability to provide energy to communities during power outages [45]. However, there are also some cons to consider. The vulnerability of modern ICT-enriched CPPS to cyberattacks is a growing concern, as these systems rely on complex networks and advanced control systems that can be targeted by malicious actors [46]. Cyberattacks on energy systems can cause significant disruptions to the energy supply, including power outages and failures in energy transmission and distribution [47]. The motivations behind this integration have been numerous, including the need to improve efficiency, reliability, and sustainability [48]. While the pros of modern CPPS are significant, there are also some cons to consider, including the cost of implementation and the growing vulnerability to cyberattacks [49]. To mitigate these risks, it is important to invest in robust cybersecurity measures to protect modern CPPS from cyberattacks and to ensure the continued operation of these critical systems.

III. Types of Cyberattacks

This section provides an in-depth look into various types of cyberattacks that pose threats to CPPSs, including false data injection attacks (FDIAs), load redistribution attacks, denial of service (DoS) attacks, phishing attacks, and man-in-the-middle (MitM) attacks. Fig. 2 shows the integrated framework of cyberattack dynamics, detection, and mitigation in CPPS. FDIAs can disrupt or destroy infrastructure by manipulating data sent to control systems, potentially leading to significant infrastructure damage and public safety risks. Load redistribution attacks manipulate sensor data regarding energy load distribution, leading to potential overloading or imbalances in the power grid. DoS attacks prevent legitimate system access, potentially causing considerable disruption and damage, while phishing and MitM attacks aim to steal sensitive information or intercept and alter communication between system components, posing considerable risks to system security.

A. False Data Injection Attacks

FDIAs, as shown in Fig. 3, are a type of cyberattack on CPPSs that involve the injection of inaccurate or malicious data into the control systems of the grid [50]. Such attacks are motivated by a range of factors, including espionage, financial gain, and disruption or destruction of infrastructure [51]. FDIAs on CPPSs can be launched by attackers gaining access to the control system network, often through exploiting vulnerabilities in software or hardware components. Once access is gained, attackers can manipulate the data being sent to the control systems, such as changing sensor readings or altering the setpoints of control devices [52]. This can cause the system to operate in unintended ways, potentially leading to cascading failures, blackouts, or physical damage to equipment [53]. In some cases, attackers may also use social engineering tactics to trick operators into unknowingly facilitating the attack, such as by providing login credentials or other sensitive information.

The consequences of successful attacks can be severe. In some cases, attackers may seek to cause physical damage to critical infrastructure by manipulating data to cause equipment to operate outside of safe parameters or by interfering with safety systems [54]. In other cases, attackers may seek to disrupt the grid by manipulating data in a way that causes outages or other disruptions. This can lead to power losses, economic impacts, and potential risks to public safety [55]. In 2015, the Ukrainian power grid suffered a widespread blackout caused by a sophisticated cyberattack that utilized false data injection techniques [56]. The attackers were able to remotely manipulate control systems and cause a blackout that left over 225 000 people without power for several hours [57]. In 2020, the U.S. Cybersecurity and Infrastructure Security Agency issued an alert warning of a cyberattack campaign targeting U.S. electric utilities that utilized false data injection techniques [58].

B. Load Redistribution Attacks

Load redistribution attacks are a type of FDIA that can be targeted at CPPSs to manipulate the sensor data regarding the energy load distribution across the network [59], [60]. This type of attack can potentially result in overloading or imbalances in the power grid, which can cause severe disruptions or power outages [61]. Load redistribution attacks involve an attacker injecting false data into the system's sensors, which can force the system to redistribute energy in an unsafe or suboptimal manner

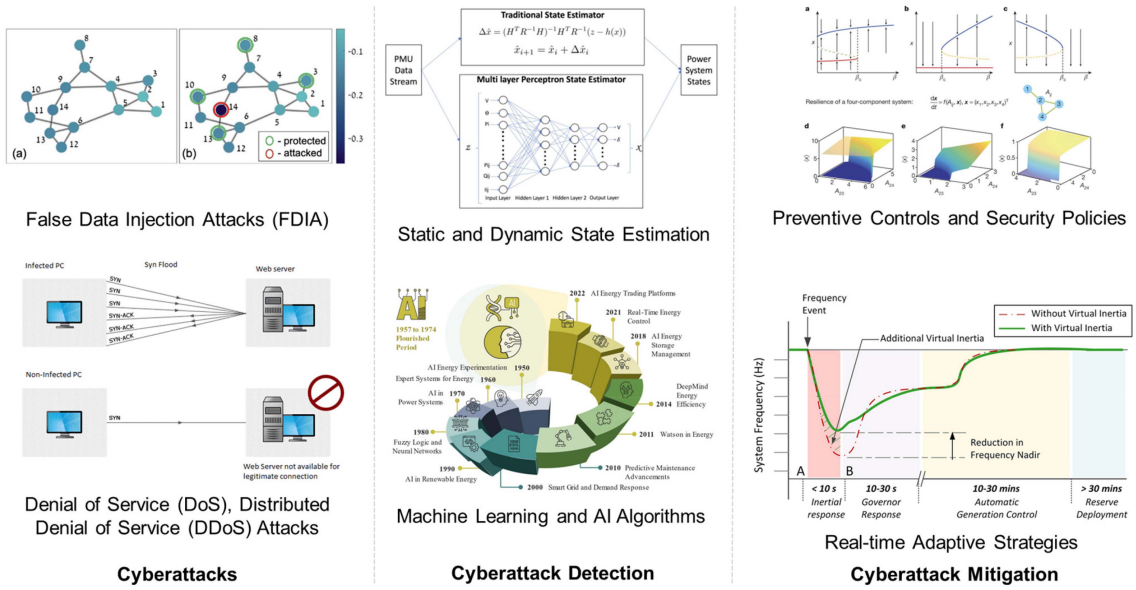

Fig. 2. Integrated framework of cyberattack dynamics, detection, and mitigation in CPPS.

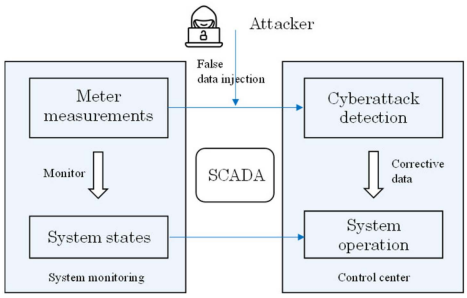

Fig. 3. Schematic of the FDIA intrusion.

[62]. For example, an attacker could overload specific parts of the power grid, causing a power outage in some areas, while other areas experience an overvoltage condition. Alternatively, an attacker could redirect power to specific areas, leading to equipment failure or other safety risks [63]. To prevent such attacks, robust security measures must be implemented in CPPSs [64].

C. DoS Attacks

DoS attacks are designed to prevent legitimate users from accessing the targeted system [65], by flooding it with a large amount of traffic or overwhelming it with requests [66]. In the case of CPPSs, a DoS attack can cause significant disruptions and damage to the power grid, leading to power outages and other disruptions [67]. DoS attacks on CPPSs can take various forms, one form is the flooding attack, which involves overwhelming the system with a large number of requests or messages, thereby causing it to become unresponsive or even crash [68]. Another form is the distributed DoS attack, which involves using a network of compromised devices (known as a botnet) to flood the system with requests from multiple sources, making it even more difficult to defend against [69]. DoS attacks on CPPSs can have severe consequences. Disruption of service is a significant risk, as DoS attacks can prevent legitimate users from accessing the system, causing inconvenience or harm to end-users [70]. Economic losses may also occur, with lost revenue, reduced productivity, and other financial consequences [71]. Several real-life examples highlight the potential impact of DoS attacks on CPPSs. In 2017, Dragonfly 2.0, a group of hackers, launched a series of DoS attacks on energy companies in the United States and Europe [72]. The attacks were aimed at gaining unauthorized access to critical systems and sensitive information. Another example is the Triton attack, which targeted a petrochemical plant in Saudi Arabia in the same year [73]. This sophisticated DoS attack aimed to disable the plant's safety systems and cause a major industrial accident.

D. Phishing Attacks

Phishing attacks are a type of social engineering attack that aims to steal sensitive information, such as login credentials or financial data, by tricking victims into clicking on a link or opening an attachment that appears to be legitimate but is actually a fake website or document [74]. Phishing attacks can also be used to deliver malware or other forms of malicious code that can compromise a system's security. In the context of CPPSs, phishing attacks can be particularly dangerous, as they can give attackers access to critical infrastructure and control systems, which could lead to physical harm or widespread power outages [75]. For example, a phishing email sent to an operator of a power plant could contain a link to a fake login page, which could capture the operator's login credentials and give the attacker remote access to the plant's control systems [76]. As such, it is essential for operators of CPPSs to be aware of the risks posed by phishing attacks and to implement appropriate security measures, such as employee training and multifactor authentication, to mitigate these risks.

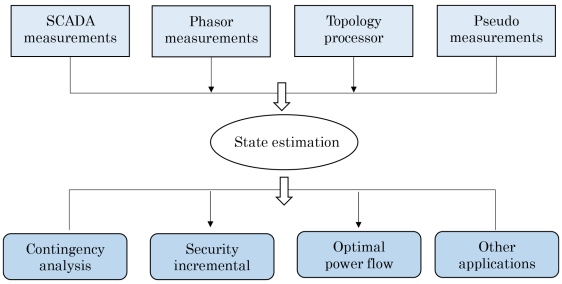

Fig. 4. Typical framework of the state estimation.

E. MitM Attacks

An MitM attack is a type of cyberattack that poses a significant threat to CPPSs [77]. The attacker can then manipulate the data being exchanged to carry out various nefarious activities. The primary goal of an MitM attack on a CPPS is to gain unauthorized access to the system's critical components. By intercepting the communication between devices or systems, an attacker can eavesdrop on sensitive information, modify the data being exchanged, or even impersonate a legitimate user or device [78]. To carry out an MitM attack, an attacker typically uses various techniques, such as session hijacking. These techniques allow the attacker to intercept, modify, or redirect the communication between devices or systems. The attacker can then manipulate the data to carry out various malicious activities [79]. To protect against MitM attacks, CPPSs must implement various security measures, such as encryption, authentication, and access control mechanisms [80]. These measures can help to prevent unauthorized access to the system's critical components and ensure that only legitimate devices and users can access the system.

IV. Cyberattack Detection

To detect cyberattacks, researchers have developed various cyberattack detection mechanisms that can be broadly classified into two general approaches: model-based and learning-based approaches [81].

Model-based approaches rely on the mathematical models of CPPSs to detect anomalies and potential cyberattacks [82]. These models can simulate the behavior of the CPPS under different scenarios and can detect deviations from expected behavior that may indicate a cyberattack [83]. Examples of model-based approaches include state estimation, Kalman filtering, and dynamic system modeling [84]. In Fig. 4, a state estimation used in CPPS operation and control is given [85]. Model-based approaches are particularly useful for detecting known cyberattacks or attacks that exploit specific vulnerabilities in the CPPS. Learning-based approaches use machine-learning algorithms to analyze and learn patterns of normal behavior from historical data collected from CPPSs [86], [87]. The algorithms can detect deviations from normal behavior that may indicate the presence of a cyberattack [88]. Examples of learning-based approaches include neural networks, decision trees, and support vector machines (SVMs) [89], [90]. Learning-based approaches are particularly useful for detecting previously unknown cyberattacks or novel attack strategies.

A. Model-Based Detection

One approach to identify malevolent cyberattacks in CPPSs is through model-based detection methodologies, which hinge on mathematical models of the system and measurements to estimate the system's internal states. The objective of model-based detection is to identify any deviations in the system's behavior that may indicate the presence of a cyber assault. One commonly employed model-based detection approach is state estimation, which involves inferring the values of system states (e.g., voltage and current) based on measurements obtained from sensors dispersed throughout the system. State estimation can be classified as either static or dynamic.

Static state estimation methodologies use a snapshot of measurements at a specific time to estimate the system's states. These methods are typically more efficient and straightforward than dynamic methods, but may not capture the full dynamism of the system. Dynamic state estimation, on the other hand, takes into consideration the time-varying nature of the system and employs a set of equations that describe the system's behavior over time. This approach can provide more precise and intricate information about the system's states, which is particularly crucial for detecting cyberattacks that may appear as subtle modifications in the system over time. Attack detection methods can be based on both static and dynamic state estimation. For instance, a static detection method may compare the estimated states with predetermined threshold values to detect anomalies that could indicate a cyber assault. In contrast, a dynamic detection method may employ machine-learning algorithms or other advanced techniques to analyze the system's behavior over time and identify deviations from expected patterns. Overall, model-based cyberattack detection is a crucial component of cybersecurity for CPPSs, and state estimation is a pivotal approach in this field. By detecting cyberattacks in real time, CPPS operators can take appropriate actions to mitigate the impact of the attack and ensure the stability and reliability of the system.

To discern between cyberattacks and sudden changes in power-grid state, a time-varying dynamic model is suggested in [91]. The study develops a dynamic state estimation algorithm to estimate and track nonstationary and time-varying power-grid states. By examining the statistical properties of the dynamic state estimations, the quickest detection algorithm is developed to minimize the worst-case detection delays and accurately differentiate between FDIA and sudden system changes. Alhelou and Cuffe [92] introduce a control technique based on the dynamic state estimation that can mitigate the impact of cyberattacks in modern CPPSs. This technique involves two distinct schemes: a dynamic observer that can dynamically detect cyberattacks and another that isolates the location of the attack. These schemes are based on observer designs that can eliminate the effects of unknown inputs. Additionally, the study proposes a fault-tolerant control technique that leverages the observer-based detection and isolation schemes. Leng et al. [93] focus on addressing the problem of instability resulting from

stealth cyberattacks that can bypass established observability tests. A detailed model of a stable dc microgrid is developed, and the stability of the system is evaluated using a describing function-based method in the presence of a nonlinear element that represents the stealth cyberattack. Milano and Gómez-Expósito [94] use Benford's law to detect cyberattacks in CPPS state estimators. One of the notable characteristics of this law is its discerning sensitivity to data manipulations and is frequently employed in the detection of fraudulent activity.

B. Learning-Based Detection

Learning-based cyberattack detection approach is fundamentally distinct from the state estimation-based detection paradigm [95], [96]. Unlike the former, the latter does not hinge on a mathematical model of the physical system [97] but relies solely on historical system data. Leveraging the multidisciplinary fields of statistics, artificial intelligence, and computer science, machine learning is capable of extracting knowledge from data [98]. In this context, machine-learning methods are harnessed for both classification and regression, the former of which serves as the bedrock for cyberattack detection [99]. Historical data are employed to train a machine-learning-based classifier, which can identify anomalous data patterns and, subsequently, detect potential cyberattacks in CPPSs.

Learning-based attack detection methods can generally be classified into three categories: supervised, unsupervised, and semisupervised methods [100]. The classification methodology consists of segregating predicted values into specific categories, with cyberattack detection serving as a quintessential classification task [101]. In essence, the principal objective of regression analysis is numerical prediction, with widespread adoption in CPPS load forecasting [102]. Ultimately, the learning-based cyberattack detection methodology serves as an invaluable and complementary approach to traditional model-based detection. The utilization of machine-learning algorithms permits CPPS operators to detect cyberattacks with greater precision and efficiency, empowering them to undertake proactive mitigation measures that safeguard the stability and reliability of CPPSs [103], [104].

A two-stage detection system for safeguarding against cyber intrusions in CPPSs is proposed in [105]. In the first stage of intrusion detection, an SVM is utilized as a detection algorithm to uncover anomalous behavior within a smart meter. In the second stage, the temporal failure propagation graph technique is employed to generate attack pathways for pinpointing attack events. Ultimately, a cutting-edge pattern recognition algorithm is employed to compute the resemblance between a detected anomalous event and pre-established cyberattacks. Khaw et al. [86] detail a deep-learning-based system designed to detect cyberattacks in transmission line protective relays. The proposed system is trained using current and voltage measurements to capture a range of fault types that may occur on transmission lines. The trained model is then utilized to identify any maliciously injected current or voltage measurements that may be used by attackers to manipulate the transmission line protective relays.

V. Cyberattack Mitigation

Cyberattack mitigation within CPPS entails a multifaceted strategy to reduce the likelihood of a successful attack while simultaneously minimizing any impact resulting from an attack [106]. This strategy encompasses the continuous monitoring and analysis of system activity, ongoing risk assessments, and the implementation of a variety of security controls capable of safeguarding against known and emergent threats [107]. Threat modeling represents a crucial aspect of cyberattack mitigation within CPPS, as it serves to identify and assess the potential risks associated with each threat [108]. If a cyberattack does occur, CPPS must have a well-defined and rehearsed defense and mitigation plan in place to mitigate the impact of the attack. This plan may include isolating infected or compromised systems, shutting down vulnerable services, and implementing patches or updates to address the attack [37]. Furthermore, response teams may be activated to investigate the attack, identify the root cause, and develop strategies for restoring the system to normal operation. Restoration and recovery represent the critical components of cyberattack defense and mitigation within CPPS. In the event of an attack, it is essential to have a well-defined plan for restoring the system to full operation as quickly as possible [109]. This plan may include repairing or replacing compromised hardware, restoring backups, and implementing additional security controls to prevent similar attacks from occurring in the future.

A. Preventive Mitigation

Planning and investment strategies to safeguard critical CPPSs against cyberattacks involve a combination of proactive measures to reduce the risk of attacks and reactive measures to minimize the impact of any attacks that occur [110]. One key proactive measure is the regular conduct of comprehensive risk assessments to identify system vulnerabilities and potential threats. This process may involve penetration testing to assess the security architecture of the system, as well as evaluations of the third-party hardware and software components to ensure that they meet established security standards. Investments in security controls and technologies are also critical to mitigating cyberattacks in CPPSs. This may include the implementation of firewalls, intrusion detection systems, security information and event management tools, and encryption technologies [111].

Cyber insurance can prove to be an indispensable tool in safeguarding critical CPPSs against the debilitating financial consequences of cyber incidents [112]. By procuring cyber insurance, CPPSs can benefit from a comprehensive risk management strategy that provides financial protection in the aftermath of a cyberattack [113]. The insurance can defray the exorbitant costs of data recovery, legal fees, and other expenses, which could prove particularly consequential to the financial viability of CPPSs. This can be particularly crucial as CPPSs, given their complex and interdependent architecture, are particularly vulnerable to catastrophic financial losses due to a cyberattack [114]. Moreover, the availability of cyber insurance can help mitigate the potential risks of cyberattacks by encouraging organizations to invest in proactive cybersecurity measures and

best practices. By offering insurance coverage, cyber insurance serves as an impetus for organizations to improve their overall security posture, fortify their defensive infrastructure, and enhance their cyber resilience. This, in turn, can reduce the likelihood of a successful cyberattack and improve the overall cybersecurity landscape of CPPSs. The multifaceted approach toward cybersecurity, coupled with the implementation of insurance coverage, can also lower the overall risk profile of CPPSs, thus enabling them to counter and effectively manage the challenges of the ever-evolving cyber threat landscape [115].

Ahmed et al. [116] introduce a pioneering approach in employing spatiotemporal deep graph networks for event detection in cyber–physical electric distribution systems. Their innovative use of deep learning to navigate the complexities of electric distribution networks marks a significant leap in predictive analytics. The reference is particularly commendable for its ability to classify a wide array of event types and effectively localize these events within the network. This work sets a new benchmark in the field by combining theoretical robustness with practical applicability, potentially transforming how electric distribution systems are monitored and secured.

Presekal et al. [117] present a novel hybrid deep-learning approach to developing an attack graph model for CPPSs. This reference stands out for its dynamic mapping of potential cyberattack pathways using graph theory and machine learning. The application of hybrid learning to capture both structured and unstructured data within power systems is a highlight of this work. The authors' simulated attack scenarios demonstrate the model's effectiveness in real-time threat detection and mitigation.

B. Adaptive Mitigation

Mitigating the impact of natural or malicious disasters on CPPS requires a multifaceted approach that prioritizes the safety and reliability of the system, minimizes damage, and restores functionality. One such strategy is resource allocation, which involves the prioritization of critical resources, such as power, communications, and emergency services [28], as well as the deployment of backup systems to ensure continued operation. Real-time data and predictive analytics can be leveraged to optimize resource allocation and anticipate potential impacts. Another important strategy involves the implementation of redundant systems and backup solutions to minimize the risk of data loss or system downtime. Redundancy can include the use of redundant power sources, communications systems, and other critical components, as well as backup storage and data replication. These measures ensure that critical systems and data are duplicated across multiple locations [118]. In summary, a comprehensive approach to mitigating the impacts of natural or malicious disasters on CPPS includes the prioritization of critical resources through resource allocation, the implementation of redundancy measures, comprehensive disaster response planning, and the use of advanced technologies, such as sensors, drones, and machine-learning algorithms. These strategies can help ensure continued operation, minimize the impact of disasters, and protect critical infrastructure [119]. Khazaei and Asrari [120] advance the state-of-the-art by shifting the focus from dc state estimation in transmission systems to ac state estimation in distribution grids, specifically targeting cyberattacks that cause overvoltages. The proposed nonlinear model is transformed into a convex optimization model via second-order cone programming relaxation, ensuring the existence of a global optimum. Zhang et al. [121] present a defense strategy that coordinates the cyber and physical layers to minimize cyber risk and overcome disruption. At the cyber layer, a multilevel Markovian Stackelberg game models the sequential actions of the attacker and defender, with the defender deploying resources in real time to protect lines based on the attacker's actions. If cyberattacks result in physical outages, the defense shifts to the physical layer. A security-constrained optimal power flow is employed to reserve a security margin of critical components, minimizing the blackout scale and potential future risk.

C. Restoration

In the aftermath of a cyberattack on CPPSs, system restoration is a critical process that involves the recovery and repair of affected systems and infrastructure [122]. The nature and scope of the damage caused by a cyberattack can be extensive and may require significant time, effort, and resources to fully restore the system to its preattack state. The system restoration process typically involves a number of interdependent steps, including damage assessment, system diagnosis, repair, and testing [123]. Damage assessment is a crucial first step in understanding the full extent of the damage caused by the cyberattack. This can involve evaluating the operational status of the CPPSs and identifying the specific systems and infrastructure that have been affected. System diagnosis, the next step in the restoration process, involves identifying the root causes of the damage and developing a comprehensive plan for repairing and restoring the affected systems. This may involve the replacement of hardware and software components, the reconfiguration of network settings, and the implementation of security updates to prevent similar attacks in the future. Once the necessary repairs have been completed, the restored systems and infrastructure must undergo rigorous testing to ensure that they are fully operational and that any vulnerabilities have been addressed. This testing can include functional testing, performance testing, and security testing to ensure that the CPPSs are fully restored and able to operate effectively and securely.

D. Contextual Application Summary

Expanding on the multifaceted strategy of cyberattack mitigation within CPPSs, it is evident that this approach encompasses several layers, aiming not only to reduce the likelihood of successful attacks but also to minimize their impact. The continuous monitoring and analysis of system activity, coupled with ongoing risk assessments, form the cornerstone of this strategy. This proactive stance is further strengthened by the implementation of various security controls, tailored to guard against both known and emergent threats.

Threat modeling, as a key component of this strategy, plays a critical role in identifying and assessing potential risks. In the event of an attack, having a well-defined and rehearsed

defense plan is crucial. This plan might include isolation of compromised systems, shutdown of vulnerable services, and rapid deployment of patches or updates. The activation of response teams to investigate and rectify the attack is equally important, ensuring that the system returns to normal operation as swiftly as possible. The restoration and recovery aspect of this strategy is critical. It involves a detailed plan for bringing the system back to full functionality postattack, including repair or replacement of compromised components, restoring backups, and bolstering security controls to thwart future attacks. Preventive mitigation measures, including comprehensive risk assessments and penetration testing, play a vital role in this strategy. They help identify system vulnerabilities and prepare the infrastructure to withstand potential cyber threats. Investments in security technologies, such as firewalls, intrusion detection systems, and encryption, are integral to fortifying CPPSs against attacks. Cyber insurance emerges as a key element in this landscape. It not only offers financial protection in the aftermath of an attack but also incentivizes organizations to invest in robust cybersecurity measures. By alleviating the financial strain of cyber incidents, insurance enables CPPS operators to focus on enhancing their security posture and resilience.

VI. Challenges

As energy systems shift to CPPSs empowered by ICTs, cybersecurity has drawn growing research attention. As described previously, this article provides a comprehensive review of three streams of research on cybersecurity for CPPSs (i.e., attack type, attack detection, and attack mitigation). Despite the efforts, several key challenges remain, which we succinctly outline in the following.

A. Interdependencies Among Distinct System Components

An important challenge for securing CPPSs is the close interdependency among distinct system components. Typically, an ICT-empowered CPPS includes a physical component (e.g., a power generator) that is tightly linked to its cyber components (e.g., monitoring sensors and control systems). Disruptions to the control system, as a result of cyberattacks, lead to incorrect operations or even power generator shutdown, which then can create a cascading effect in the entire system, thereby disrupting power supply to critical infrastructures. In addition, a multienergy CPPS has additional complexity. For example, a hybrid system incorporates solar, wind, and hydro energy sources. A fault in or cyberattack on the wind turbine's control system can cause power imbalance in the entire system, affect the overall energy output, or even create systemic failures. Deployments of multiple energy storage and conversion technologies not only amplify the intricacy of a CPPS but also elevate the linkages of different system components. To illustrate, in a system that includes battery storage and grid-tied inverters, a failure or malicious tampering of the inverter can influence the power fed into the grid and damage charge/discharge cycles in the battery storage, which, in turn, affects its useful lifespan and reliability.

B. Lack of Standards

Another key challenge is the lack of standards for security protocols and frameworks. Different standards and frameworks have been developed, with some adopted to a certain extent. Take ISO/IEC 27019 as an example, it is based on ISO/IEC 27002 and provides guidelines for information security management in the energy utility industry. Another example is the cybersecurity framework by the National Institute of Standards and Technology, which defines a set of industry standards and best practices for managing cybersecurity risks. Yet these standards are limited to addressing the unique complexities of CPPSs. For instance, most standards are not comprehensive for the high interdependencies and vulnerabilities inherent to CPPSs, especially those pertaining to multienergy systems. As a consequence, they cannot provide interoperable security solutions that can be seamlessly applied across different CPPSs.

C. Evolution of Cyberattacks

As CPPSs become increasingly intelligent, new security vulnerabilities are identified, which offer novel opportunities for attackers. The constant evolution of cyberattacks' means results in the emergence of new cyberattacks against CPPSs. Attackers can use system detection mechanisms' vulnerabilities to build covert attacks that can bypass common detection mechanisms, such as widely used fault detection, isolation, and recovery. The coupling between CPPSs' cyber layer and the physical layer is high, and any small fault caused by the attacks may propagate rapidly due to the strong coupling of dual networks, resulting in more frequent large-scale blackouts. These blackouts could severely endanger the security, stability, and economic operation of CPPSs [47], [124]. Thus, understanding the attack mechanisms and the cascading failure is essential in CPPSs' research to prevent and mitigate the effects of these attacks. The analysis of new attack mechanisms is necessary to identify and understand the emerging threats to CPPSs. The analysis will help researchers develop and design more robust and effective security mechanisms that can address these emerging threats. Moreover, the analysis of cascading failure can provide insights into the propagation of faults caused by cyberattacks and assist in developing techniques to contain the faults before they spread and cause more extensive damage. This research trend requires further investigation to develop new approaches that can effectively secure CPPSs against new and emerging threats.

D. Privacy Concerns

Privacy concerns constitute an important challenge in the fast-expanding realm of CPPSs. The dense interconnectivity and multidirectional flows of information among distinct components of a CPPS create substantial data privacy risks. As CPPSs become more intertwined with people's everyday lives, voluminous data are generated, exchanged, shared, and stored by different entities. Such data, ranging from usage behaviors to personal information, are valuable and often sought

by malicious entities. In this regard, confidentiality of individual information is a crucial facet of the privacy challenge. As systems become more interconnected and smarter, they can collect granular user data for efficiency and adaptability improvements. These data contain users' personal information, reveal their behavior details, and reflect their (sensitive) preferences, which can lead to severe privacy infringements if misused.

VII. Solutions to the Identified Challenges

In this section, we suggest some potential solutions to the identified challenges to the cybersecurity of CPPSs. We also offer strategic insights and actionable tactics to address these challenges that pertain to interdependencies, standards, holistic system visibility, and evolving cyberattacks. In particular, we underscore the importance of proactive, comprehensive, and collaborative approaches to improve the security and resilience of CPPSs, which are crucial to the continued advancement of these complex systems as well as their deployments and utilization.

A. Comprehensive Interdependency Solution

The interdependency challenge in CPPSs necessitates a systematic, multilayered approach that duly considers the nuanced interrelations of different system components. The inherent complexity of a CPPS, due to its cyber–physical nature and the interconnectedness of multiple energy storage and conversion technologies, requires comprehensive solutions capable of estimating, mitigating, and managing potential disruptions. Toward that end, advanced modeling and simulation techniques are vital and can unravel the intricate interactions in a CPPS. They must replicate the operational intricacies of the system and mimic the complex interplays of distinct components and the probable cascading effects caused by local failures. Digital twins are utilitarian and enable researchers, system architects, and operators to scrutinize the dynamics and interdependency in a CPPS, identify vulnerable nodes, and enlighten strategies and solutions for system resilience.

B. Establishment of Standardization

The lack of unified security standards and protocols constitutes a critical barrier to secured CPPSs. This requires concerted efforts to establish a comprehensive, universally agreed set of security standards that are specific to the unique challenges of CPPSs. Regulatory authorities, in close collaboration with industry stakeholders and security experts, play an important role in this endeavor. They must drive the creation and adoption of standard security protocols to facilitate and foster seamless interoperability across different CPPSs. Such efforts have to consider all important facets of security from physical component safety to cyberattack resilience and should evolve with and be guided by the related technological advancements.

C. Addressing the Evolution of Cyberattacks

The dynamic nature of CPPSs and the continuous evolution of cyber threats demand a re-evaluation of and adjustment to security strategies over time. As CPPSs become increasingly complex and interconnected, new vulnerabilities are discovered and can be exploited by cyberattacks. To develop robust preventive and mitigative measures, it is imperative to analyze the underlying attack mechanisms and the probable disastrous cascading failures they can create. A proactive, multifaceted strategy helps estimate and respond to cyberattacks launched in different shapes and forms. Toward that end, frequent threat modeling and risk assessments are needed to discover the potential system vulnerabilities, attack vectors, and the probable consequences of attacks.

D. Addressing Privacy Concerns

Multifaceted approaches are crucial to address the privacy concerns in the context of CPPS. This involves advanced privacy-preserving technologies, such as differential privacy, homomorphic encryption, and secure multiparty computation, which can provide robust protections for sensitive data while ensuring the necessary system functionalities. Data governance also should be implemented in each organization that is involved in the operations of a CPPS. Policies, structures, and processes specified in a strict regime establish explicit rules and mechanisms for data collection, access, usage, and sharing to ensure the confidentiality of sensitive data and prevent costly privacy breaches. Deployments of reliable authentication systems and stringent data access controls are integral to an effective governance framework. In addition, frequent privacy impact assessments represent an important means to help organizations stay abstract of privacy risks and threats. By understanding the privacy implications to CPPSs on a continual and timely basis, organizations can pre-emptively address vulnerabilities and mitigate privacy risks before actual data breaches. Finally, user awareness and training are a cornerstone of privacy protection and preservation strategy. A culture of respecting, valuing, and protecting data privacy must be established in the organization, which should involve users and different key stakeholders to address their privacy concerns.

VIII. Conclusion

The advances of CPPSs have brought forth exciting opportunities to enhance the effectiveness, efficiency, and flexibility in the energy sector; but they also are accompanied by worrisome cybersecurity threats and challenges. Our comprehensive review of extant literature reveals the increasing importance of CPPSs and the stressed need for strategies and methods to address cyber threats in general and cyberattacks in particular. We examine CPPSs and delve into the intricacies of different cyberattack types, strategies for attack detection, and methods for mitigation and restoration. We analyze the evolving nature of cyberattacks and highlight the increasing complexity and intricacy of CPPSs from the lens of multienergy systems. The interdependencies amongst distinct, related system components

make CPPS more susceptible to cascading failures caused by cyberattacks. In addition, the distributed nature of these systems and the multiplicity of stakeholders often restrict the entire system's visibility, which further complicates timely detections and responses to attacks. Our review underscores the criticality of adaptive strategies for attack mitigation by incorporating advanced technologies, such as predictive analytics, sensors, and drones. These strategies entail effective resource allocation, redundancy, disaster response planning, and timely backup systems. The existing literature recognizes the importance of system restoration after successful cyberattacks. Toward that end, damage assessment, system diagnosis, repair, and rigorous testing are crucial because they can ensure complete system recovery and vulnerability removals. More efforts are needed to develop innovative recovery frameworks for the enhanced resilience of CPPSs against cyberattacks.

REFERENCES

[1] J. Chen and Q. Zhu, "A cross-layer design approach to strategic cyber defense and robust switching control of cyber-physical wind energy systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, no. 1, pp. 624–635, Jan. 2023.

[2] T. Yang, Y. Liu, and W. Li, "Attack and defence methods in cyber-physical power system," *IET Energy Syst. Integr.*, vol. 4, no. 2, pp. 159–170, 2022.

[3] S. Li, P. Zhao, C. Gu, J. Li, D. Huo, and S. Cheng, "Aging mitigation for battery energy storage system in electric vehicles," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2152–2163, May 2023, doi: 10.1109/TSG.2022.3210041.

[4] S. Rath, I. Zografopoulos, P. P. Vergara, V. C. Nikolaidis, and C. Konstantinou, "Behind closed doors: Process-level rootkit attacks in cyber-physical microgrid systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2022, pp. 1–5.

[5] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019, doi: 10.1109/TSG.2018.2813280.

[6] X. Chen et al., "Design experiences in minimalistic flying sensor node platform through sensorfly," *ACM Trans. Sensor Netw.*, vol. 13, no. 4, 2017, Art. no. 33.

[7] K.-D. Lu, Z.-G. Wu, and T. Huang, "Differential evolution-based three stage dynamic cyber-attack of cyber-physical power systems," *IEEE/ASME Trans. Mechatronics*, vol. 28, no. 2, pp. 1137–1148, Apr. 2023, doi: 10.1109/TMECH.2022.3214314.

[8] M. Zhou, C. Liu, A. A. Jahromi, D. Kundur, J. Wu, and C. Long, "Revealing vulnerability of N-1 secure power systems to coordinated cyber-physical attacks," *IEEE Trans. Power Syst.*, vol. 38, no. 2, pp. 1044–1057, Mar. 2023, doi: 10.1109/TPWRS.2022.3169482.

[9] D. P. Fidler, "Was Stuxnet an act of war? Decoding a cyberattack," *IEEE Secur. Privacy*, vol. 9, no. 4, pp. 56–59, Jul./Aug. 2011, doi: 10.1109/MSP.2011.96.

[10] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[11] C. Edwards and I. Press, "An analysis of a cyberattack on a nuclear plant: The Stuxnet worm," *Crit. Infrastruct. Protection*, vol. 116, 2014, Art. no. 59.

[12] S. Kim, G. Heo, E. Zio, J. Shin, and J.-G. Song, "Cyber attack taxonomy for digital environment in nuclear power plants," *Nucl. Eng. Technol.*, vol. 52, no. 5, pp. 995–1001, 2020.

[13] H. Tang, H. Zhang, Z. Shi, X. Chen, W. Ding, and X.-P. Zhang, "Autonomous swarm robot coordination via mean-field control embedding multi-agent reinforcement learning," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, 2023, pp. 8820–8826.

[14] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017, doi: 10.1109/TPWRS.2016.2631891.

[15] M. Willett, "The cyber dimension of the Russia–Ukraine war," *Survival*, vol. 64, no. 5, pp. 7–26, 2022.

[16] A. Gochua and T. Zedelashvili, "Cyber threats and asymmetric military challenges in the context of nuclear security: Ukrainian and international cases analysis," *Ukrainian Policymaker*, vol. 7, pp. 20–27, 2020.

[17] J.-W. Myung and S. Hong, "ICS malware Triton attack and countermeasures," *Int. J. Emerg. Multidiscipl. Res.*, vol. 3, no. 2, pp. 13–17, 2019.

[18] R. Kumar, R. Kela, S. Singh, and R. Trujillo-Rasua, "APT attacks on industrial control systems: A tale of three incidents," *Int. J. Crit. Infrastruct. Protection*, vol. 37, 2022, Art. no. 100521.

[19] A. Rostami, M. Mohammadi, and H. Karimipour, "Reliability assessment of cyber-physical power systems considering the impact of predicted cyber vulnerabilities," *Int. J. Elect. Power Energy Syst.*, vol. 147, May 2023, Art. no. 108892, doi: 10.1016/j.ijepes.2022.108892.

[20] Y. Chen, M. Sun, Z. Chu, S. Camal, G. Kariniotakis, and F. Teng, "Vulnerability and impact of machine learning-based inertia forecasting under cost-oriented data integrity attack," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2275–2287, May 2023, doi: 10.1109/TSG.2022.3207517.

[21] Q. Zhang and F. Li, "Cyber-vulnerability analysis for real-time power market operation," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3527–3537, Jul. 2021, doi: 10.1109/TSG.2021.3066398.

[22] Y. Zheng, Z. Yan, K. Chen, J. Sun, Y. Xu, and Y. Liu, "Vulnerability assessment of deep reinforcement learning models for power system topology optimization," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3613–3623, Jul. 2021, doi: 10.1109/TSG.2021.3062700.

[23] X. Li and K. W. Hedman, "Enhancing power system cyber-security with systematic two-stage detection strategy," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1549–1561, Mar. 2020, doi: 10.1109/TPWRS.2019.2942333.

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

[25] E. Hallaji, R. Razavi-Far, M. Wang, M. Saif, and B. Fardanesh, "A stream learning approach for real-time identification of false data injection attacks in cyber-physical power systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 3934–3945, Oct. 2022, doi: 10.1109/TIFS.2022.3216948.

[26] H. M. Khalid, F. Flitti, M. S. Mahmoud, M. M. Hamdan, S. M. Muyeen, and Z. Y. Dong, "Wide area monitoring system operations in modern power grids: A median regression function-based state estimation approach towards cyber attacks," *Sustain. Energy, Grids Netw.*, vol. 34, Jun. 2023, Art. no. 101009, doi: 10.1016/j.segan.2023.101009.

[27] K. Bitirgen and Ü. B. Filik, "A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid," *Int. J. Crit. Infrastruct. Protection*, vol. 40, Mar. 2023, Art. no. 100582, doi: 10.1016/j.ijcip.2022.100582.

[28] Q. Su, H. Wang, C. Sun, B. Li, and J. Li, "Cyber-attacks against cyber-physical power systems security: State estimation, attacks reconstruction and defense strategy," *Appl. Math. Comput.*, vol. 413, Jan. 2022, Art. no. 126639, doi: 10.1016/j.amc.2021.126639.

[29] P. Zhao et al., "Cyber-resilient multi-energy management for complex systems," *IEEE Trans. Ind. Inform.*, vol. 18, no. 3, pp. 2144–2159, Mar. 2022, doi: 10.1109/TII.2021.3097760.

[30] Z. Zhang, S. Huang, Y. Chen, B. Li, and S. Mei, "Diversified software deployment for long-term risk mitigation in cyber-physical power systems," *IEEE Trans. Power Syst.*, vol. 37, no. 1, pp. 377–387, Jan. 2022, doi: 10.1109/TPWRS.2021.3086681.

[31] Z. Liu and L. Wang, "Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1552–1564, Mar. 2021, doi: 10.1109/TSG.2020.3028123.

[32] M. Ganjkhani, M. Gilanifar, J. Giraldo, and M. Parvania, "Integrated cyber and physical anomaly location and classification in power distribution systems," *IEEE Trans. Ind. Inform.*, vol. 17, no. 10, pp. 7040–7049, Oct. 2021, doi: 10.1109/TII.2021.3065080.

[33] M. Ghafouri, U. Karaagac, A. Ameli, J. Yan, and C. Assi, "A cyber attack mitigation scheme for series compensated DFIG-based wind parks," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5221–5232, Nov. 2021, doi: 10.1109/TSG.2021.3091535.

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

[35] K. Chen et al., "A game theory-based approach for vulnerability analysis of a cyber-physical power system," *Energies*, vol. 12, no. 15, 2019, Art. no. 3002, doi: 10.3390/en12153002.

[36] G. Wu and Z. S. Li, "Cyber—physical power system (CPPS): A review on measures and optimization methods of system resilience," *Front. Eng. Manage.*, vol. 8, no. 4, pp. 503–518, Dec. 2021, doi: 10.1007/s42524-021-0163-3.

[37] X. Cai, Q. Wang, Y. Tang, and L. Zhu, "Review of cyber-attacks and defense research on cyber physical power system," in *Proc. IEEE Sustain. Power Energy Conf.*, 2019, pp. 487–492.

[38] C. Li, Z. Dong, G. Chen, B. Zhou, J. Zhang, and X. Yu, "Data-driven planning of electric vehicle charging infrastructure: A case study of Sydney, Australia," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3289–3304, Jul. 2021, doi: 10.1109/TSG.2021.3054763.

[39] C. Li et al., "Interpretable memristive LSTM network design for probabilistic residential load forecasting," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 6, pp. 2297–2310, Jun. 2022, doi: 10.1109/TCSI.2022.3155443.

[40] IEEE Task Force on Interfacing Techniques for Simulation Tools et al., "Interfacing power system and ICT simulators: Challenges, state-of-the-art, and case studies," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 14–24, Jan. 2018, doi: 10.1109/TSG.2016.2542824.

[41] L. Yu et al., "Deep reinforcement learning for smart home energy management," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2751–2762, Apr. 2020, doi: 10.1109/JIOT.2019.2957289.

[42] S. Xin, Q. Guo, J. Wang, C. Chen, H. Sun, and B. Zhang, "Information masking theory for data protection in future cloud-based energy management," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5664–5676, Nov. 2018, doi: 10.1109/TSG.2017.2693345.

[43] Y. Li, D. W. Gao, W. Gao, H. Zhang, and J. Zhou, "Double-mode energy management for multi-energy system via distributed dynamic event-triggered Newton-Raphson algorithm," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5339–5356, Nov. 2020, doi: 10.1109/TSG.2020.3005179.

[44] P. Zhao, C. Gu, D. Huo, Y. Shen, and I. Hernando-Gil, "Two-stage distributionally robust optimization for energy hub systems," *IEEE Trans. Ind. Inform.*, vol. 16, no. 5, pp. 3460–3469, May 2020, doi: 10.1109/TII.2019.2938444.

[45] Y. Jiang, Z. Ren, and W. Li, "Committed carbon emission operation region for integrated energy systems: Concepts and analyses," *IEEE Trans. Sustain. Energy*, vol. 15, no. 2, pp. 1194–1209, Apr. 2024, doi: 10.1109/TSTE.2023.3330857.

[46] P. Wang, P. Zhong, M. Yu, Y. Pu, S. Zhang, and P. Yu, "Trends in energy consumption under the multi-stage development of ICT: Evidence in China from 2001 to 2030," *Energy Rep.*, vol. 8, pp. 8981–8995, Nov. 2022, doi: 10.1016/j.egyr.2022.07.003.

[47] V. Engström and R. Lagerström, "Two decades of cyberattack simulations: A systematic literature review," *Comput. Secur.*, vol. 116, May 2022, Art. no. 102681, doi: 10.1016/j.cose.2022.102681.

[48] J. Tian, B. Wang, J. Li, and C. Konstantinou, "Datadriven false data injection attacks against cyber-physical power systems," *Comput. Secur.*, vol. 121, Oct. 2022, Art. no. 102836, doi: 10.1016/j.cose.2022.102836.

[49] R. Jiao, G. Xun, X. Liu, and G. Yan, "A new AC false data injection attack method without network information," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5280–5289, Nov. 2021, doi: 10.1109/TSG.2021.3102329.

[50] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Inform.*, vol. 13, no. 2, pp. 411–423, Apr. 2017, doi: 10.1109/TII.2016.2614396.

[51] M. Azzam, L. Pasquale, G. Provan, and B. Nuseibeh, "Forensic readiness of industrial control systems under stealthy attacks," *Comput. Secur.*, vol. 125, Feb. 2023, Art. no. 103010, doi: 10.1016/j.cose.2022.103010.

[52] P. Zhao et al., "A cyber-secured operation for water-energy nexus," *IEEE Trans. Power Syst.*, vol. 36, no. 4, pp. 3105–3117, Jul. 2021, doi: 10.1109/TPWRS.2020.3043757.

[53] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 198–207, Feb. 2017, doi: 10.1109/TII.2015.2470218.

[54] S. Soltan, P. Mittal, and H. V. Poor, "Line failure detection after a cyber-physical attack on the grid using Bayesian regression," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3758–3768, Sep. 2019, doi: 10.1109/TPWRS.2019.2910396.

[55] K.-D. Lu and Z.-G. Wu, "Multi-objective false data injection attacks of cyber–physical power systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 9, pp. 3924–3928, Sep. 2022, doi: 10.1109/TCSII.2022.3181827.

[56] Z.-H. Pang, L.-Z. Fan, Z. Dong, Q.-L. Han, and G.-P. Liu, "False data injection attacks against partial sensor measurements of networked control systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 1, pp. 149–153, Jan. 2022, doi: 10.1109/TCSII.2021.3073724.

[57] Y. Yılmaz and S. Uludag, "Timely detection and mitigation of IoT-based cyberattacks in the smart grid," *J. Franklin Inst.*, vol. 358, no. 1, pp. 172–192, Jan. 2021, doi: 10.1016/j.jfranklin.2019.02.011.

[58] M. Tvaronavičienė, T. Plėta, S. Della Casa, and J. Latvys, "Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, U.K., France, Estonia and Lithuania," *Insights Regional Develop.*, vol. 2, no. 4, pp. 802–813, 2020.

[59] P. Zhao, C. Gu, Y. Ding, H. Liu, Y. Bian, and S. Li, "Cyber-resilience enhancement and protection for uneconomic power dispatch under cyber-attacks," *IEEE Trans. Power Del.*, vol. 36, no. 4, pp. 2253–2263, Aug. 2021, doi: 10.1109/TPWRD.2020.3038065.

[60] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011, doi: 10.1109/TSG.2011.2123925.

[61] R. Kaviani and K. W. Hedman, "An enhanced energy management system including a real-time load-redistribution threat analysis tool and cyber-physical SCED," *IEEE Trans. Power Syst.*, vol. 37, no. 5, pp. 3346–3358, Sep. 2022, doi: 10.1109/TPWRS.2021.3135357.

[62] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 889–901, Mar. 2017, doi: 10.1109/TSG.2016.2569589.

[63] Y. Liu, S. Gao, J. Shi, X. Wei, and Z. Han, "Sequential-mining-based vulnerable branches identification for the transmission network under continuous load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5151–5160, Nov. 2020, doi: 10.1109/TSG.2020.3003340.

[64] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012, doi: 10.1109/TPDS.2012.58.

[65] Z. Huo and B. Wang, "Distributed resilient multi-event cooperative triggered mechanism based discrete sliding-mode control for wind-integrated power systems under denial of service attacks," *Appl. Energy*, vol. 333, Mar. 2023, Art. no. 120636, doi: 10.1016/j.apenergy.2022.120636.

[66] W. Chen, D. Ding, H. Dong, and G. Wei, "Distributed resilient filtering for power systems subject to denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1688–1697, Aug. 2019.

[67] X.-C. ShangGuan et al., "Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks," *Control Eng. Pract.*, vol. 107, 2021, Art. no. 104678.

[68] Z. Hu, S. Liu, W. Luo, and L. Wu, "Resilient distributed fuzzy load frequency regulation for power systems under cross-layer random denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 52, no. 4, pp. 2396–2406, Apr. 2022, doi: 10.1109/TCYB.2020.3005283.

[69] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Sep. 2017.

[70] A. Wang, M. Fei, Y. Song, C. Peng, D. Du, and Q. Sun, "Secure adaptive event-triggered control for cyber–physical power systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 54, no. 3, pp. 1722–1733, Mar. 2024.

[71] K. Ibtissam, M. S. Abdelrahman, A. Alrashide, and O. A. Mohammed, "Assessment of protection schemes and their security under denial of service attacks," in *Proc. IEEE Int. Conf. Environ. Elect. Eng.*, 2022, pp. 1–6.

[72] C. Kaura, N. Sindhwani, and A. Chaudhary, "Analysing the impact of cyber-threat to ICS and SCADA systems," in *Proc. Int. Mobile Embedded Technol. Conf.*, 2022, pp. 466–470.

[73] J. Price, R. Dill, S. Dunlap, and M. Rice, "Joint test action group data acquisition for cyber-physical system security," in *Proc. Int. Conf. Smart Syst. Technol.*, 2022, pp. 179–186.

[74] U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian, "Cloud-based email phishing attack using machine and deep learning algorithm," *Complex Intell. Syst.*, vol. 9, pp. 3043–3070, 2023.

[75] M. F. Ansari, A. Panigrahi, G. Jakka, A. Pati, and K. Bhattacharya, "Prevention of phishing attacks using AI algorithm," in *Proc. 2nd Odisha Int. Conf. Elect. Power Eng., Commun. Comput. Technol.*, 2022, pp. 1–5.

[76] S. M. Han, C. Lee, and P. H. Seong, "Estimating the frequency of cyber threats to nuclear power plants based on operating experience analysis," *Int. J. Crit. Infrastruct. Protection*, vol. 37, 2022, Art. no. 100523.

[77] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electr. Power Syst. Res.*, vol. 215, 2023, Art. no. 108975.
[78] A. Vangala and A. K. Das, "Privacy-preserving blockchain-based authentication in smart energy systems," in *Proc. 20th ACM Conf. Embedded Networked Sensor Syst.*, 2022, pp. 1208–1214.
[79] R. V. Yohanandhan et al., "A specialized review on outlook of future cyber-physical power system (CPPS) testbeds for securing electric power grid," *Int. J. Elect. Power Energy Syst.*, vol. 136, 2022, Art. no. 107720.
[80] N. Hoque and D. Bhattacharyya, "Internet-of-Thing-enabled energy systems: Architectures, issues, and challenges," in *Nanoelectronics: Physics, Materials and Devices*. Amsterdam, The Netherlands: Elsevier, 2023, pp. 487–506.
[81] W. Wang, F. Harrou, B. Bouyeddou, S.-M. Senouci, and Y. Sun, "A stacked deep learning approach to cyber-attacks detection in industrial systems: Application to power system and gas pipeline systems," *Cluster Comput.*, vol. 25, pp. 561–578, 2022.
[82] A. Barboni, H. Rezaee, F. Boem, and T. Parisini, "Detection of covert cyber-attacks in interconnected systems: A distributed model-based approach," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3728–3741, Sep. 2020.
[83] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.
[84] Z. Liu and L. Wang, "FlipIt game model-based defense strategy against cyberattacks on SCADA systems considering insider assistance," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2791–2804, Mar. 2021.
[85] W. Hongxia and Giri, "PMU impact on state estimation reliability for improved grid security," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Exhib.*, 2006, pp. 1349–1351, doi: 10.1109/TDC.2006.1668709.
[86] Y. M. Khaw, A. A. Jahromi, M. F. M. Arani, S. Sanner, D. Kundur, and M. Kassouf, "A deep learning-based cyberattack detection system for transmission protective relays," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2554–2565, May 2021, doi: 10.1109/TSG.2020.3040361.
[87] Y. Yuan, Y. Guo, K. Dehghanpour, Z. Wang, and Y. Wang, "Learning-based real-time event identification using rich real PMU data," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5044–5055, Nov. 2021, doi: 10.1109/TPWRS.2021.3081608.
[88] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Trans. Ind. Inform.*, vol. 17, no. 1, pp. 650–658, Jan. 2021.
[89] A. Parizad and C. J. Hatziadoniu, "Cyber-attack detection using principal component analysis and noisy clustering algorithms: A collaborative machine learning-based framework," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4848–4861, Nov. 2022.
[90] Y. Ding, K. Ma, T. Pu, X. Wang, R. Li, and D. Zhang, "A deep learning-based classification scheme for cyber-attack detection in power system," *IET Energy Syst. Integr.*, vol. 3, no. 3, pp. 274–284, 2021.
[91] S. Nath, I. Akingeneye, J. Wu, and Z. Han, "Quickest detection of false data injection attacks in smart grid with dynamic models," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, pp. 1292–1302, Feb. 2022, doi: 10.1109/JESTPE.2019.2936587.
[92] H. H. Alhelou and P. Cuffe, "A dynamic-state-estimator-based tolerance control method against cyberattack and erroneous measured data for power systems," *IEEE Trans. Ind. Inform.*, vol. 18, no. 7, pp. 4990–4999, Jul. 2022, doi: 10.1109/TII.2021.3093836.
[93] M. Leng, S. Sahoo, F. Blaabjerg, and M. Molinas, "Projections of cyberattacks on stability of DC microgrids—Modeling principles and solution," *IEEE Trans. Power Electron.*, vol. 37, no. 10, pp. 11774–11786, Oct. 2022, doi: 10.1109/TPEL.2022.3175237.
[94] F. Milano and A. Gómez-Expósito, "Detection of cyber-attacks of power systems through Benford's law," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2741–2744, May 2021, doi: 10.1109/TSG.2020.3042897.
[95] T. Zhao, M. Yue, and J. Wang, "Robust power system stability assessment against adversarial machine learning-based cyberattacks via online purification," *IEEE Trans. Power Syst.*, vol. 38, no. 6, pp. 5613–5622, Nov. 2023.
[96] Y. Yuan, K. Dehghanpour, Z. Wang, and F. Bu, "A joint distribution system state estimation framework via deep actor-critic learning method," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 796–806, Jan. 2023, doi: 10.1109/TPWRS.2022.3155649.
[97] Y. Yuan, K. Dehghanpour, Z. Wang, and F. Bu, "Multisource data fusion outage location in distribution systems via probabilistic graphical models," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1357–1371, Mar. 2022, doi: 10.1109/TSG.2021.3128752.
[98] M. Nabil, M. Ismail, M. Mahmoud, M. Shahin, K. Qaraqe, and E. Serpedin, "Deep learning-based detection of electricity theft cyber-attacks in smart grid AMI networks," in *Deep Learning Applications for Cyber Security*. New York, NY, USA: Springer, 2019, pp. 73–102.
[99] S. D. Roy, S. Debbarma, and J. M. Guerrero, "Machine learning based multi-agent system for detecting and neutralizing unseen cyber-attacks in AGC and HVDC systems," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 12, no. 1, pp. 182–193, Mar. 2022.
[100] A. Ameli, A. Ayad, E. F. El-Saadany, M. M. A. Salama, and A. Youssef, "A learning-based framework for detecting cyber-attacks against line current differential relays," *IEEE Trans. Power Del.*, vol. 36, no. 4, pp. 2274–2286, Aug. 2021.
[101] T. Teng and L. Ma, "Deep learning-based risk management of financial market in smart grid," *Comput. Elect. Eng.*, vol. 99, 2022, Art. no. 107844.
[102] M. Elimam, Y. J. Isbeih, S. K. Azman, M. S. E. Moursi, and K. A. Hosani, "Deep learning-based PMU cyber security scheme against data manipulation attacks with WADC application," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2148–2161, May 2023.
[103] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. U. Rehman, "A secure ensemble learning-based fog-cloud approach for cyberattack detection in IoMT," *IEEE Trans. Ind. Inform.*, vol. 19, no. 10, pp. 10125–10132, Oct. 2023.
[104] A. Vedant, A. Yadav, S. Sharma, O. Thite, and A. Sheikh, "Detecting cyber attacks in a cyber-physical power system: A machine learning based approach," in *Proc. Glob. Energy Conf.*, 2022, pp. 272–277.
[105] C.-C. Sun, D. J. S. Cardenas, A. Hahn, and C.-C. Liu, "Intrusion detection for cybersecurity of smart meters," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612–622, Jan. 2021, doi: 10.1109/TSG.2020.3010230.
[106] K. Sun et al., "WAMS-based HVDC damping control for cyber attack defense," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 702–713, Jan. 2023.
[107] D. Choeum and D.-H. Choi, "Trilevel smart meter hardening strategy for mitigating cyber attacks against volt/VAR optimization in smart power distribution systems," *Appl. Energy*, vol. 304, Dec. 2021, Art. no. 117710, doi: 10.1016/j.apenergy.2021.117710.
[108] F. Wei, Z. Wan, and H. He, "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2476–2486, May 2020.
[109] M. Ni, M. Li, Y. Wu, and Q. Wang, "Concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks," *J. Modern Power Syst. Clean Energy*, vol. 9, no. 3, pp. 477–484, May 2021.
[110] P. Lau, L. Wang, Z. Liu, W. Wei, and C.-W. Ten, "A coalitional cyber-insurance design considering power system reliability and cyber vulnerability," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5512–5524, Nov. 2021, doi: 10.1109/TPWRS.2021.3078730.
[111] P. Lau, W. Wei, L. Wang, Z. Liu, and C.-W. Ten, "A cybersecurity insurance model for power system reliability considering optimal defense resource allocation," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4403–4414, Sep. 2020.
[112] D. Niyato, D. T. Hoang, P. Wang, and Z. Han, "Cyber insurance for plug-in electric vehicle charging in vehicle-to-grid systems," *IEEE Netw.*, vol. 31, no. 2, pp. 38–46, Mar./Apr. 2017, doi: 10.1109/MNET.2017.1600321NM.
[113] D. T. Hoang, P. Wang, D. Niyato, and E. Hossain, "Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: A cyber insurance-based model," *IEEE Access*, vol. 5, pp. 732–754, 2017.
[114] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," *Comput. Sci. Rev.*, vol. 24, pp. 35–61, 2017.
[115] S. Acharya, R. Mieth, C. Konstantinou, R. Karri, and Y. Dvorkin, "Cyber insurance against cyberattacks on electric vehicle charging stations," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1529–1541, Mar. 2022, doi: 10.1109/TSG.2021.3133536.

[116] A. Ahmed et al., "Spatio-temporal deep graph network for event detection, localization, and classification in cyber-physical electric distribution system," *IEEE Trans. Ind. Inform.*, vol. 20, no. 2, pp. 2397–2407, Feb. 2024, doi: 10.1109/TII.2023.3290942.

[117] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007–4020, Sep. 2023, doi: 10.1109/TSG.2023.3237011.

[118] H. Huang et al., "Cyberattack defense with cyber-physical alert and control logic in industrial controllers," *IEEE Trans. Ind. Appl.*, vol. 58, no. 5, pp. 5921–5934, Sep./Oct. 2022.

[119] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.

[120] J. Khazaei and A. Asrari, "Second-order cone programming relaxation of stealthy cyberattacks resulting in overvoltages in cyber-physical power systems," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4267–4278, Sep. 2022, doi: 10.1109/JSYST.2021.3108635.

[121] Z. Zhang, S. Huang, Y. Chen, B. Li, and S. Mei, "Cyber-physical coordinated risk mitigation in smart grids based on attack-defense game," *IEEE Trans. Power Syst.*, vol. 37, no. 1, pp. 530–542, Jan. 2022, doi: 10.1109/TPWRS.2021.3091616.

[122] Y. Liu, R. Fan, and V. Terzija, "Power system restoration: A literature review from 2006 to 2016," *J. Modern Power Syst. Clean Energy*, vol. 4, no. 3, pp. 332–341, Jul. 2016.

[123] M. Stănculescu, S. Deleanu, P. C. Andrei, and H. Andrei, "A case study of an industrial power plant under cyberattack: Simulation and analysis," *Energies*, vol. 14, no. 9, 2021, Art. no. 2568.

[124] T. Mackey, "How to prepare for a cyberattack," Accessed on: Jul. 12, 2021. [Online]. Available: https://securityboulevard.com/2021/07/how-to-prepare-for-a-cyberattack/

Alexis Pengfei Zhao was born in Beijing, China. He received the B.Eng. and Ph.D. degrees in electrical engineering from the University of Bath, Bath, U.K., in 2017 and 2021, respectively.

He was a visiting Ph.D. student with Smart Grid Operations and Optimization Laboratory, Tsinghua University, Beijing, China, in 2019. He is currently an Associate Professor with the Institute of Automation, Chinese Academy of Sciences, Beijing. He is also an Ezra SYSEN Research Associate of System Engineering with Cornell University, Ithaca, NY, USA. His major research interests include the low-carbon energy systems and cyber–physical–social systems.

Shuangqi Li was born in Beijing, China. He received the B.Eng. degree in vehicle engineering from the Beijing Institute of Technology, Beijing, China, in 2018, and the Ph.D. degree in electronic and electrical engineering from the Department of Electronic and Electrical Engineering, University of Bath, Bath, U.K, in 2023.

He was a Research Assistant with the National Engineering Laboratory for Electric Vehicles, Beijing Institute of Technology, Beijing, from 2018 to 2019. From 2022 to 2023, he was a Visiting Ph.D. Research Fellow with the Department of Electrical Engineering, The Hong Kong Polytechnic University, Hong Kong, and Smart Grid Operations and Optimization Laboratory, Tsinghua University, Beijing. In 2023, he was also a Postdoctoral Research Associate with the Department of Electrical Engineering, The Hong Kong Polytechnic University. He is currently an Eric and Wendy Schmidt AI in Science Postdoctoral Research Fellow with the Department of Systems Engineering, Cornell University, Ithaca, NY, USA. His major research interests include the big data analysis, deep-learning algorithm, deep reinforcement learning algorithm, operation and planning of smart grid systems, hybrid energy storage system, and V2G service.

Chenghong Gu was born in Anhui province, China. He received the bachelor's degree in electrical engineering from the Shanghai University of Electric Power, Shanghai, China, in 2004, the master's degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 2007, and the Ph.D. degree from the University of Bath, Bath, U.K., in 2010, all in electrical engineering.

He was with DECC U.K. to quantify the value of demand response to the energy system under 2050 pathways. He was involved in the design of the network pricing method—long-run incremental cost pricing for Western Power Distribution, which was adopted by the wide U.K. power industry. He was an EPSRC Research Fellow with the University of Bath. He is a reader with the Department of Electronic and Electrical Engineering, University of Bath. His major research interests include power economics and markets, multivector energy systems, and smart grid planning and operation.

Dr. Gu is a Subject Editor for the *IET Smart Grid*.

Xiaohe Yan was born in Shaanxi, China. He received the bachelor's degree in electrical engineering from the Xi'an University of Technology, Xi'an, China, in 2013, and the master's and Ph.D. degrees in electrical engineering from the University of Bath, Bath, U.K., in 2015 and 2019, respectively.

He was a Research Associate with Macaw University from 2019 to 2020. He is currently an Associate Professor with the Department of Electronic and Electrical Engineering, North China Electric Power University, Beijing, China. His major research is in energy storage, power system planning, analysis, and power system economics.

Paul Jen-Hwa Hu received the Ph.D. degree in management information systems from the University of Arizona, Tucson, AZ, USA, in 1997.

He is a David Eccles Chair Professor with the David Eccles School of Business, The University of Utah, Salt Lake City, UT, USA. His research interests include information technology for healthcare, business analytics, digital transformation, technology implementation and management, and technology-empowered learning and knowledge communities. He has published in various IEEE journals and transactions, *Management Information Systems Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Decision Sciences*, *Journal of Medical Internet Research*, *Journal of Biomedical Informatics*, *Communications of the ACM*, and *ACM Transactions on Management Information Systems*.

Zhaoyu Wang (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 2009 and 2012 respectively, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2012 and 2015, respectively.

He is a Northrop Grumman Endowed Associate Professor with Iowa State University, Ames, IA, USA. His research interests include optimization and data analytics in power distribution systems and microgrids.

Dr. Wang was a recipient of the National Science Foundation CAREER Award, the Society-Level Outstanding Young Engineer Award from IEEE Power and Energy Society, the Northrop Grumman Endowment, College of Engineering's Early Achievement in Research Award, and the Harpole-Pentair Young Faculty Award Endowment. He is the Principal Investigator for a multitude of projects funded by National Science Foundation, the Department of Energy, National Laboratories, PSERC, and Iowa Economic Development Authority. He is the Technical Committee Program Chair of the IEEE Power System Operation, Planning, and Economics (PSOPE) Committee, the Chair of IEEE PSOPE Award Subcommittee, and the Vice Chair of IEEE Distribution System Operation and Planning Subcommittee, and IEEE Task Force on Advances in Natural Disaster Mitigation Methods. He is an Associate Editor for IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, *IEEE Open Access Journal of Power and Energy*, *IEEE Power Engineering Letters*, and *IET Smart Grid*. He was an Associate Editor for the IEEE TRANSACTIONS ON POWER SYSTEMS and IEEE TRANSACTIONS ON SMART GRID.

Da Xie (Senior Member, IEEE) was born in Heilongjiang province, China. He received the B.S. degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 1991, the M.S. degree in electrical engineering from the Harbin Institute of Technology, Harbin, China, in 1996, and the Ph.D. degree in electrical engineering from Shanghai Jiao Tong University, in 1999.

He is currently a Professor with the Department of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University. His major research interests include multivector energy systems, electrical system simulation, power electronic equipment, and smart grids.

Zhidong Cao received the Ph.D. degree in electrical engineering from the Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences, Beijing, China, in 2008.

He is currently a Professor with the Institute of Automation, Chinese Academy of Sciences. His research direction is big data-based social computing.

Xinlei Chen (Member, IEEE) received the B.E. and M.S. degrees in electronic engineering from Tsinghua University, Beijing, China, in 2009 and 2012, respectively, and the Ph.D. degree in electrical engineering from Carnegie Mellon University, Pittsburgh, PA, USA, in 2018.

He is an Assistant Professor with Shenzhen International Graduate School, Tsinghua University. He was a Postdoctoral Research Associate with Electrical Engineering Department, Carnegie Mellon University, from 2018 to 2020. His research interests lie in AIoT, pervasive computing, and cyber-physical systems.

Dr. Chen was a recipient of several awards from top-tier conferences, including the Best Poster Award from IEEE/ACM IPSN, the Best Demo Award from ACM SenSys, and the Best Paper Award from CPD Workshop of ACM UbiComp.

Chenye Wu (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the Institute for Interdisciplinary Information Sciences (IIIS), Tsinghua University, Beijing, China, in 2013.

He is an Assistant Professor with the School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, (CUHK Shenzhen), China. Before joining CUHK Shenzhen, he was an Assistant Professor with IIIS, Tsinghua University. He was with ETH Zurich as a Wiss. Mitarbeiter (Research Scientist), working with Professor Gabriela Hug in 2016. Before that, Professor Kameshwar Poolla and Professor Pravin Varaiya hosted him as a Postdoctoral Researcher with UC Berkeley for two years. In 2013 and 2014, he spent one year with Carnegie Mellon University as a Postdoctoral Fellow, hosted by Professor Gabriela Hug and Professor Soummya Kar. His Ph.D. advisor is Professor Andrew Yao, the Laureate of A.M. Turing Award in 2000. He is currently working on data-driven power system operations.

Dr. Wu was a recipient of the Best Paper Award, and corecipient of IEEE SmartGridComm 2012, IEEE PES General Meeting 2013, and IEEE PES General Meeting 2020.

Tianyi Luo received the B.E. degree in automation from the Beijing University of Chemical Technology, Beijing, China, in 2017, and the Ph.D. degree in computer applied technology from the Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 2022.

She is currently an Assistant Professor with the Institute of Automation, Chinese Academy of Sciences. Her research interests include social computing and big data analysis, information diffusion modeling, and complex networks.

Zikang Wang received the B.S. degree in computer science from Central South University, Changsha, China, in 2016, and the Ph.D. degree in computer applied technology from the Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 2021.

She holds a postdoctoral position with the Institute of Automation, Chinese Academy of Sciences. Her research interests include knowledge graph and natural language processing.

Ignacio Hernando-Gil received the Ph.D. degree in power systems from the University of Edinburgh, Edinburgh, U.K., in 2014.

He is currently an Associate Professor with the ESTIA Institute of Technology, Bidart, France, and also with the Institute for Systems and Computer Engineering, Technology and Science, Porto, Portugal. He was previously a Prize Fellow with the University of Bath, U.K., and a Research Fellow with the University of Edinburgh, U.K. He was also in industry with PassivSystems, Ltd., U.K., and National Grid U.K. He has extensive research in risk modeling and analysis of active distribution networks and the aggregate impact of smart grid technologies on the quality of power supply.