

Review

Research and Prospect of Defense for Integrated Energy Cyber–Physical Systems Against Deliberate Attacks

Tianlei Zang ^{1,2,*} , Xiaoning Tong ^{1,2}, Chuangzhi Li ^{1,2}, Yahui Gong ^{1,2}, Rui Su ^{1,2} and Buxiang Zhou ^{1,2}

¹ College of Electrical Engineering, Sichuan University, Chengdu 610065, China; 2023223030017@stu.scu.edu.cn (X.T.); lichuangzhi@stu.scu.edu.cn (C.L.); gongyahui@stu.scu.edu.cn (Y.G.); 2023223030055@stu.scu.edu.cn (R.S.); hiway_scu@126.com (B.Z.)

² Intelligent Electric Power Grid Key Laboratory of Sichuan Province, Sichuan University, Chengdu 610065, China

* Correspondence: zangtianlei@scu.edu.cn

Abstract: The tight integration of cyber and physical networks in integrated energy cyber–physical systems (IECPS) improves system awareness and coordinated control but also heightens susceptibility to targeted attacks. A robust IECPS defense system is crucial for increasing the system’s resilience against deliberate attacks. Reducing the associated risks is essential to ensure the safe and stable operation of IECPS. In order to enhance the defense capability of IECPS against deliberate attacks, this paper discusses cyberattacks, physical attacks, and coordinated cyber physical attacks (CCPAs) in detail. The attack principles and attack models of each type of attack are described, and then the intentional attack threats faced by IECPS are analyzed. Based on this, the paper reviews the current research landscape regarding countermeasures against deliberate attacks, categorizing the findings into three key areas: preemptive prevention, process response, and post–event recovery and summarizing. The theoretical foundations, system planning, optimal scheduling, and cyber security technologies required for existing defense research are further elaborated. The unresolved issues within these key technologies are analyzed and summarized, followed by the presentation of the problems and challenges faced in defending against deliberate IECPS attacks.



Academic Editor: José Matas

Received: 27 January 2025

Revised: 26 February 2025

Accepted: 13 March 2025

Published: 17 March 2025

Citation: Zang, T.; Tong, X.; Li, C.; Gong, Y.; Su, R.; Zhou, B. Research and Prospect of Defense for Integrated Energy Cyber–Physical Systems Against Deliberate Attacks. *Energies* **2025**, *18*, 1479. <https://doi.org/10.3390/en18061479>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: integrated energy system; deliberate attacks; cyber–physical system; defense strategy

1. Introduction

The ongoing global energy transition has significantly shifted methods of energy production and consumption, gradually replacing the fossil-fuel-dominated energy system of the past with renewable energy sources. Nations worldwide have reached a widely consensus on establishing a green, low-carbon, clean, and efficient energy system, predominantly reliant on renewable energy [1]. Although renewable energy is developing rapidly, the existing energy system lacks sufficient flexibility to accommodate these unstable energy sources due to their inherent randomness and volatility [2,3]. This significantly hinders the progress of the global energy transition.

With advancements in measurement, communication, and control technologies, IECPS use advanced sensing and control mechanisms to coordinate the scheduling of multiple energy systems, thereby enhancing system flexibility and supporting large-scale renewable energy integration and utilization. In contrast to the independent operation of traditional energy systems, IECPS facilitate the coordination of energy systems characterized by diverse time scales and spatial distributions through real-time sensing and precise control

technologies. This approach significantly improves energy utilization efficiency and effectively leverages the potential for system coordination and mutual support. By effectively harnessing this coordination potential, IECPS can mitigate the impact of renewable energy integration on the overall energy system, thus increasing renewable energy consumption.

IECPS employ advanced communication technologies to enhance energy efficiency and support renewable energy integration. However, the deep integration of physical systems and high cyber–physical coupling elevates global and localized vulnerabilities. Due to system convergence, even minor faults within a single energy system can propagate across systems, thereby widening the scope of faults. In more severe scenarios, these faults may continuously accumulate across systems, ultimately resulting in significant multi-system cascading failures. A major blackout occurred at the Datan power plant in Taiwan in August 2017, caused by a disruption in the gas supply. This disruption led to intermittent blackouts across 17 counties and cities, excluding Hualien and Taitung, affecting a total of 6.68 million users [4]. In February 2021, Texas, USA, experienced an extensive blackout that was exacerbated by extreme cold weather conditions. Several natural gas facilities were shut down prematurely, causing fuel shortages and leading to the shutdown of generating units. Additionally, power plant failures and disruptions in load wheeling exacerbated the shortage of natural gas, further contributing to the widespread blackout. This event ultimately affected over 4.5 million people [5]. On the other hand, the coupling of physical and cyber systems leads to the expansion of system network boundaries, thereby significantly increasing cybersecurity risks [6]. For instance, in 2015, the malware “Black Energy” compromised the Ukrainian power grid’s cyber system, resulting in the activation of seven substation switches and causing power outages for 750,000 households over several hours. The attack was orchestrated by multiple programs with well-defined objectives and is regarded as the first significant power outage triggered by a deliberate message attack [7]. In March 2019, a cyberattack on Venezuela’s largest Simón Bolívar hydroelectric power plant triggered a major blackout across 22 states. Following the incident, although 40% of the power was restored, an explosion at the power plant significantly hindered the power restoration process [8]. In September 2019, a cyber nuclear terrorism incident at India’s largest nuclear power plant, the Kudankulam nuclear power plant, resulted in minimal physical damage but sparked widespread societal panic [9]. These events highlight that IECPS face growing risks from deliberate attacks, extreme disasters, and occasional system failures, significantly obstructing their development and the progress of energy transition. Therefore, it is necessary to improve the defense capability of IECPS to cope with the increasing threat of deliberate attacks on the system and to promote the energy transition and the development of IECPS.

Currently, researchers and scholars have extensively studied deliberate attacks on cyber–physical power system and their corresponding defense strategies, leading to the development of relatively mature defense systems. However, research focusing specifically on defending IECPS against deliberate attacks remains scarce, with a systematic review of this domain still notably absent. To address this gap, this paper first analyzes the attack modes and modeling techniques associated with deliberate attacks targeting IECPS. Secondly, based on the evolution of deliberate attacks, this paper summarizes existing defense strategies across three levels: preemptive prevention, process response, and post-event recovery. Subsequently, this paper analyzes the key technologies employed in these defense strategies and addresses the associated challenges. Finally, through systematic analysis of these technological limitations, this work identifies fundamental barriers to achieving effective defense for IECPS against deliberate attacks.

2. Methodology

Before starting the work on this paper, a comprehensive literature search was carried out in major reputed indexed databases including Web of Science, IEEE Xplore, ScienceDirect, and CNKI. In this way, it was ensured that the research results in line with the topic of this paper were taken into consideration, thereby improving the quality of the work in this paper.

We used a large number of terms and keywords in our literature search to ensure that we find significant research results that match our research topic, including but not limited to terms such as power systems, integrated energy systems, smart grids, electric vehicles, deliberate attacks, cyber attacks, information–physical co-attacks, collaborative planning, optimal dispatch, attack detection, security, resilience, and so on. By strategically utilizing a combination of these key terms, we were able to efficiently filter irrelevant documents in our indexed database, thereby accurately identifying the academic literature most relevant to our topic.

To ensure the quality, applicability, and relevance of the literature, we used a rigorous set of selection criteria. First, we limited our search to the years between 2015 and 2024 and focused on research results from the past three years to ensure that they reflected the latest trends in their field. Second, we briefly screened the titles and abstracts of the literature in order to align the selected literature with the research topic. Then, we further reviewed the keywords of the literature by matching them with the core terms we listed to make sure they were highly relevant to our study, saving time and resources by avoiding unnecessary reading and analysis. Finally, we conducted a meticulous content review of the screened literature to distill the theories, methods, and techniques related to our research topic to form a framework for the literature review. In addition, in order to help readers to understand the key theories, methods and techniques more clearly, we also used some representative literature.

In order to provide readers with a more intuitive understanding of the research trends and progress related to the work of this paper, we counted the relevant literature data retrieved from Web of Science for the last ten years. Categorized by research topics, the publication trends shown in Figure 1 were plotted.

As can be seen from Figure 1, the amount of literature related to this paper was generally on the rise during the period between 2015 and 2024. This shows that the work of this paper aligns with the current research hotspots, and at the same time, the research findings strongly support the work of this paper. This upward trend can be attributed to a number of factors. First, as we mentioned in the introduction, the development of IECPS has been driven by policy support, and all kinds of research and applications related to the development of IECPS have been supported by the policies of many countries. Secondly, various energy security incidents have raised the concern of researchers and governments about the safety of utilities, which has driven utilities and researchers to accelerate the construction of more effective defense systems to ensure the safety of IECPS. Finally, the updating of related equipment and technology has provided strong support for the research on IECPS safety. Flexible devices represented by electric vehicles and energy storage devices provide dispatchable resources for IECPS defense optimization. Also, the emerging technology represented by artificial intelligence (AI) promotes the development of IECPS attack detection and defense technology.

To further illustrate the need for the work in this paper, we also conducted a survey of intentional attacks against energy systems over the last decade, the results of which are shown in Table 1.

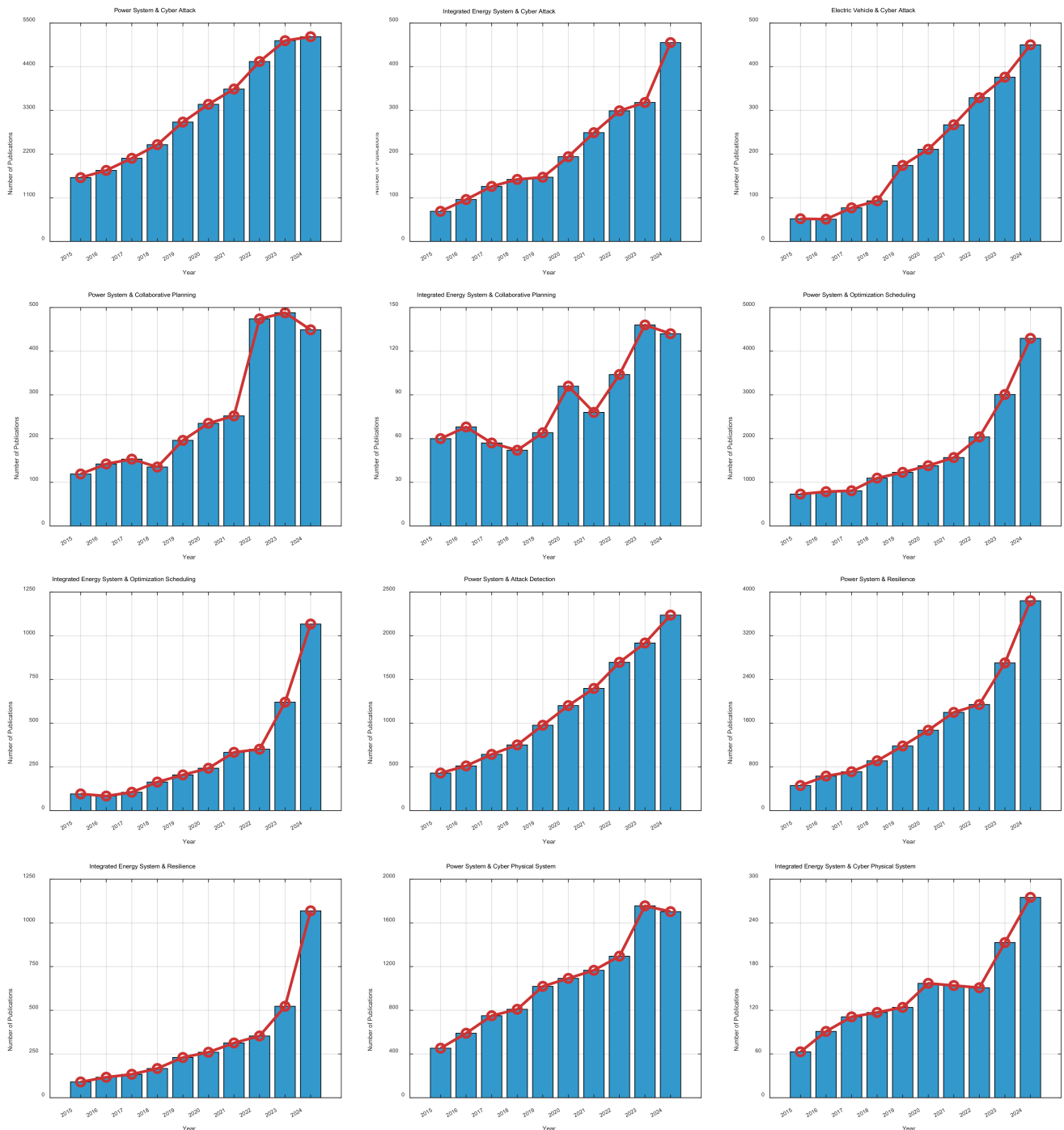


Figure 1. Publication trend charts for the research topics.

In 2015, a cyberattack targeted a power company in western Ukraine, causing widespread power outages for hundreds of thousands of users. The attack was attributed to the Russian advanced persistent threat (APT) group “SandWorm”, marking the first publicly acknowledged successful cyberattack on a power grid. In June 2020, Brazil’s Light S.A. power company was attacked by Sodinokibi ransomware, encrypting its system files and demanding a USD 14 million ransom, severely disrupting operations. In 2020, attackers used Ragnar Locker ransomware to target Portugal’s multinational energy company EDP, claiming to have obtained 10 TB of sensitive data. They threatened to release the data unless EDP paid the ransom. In May 2021, Colonial Pipeline, the largest U.S. fuel pipeline company, was hit by ransomware, forcing it to shut down all pipelines and causing massive economic losses as fuel was trapped in refineries. In April 2022, Ukraine’s

computer emergency response team announced that the Russian group “SandWorm” used the Industroyer2 malware to target Ukraine’s high-voltage substations. The attack was detected in time, preventing any damage. In February 2023, the Italian company Acea, which provides electricity and water to Rome, was attacked by the Black Basta ransomware group, disrupting its online services. These recent attacks highlight a growing number of deliberate cyberattacks on energy systems, with increasingly severe impacts. Attackers have shifted their focus from individual power companies to large enterprises that supply multiple types of energy. Their methods now involve interrupting energy supplies and accessing the core business data of energy companies for extortion. Besides the Industroyer2 malware attack in Ukraine, other energy companies have faced significant consequences from malicious cyberattacks. The Industroyer2 attack in Ukraine underscores the need for a robust energy security defense system to counter escalating malicious cyberattacks, which is the main objective of this research.

Table 1. Attacks against energy systems in the last decade.

Year	Target of Attack	Attack Method	Result	Ref.
2015	Electricity Company of Ukraine	Blank Energy malware	A major power outage that lasted several hours	[7]
2020	Light S.A. Electricity Company, Brazil	Sodinokibi ransomware	Extortion of USD 14 million.	[10]
2020	EDP Energy, Portugal	Ragnar Locker ransomware	Extortion of USD 10.9 million	[11]
2021	Colonial Pipeline, USA	-	All pipelines stopped and some services shut down	[12]
2022	High voltage substations in Ukraine	Industroyer2 malware	Stopped before causing an actual accident	[13]
2023	Acea, Italy	Black Basta ransomware	Web service crash	[14]

3. Deliberate Attacks on IECPS

IECPS effectively enhances energy utilization through advanced communication technologies and energy management systems. However, its complex coupling characteristics render it highly vulnerable to deliberate attacks by malicious actors. On one hand, the system’s precise control depends on the efficient processing of data; however, extensive data exchanges increase the burden of data detection, enabling attackers to falsify, tamper with, or disrupt data transmissions, which may lead the system to issue erroneous scheduling commands. On the other hand, a minor fault in one system can be amplified through repeated propagation across multiple systems, potentially causing the collapse of the entire integrated energy system. As a result, the impact of system failures is significantly amplified.

Exploiting the aforementioned IECPS weaknesses, the attacker executes the invasion method depicted in Figure 2. In the physical layer, the attacker may employ aggressive tactics to damage critical energy infrastructure, including the destruction of energy stations, transmission pipelines, measurement devices, and other essential facilities. This can lead to both single-point and multi-point failures that can trigger a cascading chain of failures, fulfilling the attack’s objective. The communication layer is typically divided into the communication and control layers, based on their distinct functions. Attackers within the communication layer may block or destroy communication links, delay or prevent the transmission of operational data, and obstruct the issuance of control commands,

thereby accomplishing the desired attack objectives. In the control layer, attackers can implant malware to gain system privileges, modify operational data, and ultimately induce erroneous decisions within the system. In practice, attackers often coordinate both cyber and physical attacks when planning IECPS assaults, significantly enhancing the stealth and impact of the attack, thereby causing maximum damage to IECPS. Consequently, this section examines the attack patterns and modeling techniques of deliberate attacks on IECPS from three perspectives: cyberattacks, physical attacks, and CCPAs. By analyzing these attack patterns and models, this section can provide insights into formulating defense strategies against deliberate attacks.

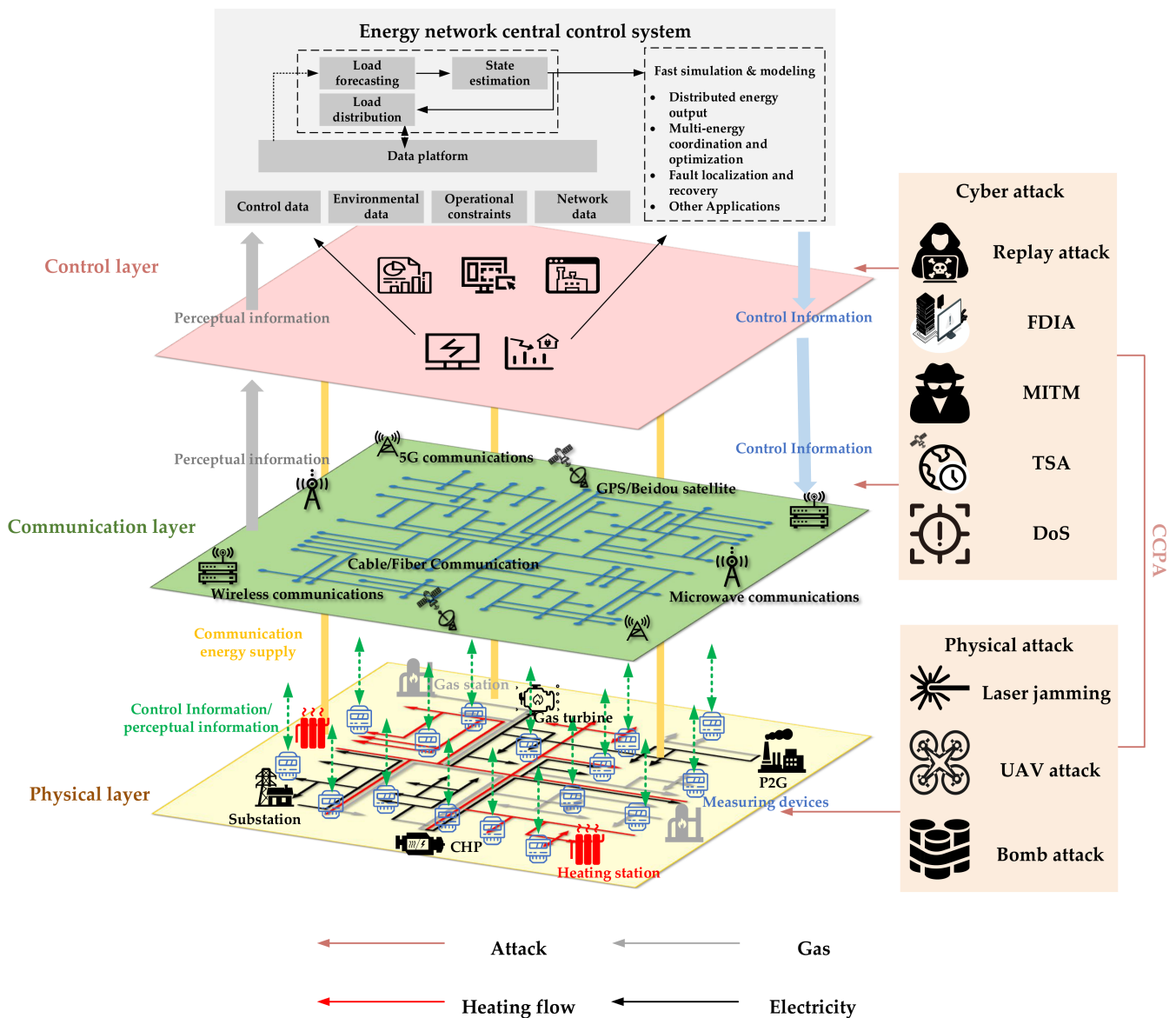


Figure 2. Typical IECPS attacks and intrusion locations.

3.1. Cyberattacks

The effective coordination of energy subsystems is intrinsically dependent on the precise control of the cyber system. Numerous sensors and monitoring devices on the physical side transmit system measurement, topology information, and environmental data via a communication network using technologies such as microwave, global positioning system (GPS), and power carrier waves. Upon receiving these data, the control center employs online simulation software to conduct real-time simulations of operational data

and system status, thereby enabling the formulation of appropriate scheduling plans. Once the scheduling plan is finalized, the corresponding operational instructions are transmitted to the control unit via the communication network, which then initiates the necessary adjustments to the system's state upon receiving these instructions. During this process, both the integrity and real-time nature of the data significantly influence the accuracy of control. Attackers compromise data integrity by rewriting, deleting, or adding data [15], and disrupt real-time data transmission by blocking or interrupting communication links [16]. These actions aim to interfere with the system's normal operation. Common forms of cyberattacks include replay attacks (RAs), man-in-the-middle (MITM) attacks, false data injection attacks (FDIAs), time synchronization attacks (TSAs), denial of service (DoS) attacks, and coordinated cyberattacks (CCAs).

3.1.1. Replay Attacks

RA is an attack against the data integrity of the system. The attacker records that the destination host has already received the information through illegal ways and sends the information repeatedly to achieve the purpose of deceiving the system [17]. In IECPS, attackers can illegally access system operation data, such as voltage, power, air pressure, and flow rate, through eavesdropping, interception, or packet capturing [18]. By repeatedly sending these data to the scheduling and control center, they prevent accurate assessment of the system's operational status. This hinders the formulation of effective scheduling strategies, ultimately compromising system stability. The attackers can also intercept the system's control commands, such as automatic generation control (AGC) frequency control signals [19], circuit breaker opening and closing commands [20], when the system is in normal operation, and constantly repeat the sending of control commands to cause erroneous actions of the system equipment, which affects the security of IECPS. Currently, some scholars are studying the detection techniques for RA, for example, by adding timestamps within the transmitted data or using more secure routing protocols [18,21].

Figure 3 illustrates the specific flow of the RA. Between time intervals t_r and t_{r+d} , the attacker intercepts system information without disrupting system operations. At time t_s , the attacker begins retransmitting the intercepted data to the target host, continuing until the conclusion of the attack. Thus, the RA can be represented as follows:

$$y(t) = y[t_r + (t - t_s) \bmod d], t \in [t_s, t_{s+(n+1)d}], \quad (1)$$

where n indicates the number of replays.

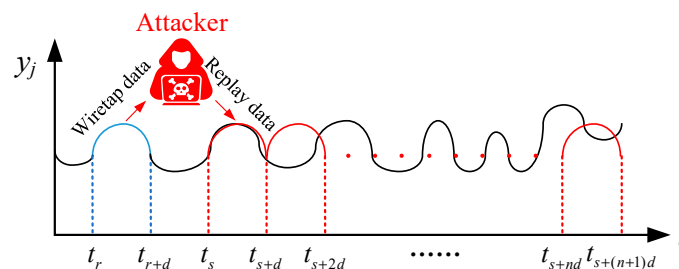


Figure 3. Schematic of the RA.

3.1.2. Man-in-the-Middle Attacks

MITM is an indirect attack method, and its attack principle is shown in Figure 4. The attacker exploits vulnerabilities in the communication protocol, employing techniques such as malware, domain name system spoofing, and address resolution protocol spoofing, to forge identities, impersonate legitimate nodes within the energy system, and establish

an illicit communication channel within the pre-existing communication network. At this stage, the attacker gains unauthorized access to the system's operational information, all while remaining undetected by the system. The attacker is capable of intercepting and injecting erroneous system data and control commands at will, thereby disrupting the normal operation of the energy system, upsetting the balance between supply and demand, and potentially causing damage on system components. In contrast to general data tampering, MITM attacks are more clandestine and challenging to detect, as they occur within the network communication link, with the attacker remaining concealed throughout the process.

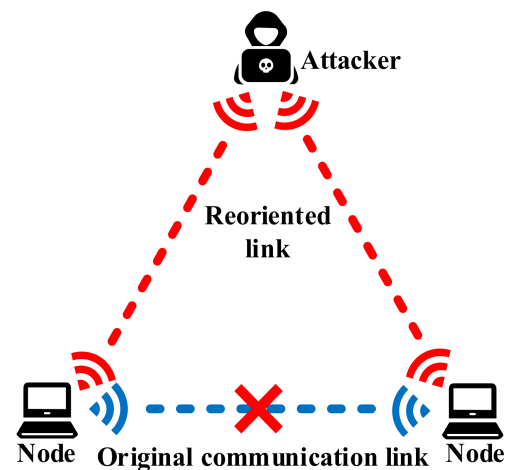


Figure 4. Schematic diagram of the MITM.

From the perspective of the attack process inherent in MITM attacks, the attacker injects erroneous data into the corresponding control unit. Once the control unit executes based on the faulty instruction, the attacker proceeds to intercept and modify the feedback operation data, thereby facilitating long-term stealth and undetected manipulation [22]. Consequently, the MITM attack can be mathematically modeled as follows:

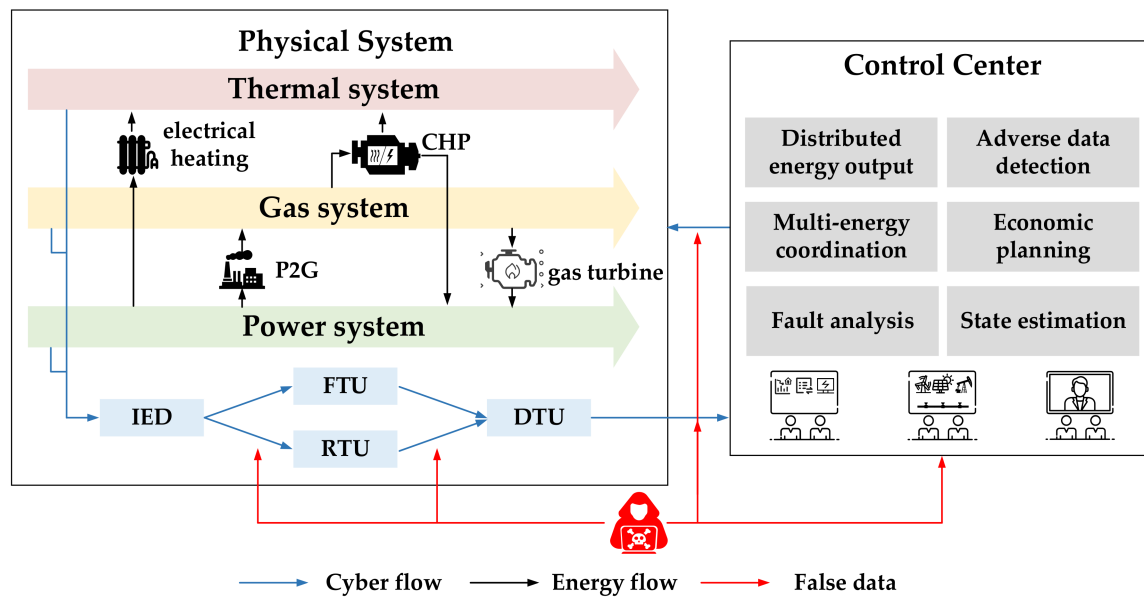
$$\tilde{u}_{da}(t) = u_{da}(t) + \gamma \quad (2)$$

$$\tilde{y}_{da}(t) = y_{da}(t) - \delta, \quad (3)$$

where $\tilde{u}_{da}(t)$ and $u_{da}(t)$ denote the control signals after and before tampering, respectively; $\tilde{y}_{da}(t)$ and $y_{da}(t)$ denote the operation data after and before tampering, respectively; γ is the modification amount of the control instruction; and δ is the modification amount of the operation data.

3.1.3. False Data Injection Attacks

FDIA is a new type of data attack, which is becoming increasingly harmful as energy systems and cyber systems become more and more coupled. The principle of FDIA is shown in Figure 5, in which the attacker carefully designs erroneous data that can bypass the undesirable data detection mechanism, and then replaces the erroneous data with the measurement data on the physical side or the estimation of the state of the control center to mislead the control center to make wrong decisions or cause wrong actions of the actuators on the physical side, thus leading to an unsafe operation of the system.



IED: IED stands for intelligent electronic device
 FTU: FTU stands for feeder terminal unit
 RTU: RTU stands for remote terminal unit
 DTU: DTU stands for data transfer unit

Figure 5. Diagram of FDIA mode of action.

With the continuous development of FDIA, FDIA can be roughly divided into general FDIA, load redistribution attack, and false topology attack. We conducted a literature survey based on the above three typical FDIAs and formed the FDIA cases for energy systems shown in Table 2.

Table 2. FDIA cases for energy systems.

Type	Target	Ref.
General FDIA	State estimator	[23]
	Energy market	[24]
	RTU	[25]
	AGC	[26–33]
Load redistribution attack	Power system	[34–36]
	Weather forecast system	[37,38]
	Integrated energy system	[39]
False topology attack	DC power flow model	[40–42]
	AC power flow model	[43,44]

• General FDIA model

The key to successfully launching a FDIA lies in bypassing the system's bad data detection mechanism. Most current research has identified the residual detection method as the detection method to be avoided in FDIA. Therefore, the attack vector a needs to satisfy the following constraints:

$$z + a = H(x + x_a) + e \quad (4)$$

$$r = z - h(\hat{x}) \quad (5)$$

$$\|r\|_2 \leq \varepsilon, \quad (6)$$

where z is the system measurement data; x and x_a are the state estimation bias caused by the system state quantity and false measurements, respectively; H is the matrix describing the relationship between the measurement value and the state quantity; e is the measurement error; r is the state estimation residual; $\hat{x}$ is the state estimation value; $h(\cdot)$ is the nonlinear function describing the relationship between the measurement value and the state quantity; and ε is the threshold value for residual detection. Constraints (6)–(8) are the basic conditions followed in constructing the FDIA, and in the actual construction of the FDIA model, it is necessary to determine the target data to be modified and the modification range of the target data, so as to establish a specific FDIA model.

- **Load redistribution attack model**

As a specific form of FDIA, the LR attack requires the attacker to circumvent both the state estimator and bad data detection mechanisms during its construction, thus necessitating the preservation of the system's total load [39].

$$\sum_{i=1}^{N_d} \Delta D_i = 0 \quad (7)$$

$$\Delta F_L = -S_F K_D \Delta D, \quad (8)$$

where ΔD_i is the load modification amount of load node i ; ΔF_L is the line current attack vector; S_F is the transfer factor matrix; K_D is the node–load association matrix; ΔD is the load modification vector; N_d is the number of load nodes.

To avoid injected false load data being detected by the scheduler, the amount of load modification should be set within a reasonable range:

$$-\zeta D \leq \Delta D \leq \zeta D, \quad (9)$$

where ζ is the range of modified quantities of the load; D is the vector of measured values of the load node.

Furthermore, the number of measurement devices under attack, including load and current measurement instruments, must be constrained:

$$\eta_{D,i} = \begin{cases} 0 & \Delta D_i = 0 \\ 1 & \Delta D_i \neq 0 \end{cases} \quad (10)$$

$$\eta_{FL,j} = \begin{cases} 0 & \Delta F_{L,j} = 0 \\ 1 & \Delta F_{L,j} \neq 0 \end{cases} \quad (11)$$

$$\sum_{i=1}^{N_d} \eta_{D,i} + 2 \sum_{j=1}^{N_l} \eta_{FL,j} \leq N_a^{\max}, \quad (12)$$

where $\eta_{D,i}$ is the 0–1 integer variable corresponding to the first load node; $\eta_{FL,j}$ is the amount of current modification on the first line; N_l is the number of lines; and $N_a^{\max}$ is the maximum number of attacks.

- **False topology attack model**

It is crucial to emphasize that, once the attacker manipulates the system topology, a false disconnection arises within the network. This manipulation leads to a discrepancy between the system topology information and the operational data. To evade detection by the system, the attacker must also alter the pipeline data. Taking the power system false topology attack as an example, the attack model actually comprises two parts: topology tampering and power tampering [43].

- (1) The topology tampering part involves an attacker trying to fake the disconnection of a transformer branch by tampering with the transformer protection action information, thereby disconnecting the circuit breakers at both ends:

$$\psi_{(0)}^T = 0 \Rightarrow \psi_{(1)}^T = 1 \rightarrow \begin{cases} \zeta_{(0)}^{CB,f} = 0 \Rightarrow \zeta_{(1)}^{CB,f} = 1 \\ \zeta_{(0)}^{CB,t} = 0 \Rightarrow \zeta_{(1)}^{CB,t} = 1 \end{cases}, \quad (13)$$

where $\psi_{(0)}^T$ and $\psi_{(1)}^T$, respectively, indicate the protection action state of the transformer branch before and after the attack; $\zeta_{(0)}^{CB,f}$ and $\zeta_{(1)}^{CB,f}$, respectively, indicate the state of the front-end circuit breaker of the transformer before and after the attack, with a value of 0 indicating that the circuit breaker is closed and a value of 1 indicating that the circuit breaker is open; $\zeta_{(0)}^{CB,t}$ and $\zeta_{(1)}^{CB,t}$, respectively, indicate the state of the back-end circuit breaker of the transformer before and after the attack, with a value of 0 indicating that the circuit breaker is closed and a value of 1 indicating that the circuit breaker is open.

In contrast to transformer protection, when an attacker simulates a transmission line fault, it is necessary to alter the information of two distinct protection devices. These two sets of devices control the state of two separate circuit breakers:

$$\begin{cases} \psi_{(0)}^{L,f} = 0 \Rightarrow \psi_{(1)}^{L,f} = 1 \rightarrow \zeta_{(0)}^{CB,f} = 0 \Rightarrow \zeta_{(1)}^{CB,f} = 1 \\ \psi_{(0)}^{L,t} = 0 \Rightarrow \psi_{(1)}^{L,t} = 1 \rightarrow \zeta_{(0)}^{CB,t} = 0 \Rightarrow \zeta_{(1)}^{CB,t} = 1 \end{cases}, \quad (14)$$

where $\psi_{(0)}^{L,f}$ and $\psi_{(1)}^{L,t}$ denote the operational states of the protective devices at each end of the transmission line, while $\zeta_{(0)}^{CB,f}$ and $\zeta_{(1)}^{CB,t}$ represent the states of the corresponding circuit breakers at the respective locations.

When all branch circuits connected to a bus need to be disconnected by an attacker, the action information of the bus protection needs to be tampered with, thus changing the breaker state:

$$\psi_{(0)}^B = 0 \Rightarrow \psi_{(1)}^B = 1 \rightarrow \begin{cases} \zeta_{(0)}^{CB,1} = 0 \Rightarrow \zeta_{(1)}^{CB,1} = 1 \\ \zeta_{(0)}^{CB,2} = 0 \Rightarrow \zeta_{(1)}^{CB,2} = 1 \\ \dots\dots\dots \\ \zeta_{(0)}^{CB,n} = 0 \Rightarrow \zeta_{(1)}^{CB,n} = 1 \end{cases}, \quad (15)$$

where $\psi_{(0)}^B$ is the state of the busbar protection device.

- (2) In the power tampering part, the attack vectors need to be designed to ensure the data matching, i.e., the attack vectors need to be made to ensure that the power remains balanced before and after the attack:

$$\Delta P_l = -S_{(0)}^{PF,l} K_{(0)}^{PD,l} D_{(0)}^{P,l}, \forall l \in C \quad (16)$$

$$\Delta P_l = -S_{(1)}^{PF,l} K_{(1)}^{PD,l} D_{(1)}^{P,l} + S_{(0)}^{PF,l} K_{(0)}^{PD,l} D_{(0)}^{P,l}, \forall l \in L - C, \quad (17)$$

where ΔP_l is the false data of injected branch volume measurement; $S_{(0)/(1)}^{PF,l}$ is the transfer factor matrix of the lines before and after the attack; $K_{(0)/(1)}^{PD,l}$ is the node-load correlation matrix of the lines before and after the attack; $D_{(0)/(1)}^{P,l}$ is the node power measurement matrix of the lines before and after the attack; C is the set of lines to be attacked; and L is the set of system lines.

3.1.4. Time Synchronization Attacks

With the promotion of integrated energy systems, a large number of distributed energy systems will appear in the future. Scheduling these distributed energy systems requires

ensuring that the clock signals of the distributed systems remain synchronized, which relies on the accuracy of the time scale signals from GPS/Beidou satellites and the correctness of the system clock synchronization protocol. However, the time synchronization devices of some energy systems are synchronized using civilian GPS clock signals that lack encryption mechanisms, which gives attackers an opportunity to forge clock signals. As shown in Figure 6, an attacker transmits a forged GPS clock signal in the vicinity of an attack target, and the attack target's time synchronization device has its internal time changed after receiving the forged GPS signal. The measurement device controlled by this synchronization device will sample the data at the wrong time, resulting in time misalignment in the measurement data transmitted to the control center. Currently, most of the processing schemes only consider the measurement errors caused by noise and packet loss, allowing TSA to easily bypass the system's protection mechanisms [45]. Furthermore, the deliberate attacker does not intrude or make physical contact with the time synchronization device, so this type of attack is difficult to localize.

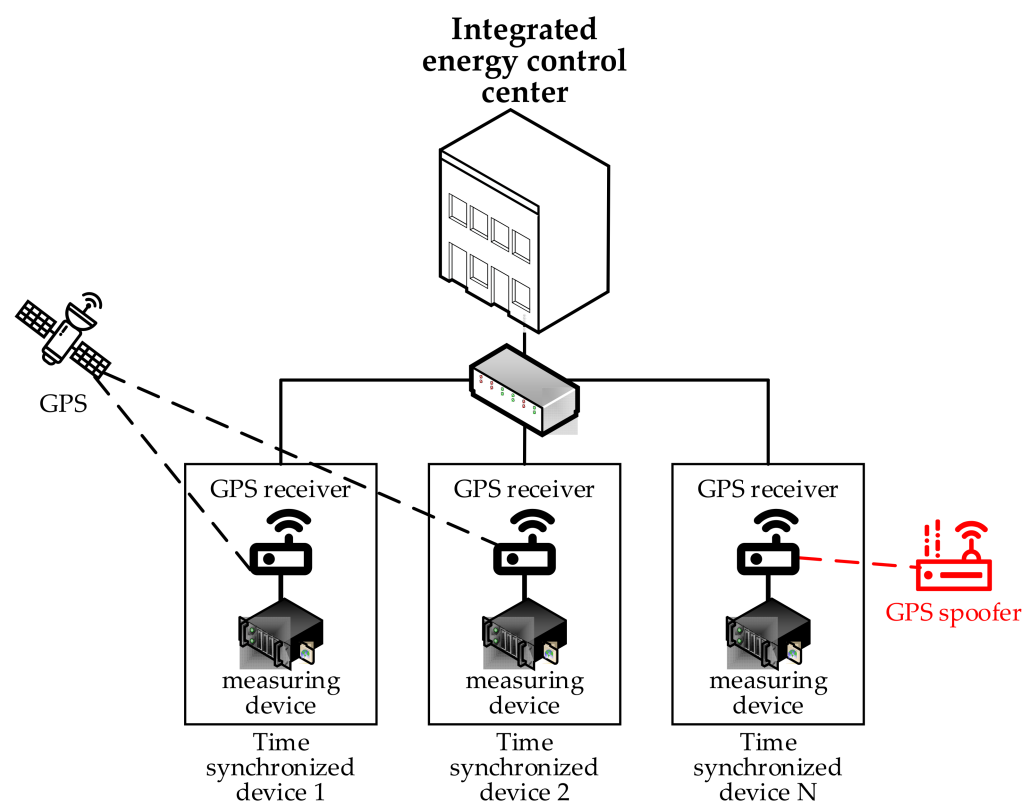


Figure 6. Schematic of the TSA.

Although time synchronization attacks are not easy to detect, this does not mean that the clock signals can be modified at will. Literature [46] states that if an attacker blindly attacks the PMU, it may be detected by bad data algorithms. Therefore, when designing the TSA, it is necessary to know how much measurement deviation is caused by modifications of the clock signal. For a signal with a frequency of f Hz, assuming that the time when it is not attacked is t and the time after the attack becomes $\tilde{t}$, the resulting phase angle deviation is

$$\sigma = f \times (\tilde{t} - t) \times 360^\circ, \quad (18)$$

where σ is the phase angle estimation error.

Once the phase angle deviation is determined, the induced measurement deviation can be expressed as

$$\pi_\theta = z_0(e^{j\sigma} - 1), \quad (19)$$

where π_θ is the measurement deviation; z_0 is the original measured phase.

3.1.5. DoS Attacks

DoS attack is a form of network-based assault that renders a service unavailable to legitimate users by overwhelming the target computer, network, or service with excessive resource demands [47]. Figure 7 illustrates a simple DoS attack based on the ping command, which causes a buffer overflow on the target host by sending packets exceeding the maximum allowed size, which in turn triggers the target host to crash or reboot. Based on this DoS attack, in [48], researchers focused on analyzing its impact on the load frequency control system and constructed a DoS attack model that blocks the transmission of packets to the data center. In [49], the possibility of launching DoS attacks on multiple AC regions within a multi-terminal high voltage direct current system is investigated, and a DoS attack scheme for frequency restoration and power allocation is proposed. In [50], the authors expanded their perspective to integrated energy systems, qualitatively analyzing the impact of DoS attacks on the economic scheduling of integrated energy systems, and proposed a DoS attack scheme comprising an optimal attack sequence and attack nodes. Furthermore, to enhance the economic damage capability of the attack, an FDIA is also launched on the measurement equipment and communication links. In [51], the authors provide a comprehensive introduction to various attack methods, including DoS attacks, and modeling approaches targeting load frequency control systems.

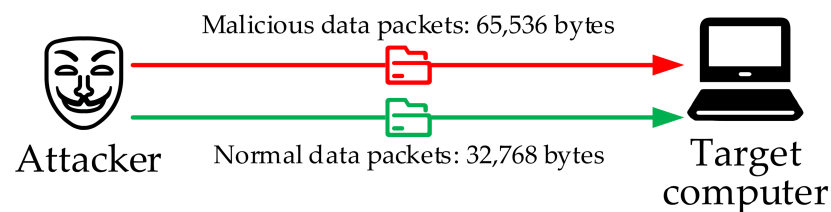


Figure 7. Diagram of Ping of Death attack.

Distribution denial of service (DDoS) attack is a more stealthy attack compared to DoS attack. The attacker obtains the control of the hosts distributed in different locations, and then collaborates to control these hosts to send a large number of requests to the server. This leads to traffic congestion, causing the server to lose the ability to interact with the normal equipment. In [52], it is illustrated how vulnerabilities in wide-area measurement systems can be exploited to launch DDoS attacks against distributed generators. In [53,54], the authors hindered the energy transfer between the grid and electric vehicles (EVs) by launching a DDoS attack on an EV charging pile. In [55], a non-zero-sum game-theoretic model considering DDoS attacks is designed to study the resource allocation between attackers and defenders. In [56], while investigating cyberattacks in the electric vehicle sector, the authors specifically highlight the impact of DDoS attacks on electric vehicles.

Currently, most research focuses on simulating the behavior of DoS attacks rather than directly establishing mathematical models for them. If DoS attacks are treated as data traffic, for example, assuming that the attack traffic exhibits bursty traffic, this traffic can be regarded as an impulse function:

$$R(t) = \begin{cases} s & \text{if } t \in [t_0, t_0 + \mu] \\ 0 & \text{otherwise} \end{cases}, \quad (20)$$

where $R(t)$ is the number of requests of DoS attack traffic at the time; s is the attack strength; t_0 and μ are the attack start time and duration, respectively.

If the attack is described as a loss of packets, the attack can be represented using state equations for discrete systems [47]:

$$x_{k+1} = Ax_k + Bu_k + \omega_k \quad (21)$$

$$M_k = \{\lambda_1 x_1, \lambda_2 x_2, \dots, \lambda_k x_k\}, \quad (22)$$

where x_k is the k momentary state quantity; u_k is the k momentary control signal; ω_k is the error term; M_k is the monitoring dataset; and λ_k indicates whether the monitoring system collects system measurements or not, and if the value is 0, it means that the DoS attack has caused packet loss.

3.1.6. Coordinated Cyberattacks

Such CCAs exhibit high flexibility and complexity, which poses significant challenges for defenders to adapt to evolving threats and design effective countermeasures [57]. Table 3 shows some of the retrieved CCA. In [58], a synergistic attack model combining FDIA and delay attacks was proposed for the AGC system, aiming to disrupt its normal frequency control functions. In [59,60], tampering with operational data on the gas and power sides, respectively, causes a reduction in gas turbine output, which subsequently leads to a loss of load in the power system. In [61], the authors proposed a destructive electro–thermal coordinated attack that exposes the potential information risks in electro–thermal integrated energy systems by jointly altering the load data of both power and thermal systems. In [62], a novel attack scheme for power systems based on FDIA and DoS attacks was presented. This scheme leads to tripping by tampering with the synergistic line topology and then uses a DoS attack to prevent the system from scheduling and ultimately leads to a large-scale system failure. With the development of artificial intelligence methods, some scholars have used AI algorithms to construct information cooperative attacks. In [63], deep reinforcement learning-based software intrusion attack and FDIA attack models were constructed, using the deviation of regional control errors in AGC systems as a reward function. In [64], a deep neural network was used to combine a time synchronization attack and a DoS attack, targeting the distributed secondary control device of microgrid. In addition, in [65,66], information collaboration attacks were constructed using attack graphs and heuristic algorithms, respectively.

Table 3. CCA Cases.

Attack Targets	Modeling Methods	Cyberattack							Ref.
		RA	MITM	FDIA	TSA	DoS	Time Delay Attack	Soft Intrusion	
AGC	Optimization model			✓			✓		[58]
Integrated power and gas system				✓					[59]
Integrated power and gas system				✓					[60]
Integrated heat and electric system				✓					[61]
Power system				✓		✓			[62]
AGC	Deep reinforcement learning			✓				✓	[63]
Microgrid	Deep neural network				✓	✓			[64]
Power system	Attack graph model	✓		✓					[65]
Power system	Heuristic algorithm		✓	✓					[66]

The CCA above illustrates that attackers can combine various types of cyberattacks to suit their objectives. By targeting different system levels or operational stages, they can exploit the weaknesses of individual attack types, increase their success rate, and amplify the destructive impact. Therefore, it is necessary to strengthen the attention to CCA to deal with complex network threats.

3.2. Physical Attacks

The foundation of IECPS is the physical system, and the safe and stable transmission of all energy depends on the integrity of physical equipment. Therefore, physical facilities are a prime target for attackers. In IECPS, attackers gather information on the infrastructure and critical equipment of the integrated energy system. They identify targets such as substations, natural gas stations, and transmission pipeline communication equipment, then deploy graphite bombs, drone strikes, and laser jamming to damage physical assets [67]. Graphite bombs disrupt power systems by dispersing highly conductive graphite fibers that attach to power infrastructure, resulting in short circuits or insulation breakdowns, which can lead to catastrophic equipment failures and widespread power outages [68]. Beyond graphite bombs, other types of explosive devices, including drones equipped with bombs, can be deployed to target energy systems, enabling precise strikes on critical infrastructure [69]. Laser jamming refers to an attack technique that utilizes high-energy lasers to disrupt and damage sensitive measurement components within energy systems, potentially resulting in inefficient operation and significant economic losses. In addition to the aforementioned methods, some unscrupulous individuals engage in power theft by tapping into wires, resulting in non-technical losses to the operator [70].

Since physical attacks often result in infrastructure damage, attack modeling often assumes that the attack results in a functional defect or complete loss of the target facility. Consequently, physical attacks can be modeled according to the following equation:

$$(1 - \tau b_q)F_q, q \in I_P, \quad (23)$$

where τ is a factor between 0 and 1 characterizing the degree of impact of the attack on the device's functionality; b_q is an attack variable that takes the value of 1 if the device q suffers from an attack, and 0 otherwise; F_q characterizes the specific functionality of the device q ; and I_P is the set of physical devices of IECPS.

During an attack, the attacker's resources are constrained due to limitations in their attack capabilities, preventing them from damaging the entire energy system:

$$\sum_{q \in I_P} b_q \leq N_a^{\max}. \quad (24)$$

3.3. Coordinated Cyber–Physical Attacks

Security is a major concern in the management of energy systems, and with the further improvement of energy system operation and management systems and the significant enhancement of system protection devices, security incidents caused by physical defects are becoming increasingly rare. The possibility of attacks relying solely on large-scale destruction of physical facilities is decreasing. Considering the close coupling of the cyber network and physical network of the integrated energy system, launching a coordinated attack from both the physical and cyber sides can achieve greater attack benefits. On the one hand, the attacker can expand the attack scope and enhance its effect through physical attacks by utilizing the cyber–physical coupling mechanism; on the other hand, the attacker can tamper with the system operation data through cyberattacks, thereby concealing the physical attacks and causing persistent system failures.

Figure 8 illustrates a typical IECPS coordinated attack process. The attacker uses FDIA and DoS attacks on the cyber side to compromise data integrity and disrupt cyber system availability, while employing brute force damage on the physical side to destroy physical components, such as system pipelines and measurement instruments. The cooperation between these two types of attacks ultimately leads the control center to make incorrect decisions, resulting in a larger system failure. The process of the attack is actually composed

of two different types of attacks. The process actually contains two different synergistic approaches, i.e., physical attack prioritization and cyberattack prioritization.

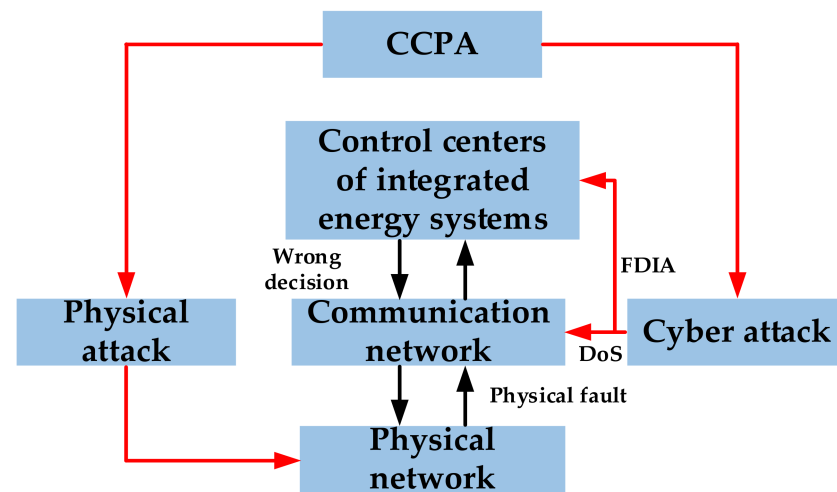


Figure 8. Process of CCPA.

3.3.1. A Coordinated Strategy for Prioritizing Physical Attacks

Physical attack priority refers to the strategy where the attacker first causes system failure by damaging the physical line. Subsequently, the attacker masks the failure by injecting false data or delaying the upload of the failure information to the control center via a DoS attack. This creates a time lag, allowing the attacker to further exacerbate the system failure and compromise its safe, stable operation. In [71], following the destruction of the system line, the disconnection is concealed by falsifying the node power and line current readings of the measurement unit. This leads to a false overload event, misleading the dispatch system to make erroneous decisions. In [72], FDIA is utilized to mask the system disconnection, and then a DoS attack is utilized to reduce the use of attack resources, effectively reducing the difficulty of the attack. In addition to physical disconnection, in [73], the feasibility of covert attacks on compensating reactors is investigated, and the attack setup methods under the attacker has complete and incomplete information are given.

3.3.2. A Coordinated Strategy for Prioritizing Cyberattacks

Prioritization of cyberattacks is the opposite of prioritization of physical attacks, where the attacker first launches a cyberattack, for example, by preventing the control center from receiving operational data, and then launches a physical attack. When the system communication is cut off, the attacker can carry out physical damage at will without any countermeasures if allowed. In the coordinated approach prioritizing cyberattacks, cyberattacks are mostly dominated by LR attacks [57]. In [74], the attacker initially employs LR attacks to alter the system load data. Upon successful execution of the LR attack, a physical attack is swiftly carried out, with subsequent LR attacks used to continuously obscure the ongoing attacks on the line. In [75], a coordinated attack method against generators is proposed, where the attacker first employs an LR attack to change the load demand of the system, and then conducts a physical attack to cause the generator to trip, but this attack is not covert.

From the attack mode and model analysis of the above attacks, it can be seen that cyberattacks primarily induce erroneous system scheduling decisions or impair system functionality. Meanwhile, physical attacks collaborate with cyberattacks to amplify the attack's impact. However, most of the above studies are based on more idealized assumptions, and most of them focus on power systems. Consequently, the countermeasure

strategies proposed in these research results may not effectively defend against real IECPS coordinated attacks. Therefore, it is necessary to more fully consider the characteristics of IECPS and establish more sophisticated defense mechanisms to resist the threat of deliberate attacks.

4. Defense Strategies Against Deliberate Attacks on IECPS

From the attack mode and development trend of deliberate attacks, it can be seen that the deliberate attacks against integrated energy systems have become more covert and diversified, the risk of deliberate attacks on the system is rising, and it is difficult for the existing security system to cope with the increasingly complex threats of deliberate attacks. In order to resist the threat of deliberate attacks, scholars have conducted in-depth research on the defense of deliberate attacks from system planning, attack detection, multi-energy scheduling and other aspects. However, most of these studies are carried out for a specific attack event, and due to the lack of refining and summarizing of these studies, there is no defense system for diversified deliberate attacks. In order to improve the system's ability to cope with diversified deliberate attacks, this section, following a synthesis of existing research findings, describes the IECPS defense strategy against deliberate attacks in three stages, i.e., preemptive prevention, process response, and post-event recovery and summarizing, in accordance with the process of deliberate attack evolution. Figure 9 illustrates the specific defense strategies for each of the three stages.

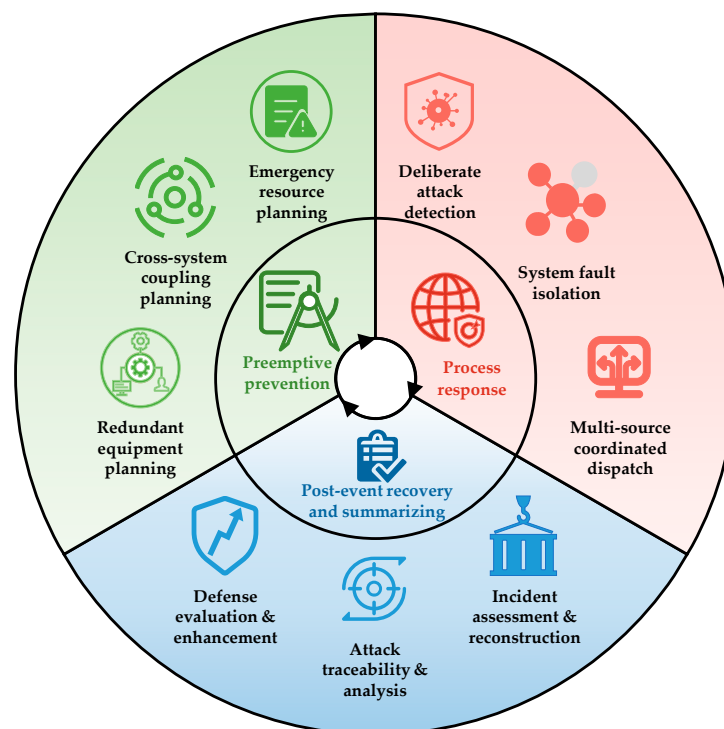


Figure 9. Deliberate attack defense strategy for IECPS.

4.1. Preemptive Prevention

In response to the numerous potential deliberate attacks, IECPS must first fortify its resilience against perturbations. Incorporating the effects of deliberate attacks into the early-stage planning of IECPS is crucial for enhancing the system's responsiveness to attack-induced perturbations [76]. Failing to consider the impacts of deliberate attacks before they occur may lead to a more costly response through emergency dispatch in the event of such an attack [77]. This section focuses on analyzing the existing research results

from a planning perspective and proposing a preemptive strategy to deal with deliberate attacks.

4.1.1. Redundant Equipment Planning

When a deliberate attack occurs and some functions of IECPS are destroyed, the system's first priority is to repair the damaged functions. In order to ensure that the restoration is carried out with precision, a comprehensive assessment of the damage caused by the attack needs to be carried out to identify which system physical facilities and cyber components need to be rebuilt. Immediately after the completion of the restoration of system functions, it is necessary to carry out an investigation of the attack on the invasion method, in-depth analysis of the system vulnerabilities exploited by the attacker, and through this analysis as a breakthrough to further explore other potential vulnerabilities in the system. Finally, it is necessary to conduct a comprehensive evaluation of the defense measures, identify the weak links in the defense process, and take corresponding improvement measures to optimize and enhance the overall defense capability of the system.

For IECPS, the configuration of device redundancy is a critical strategy to bolster its defense capabilities against deliberate attacks, representing a foundational approach in system design. Redundancy encompasses two interpretations: the first refers to unnecessary or superfluous components, while the second involves the deliberate duplication of critical parts. In this context, redundancy in equipment planning pertains to the latter interpretation. In energy systems, to ensure security and reliability, the deliberate duplication of key components or functions can significantly mitigate the risks associated with equipment compromise and minimize system losses following deliberate attacks. Redundant equipment planning can be classified into two categories based on the role of the redundant components: the energy equipment level and the cyber system level.

At the level of energy devices, in [78], the effect of parallel connection of multiple devices to improve the safety of an integrated energy system is theoretically analyzed. In [79], the impact of a multi-energy microgrid system failure is reduced by configuring additional microturbines and solar cells. In [80], researchers proposed a redundancy planning method for combined cooling heating and power equipment based on the probabilistic analysis using a Markov model, which resulted in a significant reduction in the interruption rate of energy supply when the system suffers a fault. In addition to the redundant configuration of energy supply equipment mentioned above, the planning of energy storage devices is also an important means to improve the reliability of energy supply. In [81], the load loss of the system under extreme events is effectively reduced by rational allocation of the capacity and power of the energy storage system. In [82], a planning method for mobile energy storage in distribution networks is proposed to utilize the mobility and flexibility of mobile energy storage to improve the power supply reliability of distribution systems. In [83], the optimization method of mobile energy storage capacity under multiple line failure scenarios is further explored and the power loss status of the system is substantially improved.

At the cyber level, the main protection against deliberate attacks is through the configuration of redundant measurement devices. Redundant configurations of measurement devices can, to a certain extent, maintain the data integrity of state estimation, thus resisting to reduce the risk of deliberate attacks. In [84], the relationship between the level of measurement redundancy and the risk of FDIA is revealed through criticality analysis, and graph theoretic metrics are proposed to analyze the vulnerability of the measurement system. In [85], in order to solve the problem of insufficient state estimation measurements in distribution networks, a data processing method is designed to handle the phase measurement data and advanced metering system data of distribution networks, which

increases the redundancy level of distribution network measurements and improves the ability of state estimation to resist FDIA. In [86], the weaknesses of the distribution system are analyzed, and synchronized phase measurement units are arranged at vulnerable nodes to improve the ability of the system to recognize network attacks. In addition, in order to prevent all kinds of attacks intruding from the communication link, in [87], a redundant gateway planning method is proposed, and artificial noise signals are also added to mitigate the impact of information attacks during system operation. In [88], a blockchain-based multi-control architecture is proposed to improve the likelihood of detecting and recognizing deliberate attacks through redundant controllers. In [89], a defense method for deploying time-slotted channel hopping devices is proposed for time synchronization attacks, where time-slotted channel hopping is utilized to establish a trust model to ensure high-precision synchronization of all communication nodes.

Although redundant equipment planning can enhance the system's ability to detect and resist deliberate attacks, it inevitably leads to an increase in the initial investment cost. This increase is a non-negligible factor for small-scale integrated energy systems, on par with system security. Therefore, balancing investment costs and security performance is the focus of the study of redundant equipment planning for small-scale IECPS. In [90], an optimization model for determining the number and location of PMUs is developed based on the network-wide observability of the power system, which is achieved by using as few PMU devices as possible. In [91], the authors proposed a two-stage robust optimization model for energy storage allocation to study the optimal investment strategy for energy storage with consideration of economics. In [92], the researchers analyzed the methods and effects of redundancy planning for integrated energy systems using the k-out-of-n model, and concluded that a win-win situation for both economy and resilience can be achieved within a certain redundancy level. Therefore, through rational redundancy design based on the consideration of risk aversion benefits, it can bring a greater return than the initial investment cost.

4.1.2. Cross-System Coupling Planning

With the advancement of the low-carbon transition of the global energy system, fuel vehicles are gradually replaced by EVs, and a large number of EVs are connected to the power grid through charging piles, resulting in a coupling relationship between the transportation system represented by EVs and the power system. Furthermore, the ongoing digital transformation, this coupling relationship between energy and transportation is being strengthened. On the one hand, the planning and configuration of the energy system influences the access location of new loads, such as EVs, through the layout of charging piles; on the other hand, the time-sharing tariff mechanism of the energy system can influence the access time of new loads. This spatio-temporal characteristic makes EVs have strong randomness after accessing the power grid, and this randomness is both a challenge and an opportunity for the control of the energy system. In terms of challenges, the random access of EVs to the grid may increase the system load pressure and exacerbate the peak-to-valley difference, and it has been demonstrated that attackers can take advantage of this weakness to launch attacks on the grid [93]. In terms of opportunities, if the cyber system is used as a link to improve the interaction between the transportation system and the energy system, cross-system integration and coordination can be achieved, which in turn can enhance the resistance of the energy system to deliberate attacks [77].

Figure 10 presents the schematic diagram of the coupling planning between IECPS and the transportation system. IECPS provide energy support for the transportation system, and the transportation system provides flexibility resources for the optimal operation of the energy system and contingency protection in case of emergency. When not intentionally

attacked, the cyber system guides EVs to charge in an orderly manner by integrating transportation information, reducing the local load pressure of the system and improving the robustness of the energy system. In the event of a deliberate attack causing interruption of energy supply, mobile power generation vehicles can be dispatched to support the power grid and gas network, ensuring that energy supply is restored as swiftly as possible. When the attack causes communication interruption, emergency communication vehicles or low-altitude aircraft are used for communication networking to restore data interaction between the control center and the faulty area. By integrating the resources of both the energy system and transportation system, the ability of IECPS to respond to deliberate attacks can be significantly enhanced.

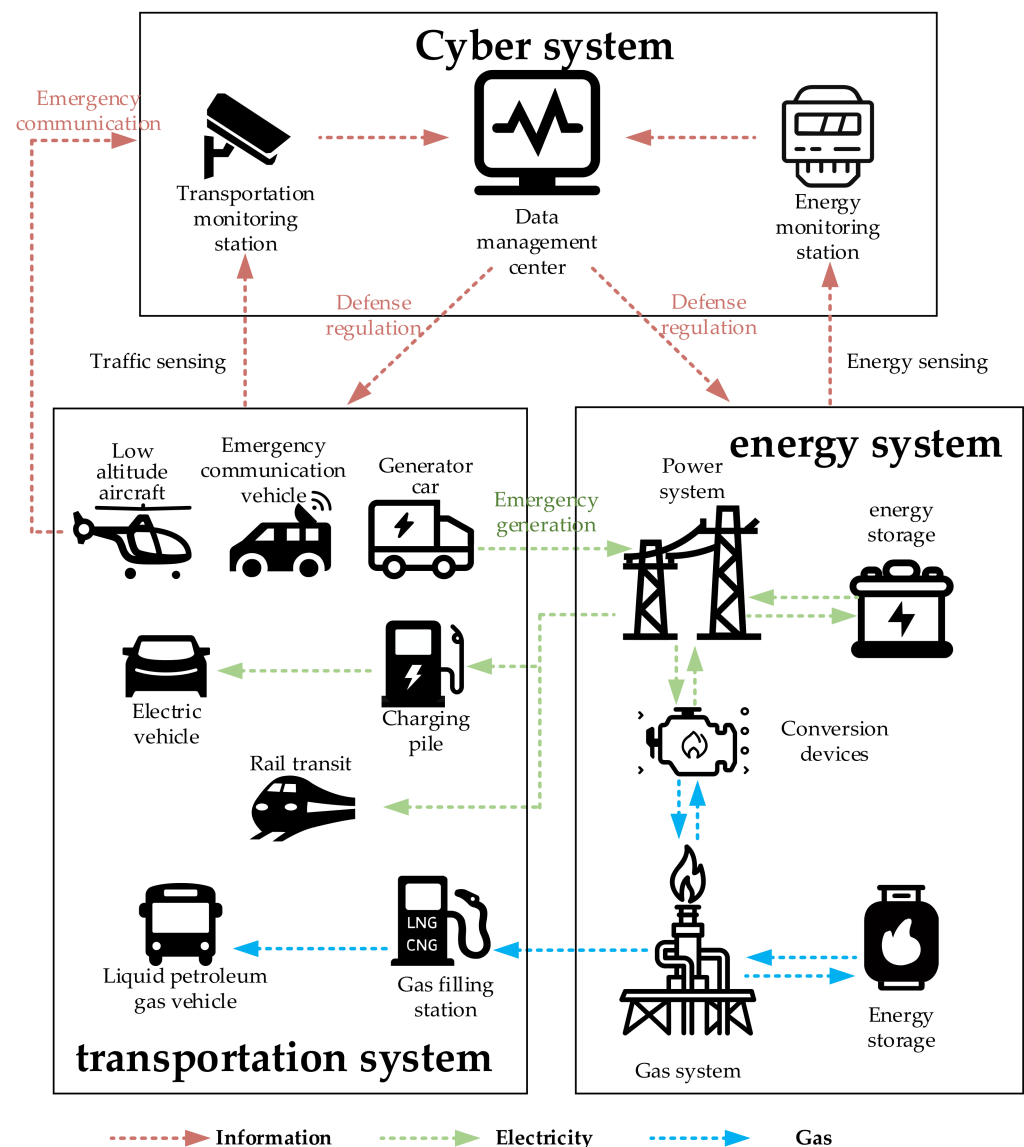


Figure 10. Schematic diagram of IECPS and transportation coupling planning.

In recent years, researchers have increasingly focused on developing strategies to bolster the defense capabilities of IECPS against deliberate attacks, particularly through the integration of energy and transportation systems. In [94], the integration of the transportation system into energy management not only decreases energy consumption costs but also establishes a robust and precise energy planning framework underpinned by a reliable decentralized structure, thereby ensuring effective safeguarding of interactions between the energy and transportation systems against deliberate attacks. In [95], the pivotal role of

energy transportation in improving the economic efficiency and defense resilience of the power system is highlighted, with a series of uncertainty sets being introduced to model system losses under extreme attacks. Furthermore, a coordinated planning approach for both the power system and the energy transportation network is proposed, which takes into account the potential impacts of such extreme events. In [96], several provisions across energy, transportation, and information sectors are integrated to incorporate low-carbon distributed power sources and electrified transportation into a unified digital platform for energy emergency management, thereby coordinating diverse resources to enhance the resilience of the integrated energy system against extreme events.

4.1.3. Emergency Defense Resource Planning

Given the challenges associated with executing large-scale physical attacks, some attackers may proactively initiate deliberate assaults during extreme disaster events to disrupt the normal course of rescue and relief operations. When confronted with the imminent threat of an extreme disaster, heightened attention must be given to the possibility of deliberate attacks. Studies have shown that during natural disasters, the risk of an integrated energy system collapse increases significantly when attackers execute deliberate human-based assaults [97].

Figure 11 illustrates the pre-event emergency defense resource planning framework, which is composed of three parts: system perception, risk warning, and emergency resource allocation. First, emergency resource planning is based on accurate system perception, which requires strengthening the control center's ability to collect and process various key information of the system. In [98], a multi-state model is formulated to accurately capture the power output of wind turbines by analyzing the comprehensive uncertainty of wind speed, which greatly improves the situational awareness of the wind power system. A multi-failure coordination strategy incorporating transportation information was introduced in [99] to use real-time information about transportation for system optimization. In [100], the wind speed, rainfall rate, and ice load at the transmission line were calculated based on a weather model, and the relationship between the ice load and the line failure rate was obtained by curve fitting. However, for complex heterogeneous system like IECPS, which contains multi-energy flow characteristics [101], the above power system-oriented perception methods cannot meet the interaction needs of various subsystems due to the strong coupling of various types of sensing data.

Secondly, it is imperative to enhance the system's risk assessment and early warning capabilities. Timely detection and early warning of extreme disasters provide the dispatch center with sufficient lead time to deploy emergency resources, thereby significantly reducing potential system losses. In [102], a multi-indicator approach for predicting landslides is proposed, enabling accurate forecasting of landslide occurrences. In [103], an early warning system for various geohazards is developed, utilizing a high-performance water-sensitive bio-ion battery to provide timely alerts regarding soil seepage. In [104], from the perspective of multivariate information fusion, distribution network uncertainties, and other contributing factors are synthesized, leading to the development of a distribution network disaster resilience index system and a predictive model, thereby enhancing the early warning capabilities for distribution network disasters. In [105], the impact of typhoon-induced rainstorms on the failure probability of electrical equipment is analyzed, and a spatio-temporal early warning methodology for natural disasters is proposed, capable of predicting the spatio-temporal evolution of these disasters and performing quantitative analysis on the failure rates of transmission line components.

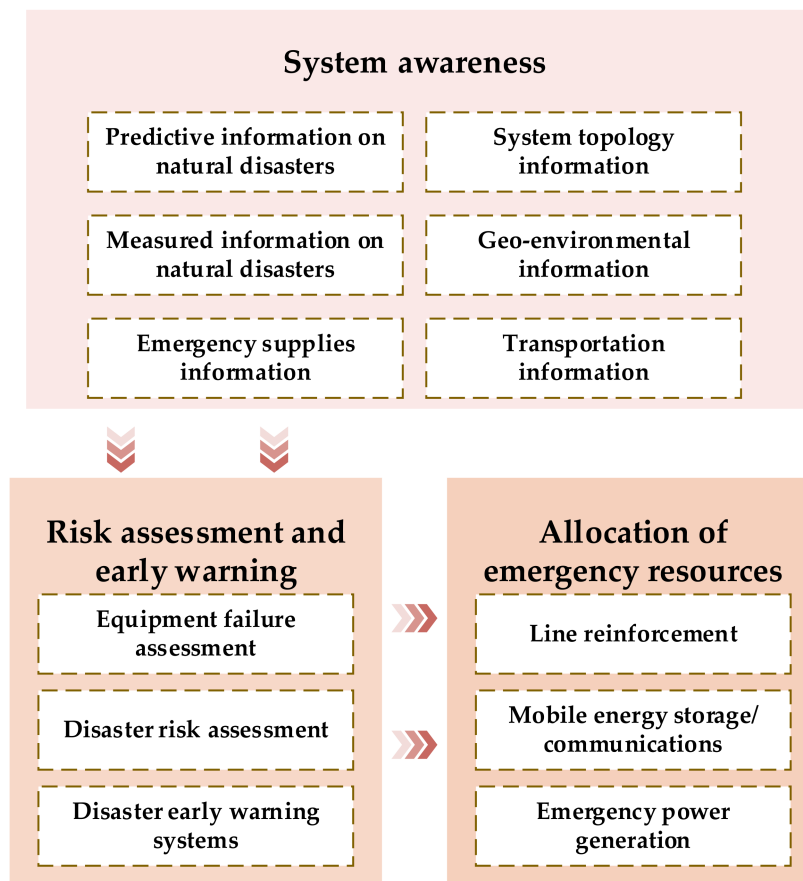


Figure 11. Framework of pre-event emergency defense resource planning.

Finally, emergency defense resources are deployed in advance through a scientific and reasonable emergency resource allocation strategy. In [106], it is proposed to deploy mobile energy storage in advance at key grid locations, enabling rapid power supply to the microgrid after a fault, thereby preventing serious consequences due to power shortage. In [107], an ex-ante optimization model incorporating mobile energy storage, liquefied gas storage, and pipelines/lines is proposed with the objective of minimizing load losses. In [108], a pre-disaster cooperative scheduling strategy that takes into account line reinforcement, fixed/mobile generators, and mobile gas storage tanks in concert is proposed for an integrated electric–gas energy system. In addition, studies have been conducted to improve the system’s resilience to extreme events by clearing vegetation on both sides of the line, using snow and ice resistant conductors, and increasing the line inspection program before the disaster arrives.

4.2. Process Response

When an attacker initiates a deliberate attack on IECPS, the system’s defense mechanism responds in accordance with the stealth and intensity of the attack, effectively countering attackers with varying levels of attack capabilities. For attackers with limited capabilities, the deliberate attack detection mechanism promptly identifies the attack before it causes any significant impact, thereby preventing the attacker from inflicting damage on the system. In cases where attackers bypass the deliberate attack detection but fail to cause substantial damage, the fault induced by the attack is initially contained by the system’s fault isolation mechanism, preventing its propagation across domains and halting further escalation. Subsequently, the complementary support capabilities of IECPS are leveraged

for multi-source cooperative scheduling, mitigating the effects of deliberate attacks and enabling rapid recovery within a short timeframe.

4.2.1. Deliberate Attack Detection

Because of its important position in social production activities, IECPS have become one of the main targets for lawbreakers to damage and seize benefits, and various kinds of targeted attacks are emerging [109]. In the process of continuous confrontation with deliberate attacks, researchers and scholars have proposed a variety of attack detection methods, and the deliberate attack detection mechanism has made great progress. As shown in Figure 12, IECPS deliberate attack detection methods can be classified into state estimation-based detection methods, statistical model-based detection methods, and data-driven detection methods.

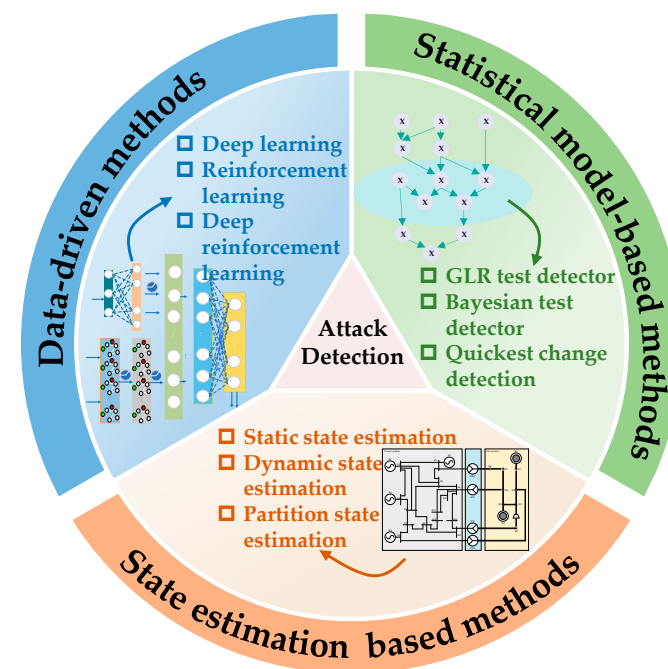


Figure 12. Deliberate attack detection methods.

- **State estimation-based detection methods**

Bad data detection (BDD) is widely used in various commercial energy management system software because of its ability to detect erroneous measurements due to equipment failures, communication interruptions, and other factors during system operation [110]. Its principle is realized by determining whether the residual difference between the state estimation result and the measurement result satisfies a threshold value. To prevent false detection, the residual threshold is set with a certain criterion, which is used by deliberate attackers to construct false data that satisfy the residual test, thus easily bypassing this line of defense and causing damage to the system. Faced with this situation, some studies have suggested lowering the threshold of BDD to enable FDIA detection. In [111], considering that lowering the threshold may result in false detection proposed a partitioned detection approach, which improves the possibility of attack detection by decomposing the system into multiple subsystems and lowering the BDD threshold for each subsystem separately.

Partition-based detection methods can enhance the probability of FDIA detection but still do not address the shortcomings of the BBD principle. This is mainly due to the fact that traditional detection methods use steady-state estimators and lack real-time information about the system. To address this issue, scholars employ dynamic state

estimation to improve the detection probability of attacks. Dynamic state estimation mainly uses kalman filter (KF) and its variants. The variants of KF include extended KF, untraceable KF, adaptive KF, integrated KF, and particle filters designed for nonlinear systems [112]. In [113], a Euclidean distance detector is used to detect the difference between the result of the KF estimation and the measured value to determine whether the system is subjected to FDIA or not. The proposed method achieves better detection accuracy than the traditional BDD; however, it possesses two limitations. First, although it applies a dynamic estimation method, it only considers time-invariant states and ignores the dynamic nature of state variables. In addition, the proposed detector cannot lack the capability to differentiate between FDIAs and faults caused by physical issues. To tackle this challenge, some scholars introduced dynamic state estimation into the BDD detection mechanism, which utilizes the principle that the state quantities of the dynamic state estimation deviate from the steady state estimation of the state quantities more after false data injection. The specific flow is shown in Figure 13. Based on this principle, in [114], the FDIA detection method for extended KF is designed. In [115], the detection method of adaptive KF is designed to realize the attack detection of vehicle–network data. Literature [116] combines the untraceable KF with extreme gradient boosting to achieve the detection of FDIA, and corrects the data tampered by FDIA through the central limit theorem. Considering the problem of less quantitative measurements in distribution networks, which is difficult to meet the demand of state estimation, in [117], a pseudo-quantity side load model is established for state estimation, and then it is combined with adaptive untraceable KF for FDIA detection, and the results show that this method has a higher detection capability compared to the traditional detection methods.

Although introducing KF into BDD can improve the detection rate of FDIA, this approach still has drawbacks. On the one hand, the accuracy of attack detection relies on the accuracy of KF prediction, which may lead to false positives; on the other hand, the attacker has sufficient time to learn about the system and constructs false data to satisfy the threshold after obtaining the threshold setting of the system. These problems can be attributed to the static characteristics of traditional cyber systems [110]. To address this shortcoming, researchers have attempted to make it impossible for attack vectors to bypass detection mechanisms, such as BDD, by altering the system parameters required for attackers to construct attack vectors. Based on this, the moving target defense (MTD) attack detection methodology is proposed.

The principle of MTD is to actively change the transmission line parameters by controlling the distributed flexible AC transmission system devices deployed on the transmission line. This invalidates the parameter information used by the attacker to construct the attack vectors, making them more easily recognizable by FDIA detection algorithms. In [118], the authors derive the feasibility of MTD in FDIA detection and provide a completeness analysis for implementing MTD. In [119], the authors change the transmission line parameters without affecting the normal operation of the system, significantly reducing the likelihood of false detections. Although MTD is able to improve the detection probability of the attack, it increases the system loss because it changes the system parameters. Therefore, in [120,121], planning and operational methods to reduce the cost of implementing MTD within the system are explored from an economic perspective.

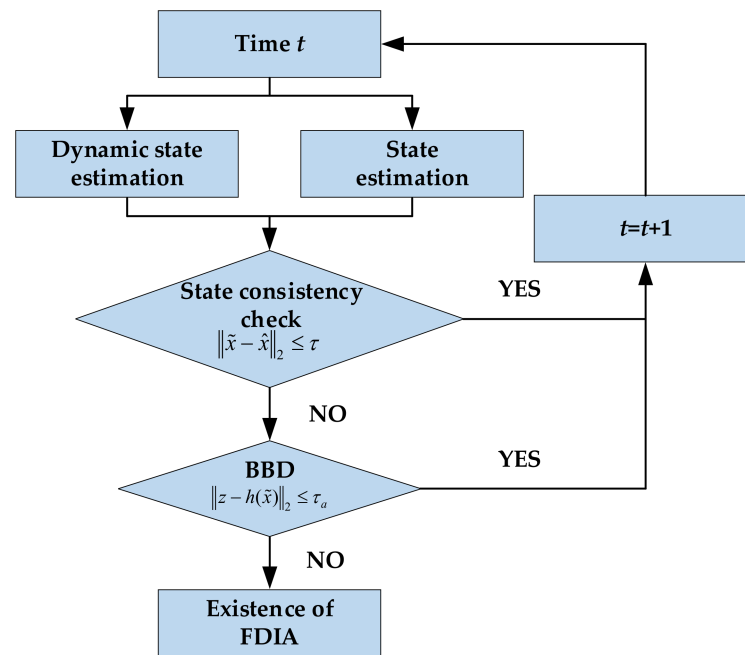


Figure 13. Detection flow based on dynamic state estimation.

• Statistical model-based detection methods

In addition to utilizing state estimation models for detecting deliberate attacks, statistical models can also be employed to identify such attacks effectively. Currently, several widely adopted detection models include the generalized likelihood ratio (GLR) detection model, the Bayesian test model, and the quickest change detection (QCD), among others.

The GLR detection model is used to detect cyberattacks in power systems through statistical likelihood ratios. It is generally used for weak FDIA detection because it cannot detect a large number of compromised samples [110]. In [122], based on the GLR model, it is proposed to use the l_1 paradigm to realize the attack detection, and it is pointed out that with the increase in detection samples, the GLR model has a better detection effect for the same FDIA. Literature [123] combines GLR model with the square root traceless KF and achieves the detection of general imperfect FDIAs by testing the sequential dynamic event regularization distance obtained from the square root traceless KF. From the above description, it is evident that this detection method has significant limitations. Additionally, literature [124] specifies that this detection method does not work properly when the system measurements are corrupted by non-Gaussian noise distributions.

The Bayesian test model-based detection method focuses on identifying a priori information and deriving probabilities using Bayesian theory, once the probability of the FDIA vectors has been determined through Bayesian inference, it is able to derive Bayesian based recursive predictions using system measurements and predictions to perform attack detection. In literature [125], the authors designed Bayesian detectors for each monitoring node to enable attack detection in distributed systems. In literature [126], an attacker-defender Bayesian game-theoretic detection model for FDIA attacks is developed to determine protection choices for critical measurements. In [127], a Bayesian model-based anomalous data traffic detection mechanism is presented, which distinguishes between DoS attacks in wireless sensor networks and high traffic generated by legitimate user communications.

QCD is a method for rapid detection of sudden changes by minimizing the delay between the occurrence of the change and its monitoring through sequential or real-time observations. In [128], multiple meters are used to measure different output signals of a PV system, and the time correlation of fault signals and the signal correlation between different

meters are utilized to achieve fast fault detection. A PMU phase angle measurement acquisition method based on line interruption transient dynamics algorithm was developed in [129], which is able to quickly acquire real-time PMU measurements and speed up the identification of line interruptions. Since QCD is a dynamic detection framework, it is often used together with cumulative sum test (CUSUM), dynamic state estimation, and Bayesian modeling. In [130], the use of the CUSUM algorithm is proposed for detecting spurious data injected into energy management systems. In [131], the adaptive level-triggered sampling technique is applied on this basis to achieve more accurate detection; however, the method is unable to detect covert FDIA attacks. In [132], a dynamic estimation algorithm is proposed to estimate and track time-varying and non-stationary grid states, and a QCD algorithm for distinguishing between FDIA and sudden system changes is developed by analyzing the statistical properties of dynamic state estimation. This involves identifying the parameters of the detector and quantifying the performance of the detection model based on the Markov chain model.

- **Data-driven detection methods**

With the development of AI, various machine learning methods have been widely applied to detect deliberate attacks, both offline and online [133]. Among them, supervised learning classifiers are the most popular attack detection technique, which utilizes historical data to train a model to reflect the operational state and statistical characteristics of the energy system [110]. With sufficient historical data training, the method produces better models, leading to more accurate detection results. In [134], three algorithms, K-nearest neighbor, support vector machine, and sparse logistic regression, are used for attack classification. A supervised learning attack detection framework is established to address the issue of sparse measurement matrices in the state estimation method. In [135], a two-layer neural network architecture based on sequence decomposition reconstruction is proposed, combining decision trees with long and short-term memory neural networks. This architecture can accurately identify and remove attack data from PMU data. In [136], deep learning techniques are used to learn the FDIA attack behavior patterns in historical measurement data. The difference in patterns between identifying damaged data subjected to FDIA and normal data serves as the basis for classification. However, this method cannot cope with scenarios in which the topology undergoes drastic changes over a short period. In [137], more protocol features are extracted by wavelet decomposition of protocol messages. These extracted features are then learned by deep neural networks, which mines the attack behaviors from two aspects: temporal features and spatial features. The recognition ability of highly stealthy false data injection attacks is superior to that of traditional deep learning methods.

Although the aforementioned methods exhibit high detection accuracy, they necessitate a large number of training datasets, which are often challenging to acquire, particularly complete attack data in practical operations. In [138], to address the issue of imbalance among normal, faulty, and attack datasets, an extreme gradient-enhanced classifier based on integrated learning is employed to improve dataset balance. Beyond overcoming the imbalance of training samples in AI-based detection of deliberate attacks, considerations regarding real-time detection and attack localization are also essential [139]. In [140], a Bayesian-based approximation filter is utilized to minimize communication overhead and time complexity, thereby enhancing both real-time performance and immunity against cyberattack detection in surveillance systems. In [141], a detection method based on attention-deep reinforcement learning is proposed for intrusion identification defense, with deliberate data attacks localized using an enhanced graph convolutional network algorithm.

Considering the high dependence of supervised learning on prior knowledge, the researchers tried to introduce semi-supervised learning into system attack detection. Figure 14 illustrates the distinction between supervised and semi-supervised learning detection algorithms, highlighting that the training set for semi-supervised learning detection algorithms comprises both labeled and unlabeled datasets. A semi-supervised anomaly detection model was built in [142] and the results proved that semi-supervised methods have better detection performance. In [143], semi-supervised K-means clustering is utilized to learn different attack patterns and achieve the recognition of multiple attack types. However, the method relies heavily on the label quality of the original training samples. To solve this problem, in [144], a semi-supervised deep learning method is used to train a small number of labeled samples and a large number of unlabeled samples to achieve accurate detection of deliberate attacks.

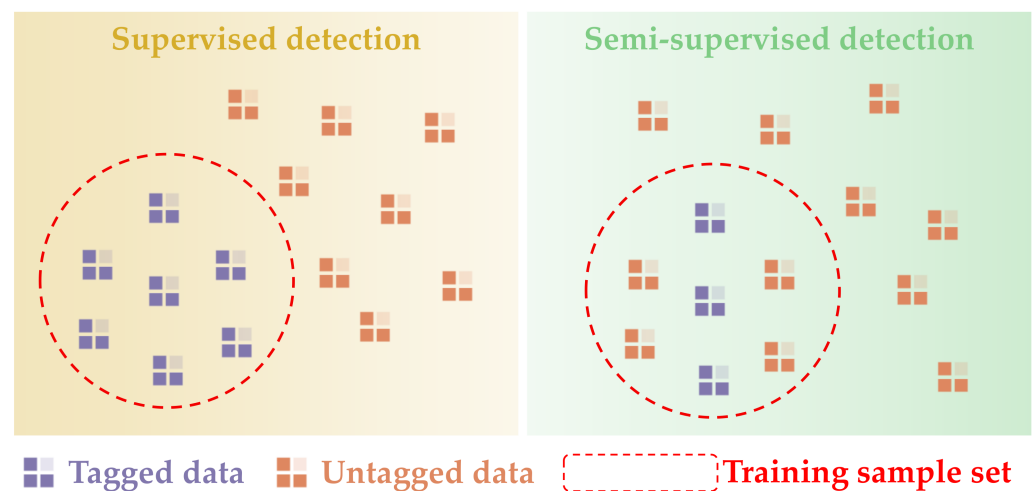


Figure 14. Difference between supervised and semi-supervised learning detection methods.

Although semi-supervised learning can achieve attack detection with fewer samples of attack data, it is still not free from the limitation of labels. The obtained model has limited generalization ability and may struggle to adapt to the dynamic changes in the system. Unsupervised learning is able to learn the relationship between the operational data autonomously and can remove the labeling limitation. In [145], system parameters and topology are used as validation information, and a fuzzy C-mean clustering algorithm is used to realize unsupervised detection of attack messages. This method maintains high accuracy under topology changes. In [146], an adversarial migration learning framework is used to establish the mapping relationship between system parameters and messages, and unsupervised learning of attacks is realized by referring to system parameters and topology data. Although the above studies performed unsupervised learning of attack features, they need to utilize system parameters and topology data for assistance. In [147], using local outlier factor analysis technique, an unsupervised detection method without the need for system parameters and topology data is proposed to achieve accurate detection of FDIA.

4.2.2. System Fault Isolation

Despite extensive research on deliberate attack detection methods, these approaches may still exhibit limitations when addressing complex and diverse deliberate attacks, potentially disrupting the system's normal operation and leading to system losses. If the impact of deliberate attacks is minimal, faults induced by the attacks can be swiftly rectified through emergency system adjustments. It is important to note that although the impact of deliberate attacks may be minimal, this does not imply that the damage caused by the attack will not escalate. If a deliberate attack is not adequately addressed during the emergency

regulation phase, its impact may be amplified through the coupling of energy subsystems, as well as between cyber systems and physical systems [148]. Therefore, emergency regulation in IECPS should prioritize fault isolation and block the fault propagation path to prevent further escalation. In [149], the effects of grid fault currents and the voltage characteristics of protective devices under pre-fault, during fault, and post-fault conditions are examined, and a fault isolation method based on line and bus voltage measurements is proposed. In [150], real-time switch state data are employed to reflect dynamic changes in power system topology, and the Floyd–Warshall algorithm is used to trace the paths of circuit breaker disconnections for each electrical component, thereby formulating a fault isolation set. While the aforementioned method can effectively isolate system faults, it fails to account for tampering by deliberate attacks, which may inadvertently facilitate the attacker in achieving their objectives. In consideration of the impact of deliberate attacks on information transmission between measuring elements, the control center, and actuating elements, literature [151] achieves decentralized fault isolation by mapping the relationship table of protection devices, enabling accurate and swift isolation of faulty distribution system segments without reliance on a central controller. In [152], a novel fault isolation scheme based on active converter control is proposed, where a trapezoidal wave is injected into the converter to identify the faulted line by counting the high-level pulses of the trapezoidal current. Isolation is then performed using a corresponding DC switch during the low-level pulses. This scheme operates using DC switches without the need for communication, effectively mitigating the risk of deliberate tampering by attackers.

Currently, research and engineering applications concerning fault location, treatment, and isolation in single power systems have matured [153]. However, fault isolation technologies for IECPS are still in their infancy. Since a single fault in integrated energy systems can trigger abnormal operation in other subsystems, isolating faults in each subsystem individually is not feasible; instead, a holistic approach is necessary. Researchers are currently endeavoring to establish an effective fault management framework for fault isolation in complex multi-energy coupled systems. In [154], a building-wide fault diagnosis method based on discrete Bayesian networks was proposed, aimed at accurately identifying and isolating major cross-system faults during operation. In [155], building upon this foundation, a weather- and schedule-based pattern-matching Bayesian network was further designed to diagnose and isolate cross-system faults in integrated building energy systems. To further improve the accuracy of fault diagnosis and isolation, literature [156] combined model-based and Bayesian network-based methods, achieving a 45.7% increase in fault isolation accuracy through the complementary strengths of both approaches.

Although the aforementioned methods offer high accuracy in fault diagnosis and isolation, the Bayesian network-based isolation approach significantly depends on domain expert knowledge, which limits its scalability. To facing this challenge, researchers have adopted data-driven methods for fault diagnosis and isolation. In [157], a data mining technique was developed to aggregate and cluster system information, providing algorithmic support for system fault diagnosis by extracting energy efficiency data from integrated energy systems. In [158], a gradient boosting regression algorithm was used to predict the operational states of coupled components in integrated energy systems, enabling fault identification and localization. In [159], nine types of faults and three sub-faults in integrated energy systems were analyzed, and a two-level fault isolation scheme was developed using convolutional neural networks, consisting of a high-level classifier for system faults and a low-level classifier for sub-faults, achieving accurate isolation of predetermined faults. In [160], an entropy-based causal learning framework was proposed to learn Bayesian network structures. This framework identifies causal relationships between fault states and fault manifestations, thereby establishing a Bayesian network model that includes

multiple cross-system fault outcomes. It is evident that data-driven approaches do not require domain expert knowledge, thereby facilitating model development and expansion easier, and enabling the handling of more unknown system faults. Therefore, they are more suitable for addressing unknown deliberate attacks.

4.2.3. Multi-Source Coordinated Dispatch

After fault isolation, the primary task is to rapidly restore the system's energy supply. In traditional single-energy systems, operators are limited to dispatching emergency resources within the system, with repair speed hindered by the availability of these resources, resulting in prolonged recovery times. Despite some studies have introduced energy storage [161–163] and emergency generators [164–166] to provide backup support for critical loads, the mitigation of system losses remains limited. Other studies have considered introducing renewable energy sources during faults to supply power and reduce load loss during fault recovery [167]. However, this method is characterized by significant uncertainty, as its effectiveness is greatly impacted by weather conditions. In [168], active load shedding was employed to mitigate the risk of larger-scale energy supply disruptions during extreme events. Due to the uncertainty of fault severity and the cost limitations of emergency resource allocation, it is not feasible to configure backup equipment at every node of the system. Consequently, the aforementioned mitigation strategies exhibit limited effect in addressing faults in single-energy systems.

In integrated energy systems, operators have comprehensive control over different energy subsystems and can support load supply to faulty systems by coordinating the scheduling of these subsystems. In [169], the authors analyzed a case where the natural gas system supported the economic and secure operation of the power system, highlighting that the flexibility of natural gas infrastructure can effectively address intermittent power shortages in the electricity grid. In [170], the authors coordinated and optimized the output of gas turbines and P2G devices to mitigate safety violations in integrated energy systems caused by wind power forecast errors in real-time. In [171], the authors further explored how coordinating the scheduling of electrical, gas, and thermal subsystems could mitigate the impact of extreme disasters, such as earthquakes, hurricanes, and floods, ensuring high-quality energy supply restoration. During the coordination of subsystems, power imbalance risks may arise, at which point selective load shedding or transfer can be implemented. In [148], the authors mentioned initiating ice storage systems to release cold energy by melting ice, thereby substituting electrical refrigeration and mitigating the power imbalance. In [172], the authors discussed reducing a range of non-critical loads and increasing the utilization of electrical and thermal energy storage to ensure that energy demands of critical loads can still be met during extreme events. In addition to load shedding and transfer, energy balance within subsystems can also be achieved through network reconfiguration and partitioning. In [173,174], network reconfiguration was performed for electric–thermal and gas–electric integrated energy systems, respectively, to ensure power supply in non-fault areas. In [175], the authors actively disconnected loads with islanding capabilities and performed energy coordination within these loads to form energy-balanced islanded integrated energy microgrids.

With the continuous development of integrated energy systems, the scope of multi-source coordinated scheduling is no longer limited to the coordination of energy flows, such as natural gas, thermal energy, and electricity, but has also expanded to the transportation system. In [176], researchers used the Delphi method to survey members of the U.S. Department of Energy's Electricity Advisory Committee, pointing out that vehicle–grid integration can significantly enhance the resilience of energy systems. Additionally, the study conducted a detailed analysis of the potential roles of three integration modes:

grid-to-vehicle (G2V), vehicle-to-grid (V2G), and vehicle-to-building (V2B). Among these, G2V and V2G play important roles in frequency regulation of the grid during extreme events, while V2G and V2B can offer backup energy supply to integrated energy systems, thereby reducing the economic losses caused by power grid interruptions. In [177], the authors analyzed the post-disaster recovery process of the transportation–energy coupled system and found that damage to the transportation network severely impacts the recovery of system load. In [178], the authors considered integrating integrated energy systems and transportation systems to prevent deliberate attacks, utilizing the social participation of EV users to alter vehicle usage patterns and supporting the energy system through V2G. In [179], the authors alleviated system losses caused by communication disruptions by dispatching emergency communication vehicles to support the networking of cyber systems. In addition to the above-mentioned ground transportation systems, unmanned aerial vehicles and helicopters can also be used to support IECPS in counteracting deliberate attack threats. In recent years, the flourishing development of the low-altitude economy has provided a foundation for this approach. The rapid recovery from deliberate attacks using low-altitude aircraft is foreseeable.

4.3. Post-Event Recovery and Summarizing

After a deliberate attack occurs, some functions of IECPS are damaged, and the primary task of the system is to repair the compromised functions. To ensure precise implementation of the repair work, a comprehensive assessment of the damage caused by the attack is required to identify which physical infrastructure and information components need to be rebuilt. Once the system functions are restored, the next step is to investigate the method of the attack, deeply analyze the system vulnerabilities exploited by the attacker, and utilize this analysis as a breakthrough to further uncover other potential vulnerabilities within the system. Finally, a comprehensive evaluation of the defense measures is required to identify any weaknesses in the defense process and to implement corresponding improvements, thereby optimizing and enhancing the overall defense capability of the system.

4.3.1. Incident Assessment and Reconstruction

Unlike the recovery and reconstruction of single systems, the recovery and reconstruction of IECPS is characterized by significant complexity and multidimensionality. This complexity arises from the coupling of multiple energy subsystems and the high degree of interaction and dependency between cyber and physical systems within IECPS. Specifically, the recovery and reconstruction efforts must not only assess the damage to various energy subsystems, such as electricity, thermal, and natural gas, but also consider the interdependencies between these systems. For example, a fault in the power system may trigger a chain reaction in the thermal system, while a disruption in natural gas supply may further affect the normal operation of power generation equipment. Furthermore, forcibly restoring the load of a heavily impacted system may result in more severe load shedding in coupled systems, and focusing solely on the repair of one subsystem is often insufficient to meet the comprehensive recovery requirements of IECPS. In addition to the coupling of physical systems, IECPS also integrates physical systems with cyber systems. Cyber systems play a key role in energy flow, equipment scheduling, and system monitoring and are prime targets for deliberate attacks. Consequently, cyber systems may also be damaged following a failure. As a result, the recovery efforts must comprehensively consider the damage to both physical coupling and cyber–physical coupling.

Under this background, a detailed assessment of IECPS following a deliberate attack is crucial. The assessment of physical coupling focuses on the integrity of energy flow and the functionality of equipment, while the evaluation of cyber–physical coupling emphasizes

the reliability of information transmission, the effectiveness of control signals, and the coherence of system operations. Through detailed post-disaster assessment, a comprehensive understanding of the specific damage to the system, including equipment failures, network disruptions, and abnormal energy flows, can provide precise guidance for the recovery and reconstruction efforts. This not only helps in formulating targeted repair strategies but also improves resource allocation efficiency, ensures clear prioritization of reconstruction efforts, and ultimately achieves the rapid and comprehensive recovery of IECPS.

Although researchers have recognized the importance of the cyber–physical coupling relationship in post-disaster reconstruction, related studies remain relatively scarce and predominantly concentrate on post-event recovery in power systems. In [180], the interaction recovery between cyber systems and physical systems was initially studied. A model for cyber–physical coordinated recovery was developed by analyzing the impact of cyber systems on generator output adjustment, power line instability, and recovery delays. The study results indicate that neglecting the constraints imposed by cyber systems on physical system recovery may lead to operational discoordination and even cause secondary black-outs. However, this approach only explored the constraints of cyber systems on physical system recovery and did not consider in depth the impact of physical system faults on cyber system recovery. To address this limitation, Ref. [181] further incorporates the dual failures of both cyber and physical systems into the research scope. By examining the interactions between maintenance scheduling, cyber system operations, and power system operations, it establishes a collaborative restoration model for the transmission system. This approach significantly enhances the coordination and reliability of the restoration process. Meanwhile, in [182], the research scope was expanded to not only focus on the interactive coordination of cyber and physical systems but also include the uncertainty of new energy output in the recovery process framework. The research results provide new solutions for extreme event recovery in power systems with high proportions of renewable energy integration. Additionally, in [183], the authors studied the full lifecycle of extreme events. They systematically constructed a cyber–physical coordinated model throughout the entire process from fault diagnosis to system recovery and proposed a sequential multi-stage coordinated recovery strategy for power cyber–physical systems, further advancing the reconstruction efforts of cyber–physical systems after extreme events. In summary, although existing research has made progress in cyber–physical coordinated recovery, there is still a lack of diverse research perspectives. There is an urgent need to study cyber–physical coordinated recovery strategies for IECPS.

4.3.2. Attack Traceability and Analysis

After a deliberate attack occurs, regardless of whether it causes damage to the system, attack traceability should be immediately initiated. Traceability analysis is a key step in uncovering the nature and mechanisms of an attack event. By analyzing system logs, communication traffic, and system operational states in detail, it is possible to identify the attacker's intrusion path, attack method, and the system vulnerabilities exploited. A comprehensive analysis of the entire attack event provides a scientific basis for the formulation of subsequent defense strategies.

Following the conduct of attack traceability, prompt optimization and upgrading of the system's security measures, based on the analysis results, is imperative. Firstly, the intrusion detection system should be updated by enhancing its rule base and behavioral analysis models, thereby enabling the identification of similar attack patterns and the issuance of early warnings. Secondly, the antivirus database should be supplemented, utilizing the latest malware signature libraries, thereby enhancing the system's capability to detect viruses and Trojans employed in the attack. At the same time, the security policy database

should be upgraded to strengthen system access control policies, improve data encryption mechanisms, and optimize network partition configurations, thereby minimizing potential attack paths. Forensic analysis, as a method for post-event collection and analysis of threat information related to cyberattacks, is widely applied in the fields of the internet, power systems, and IECPS security. It includes three steps: intrusion/attack evidence collection, threat information analysis, and evidence presentation. In [184], the role of deep packet inspection in malware detection, packet capture, and analysis was studied in depth, and a conceptual framework for deliberate attack data analysis and forensic analysis was proposed. In [185], data analysis of network traffic logs was performed to identify digital forensic traces, thereby studying the impact of FDIA on advanced metering infrastructure. Subsequently, a testing platform for advanced metering infrastructure was then designed and developed, with the aim of generating FDIA logs. In [186], considering that noise generated during system operation might interfere with forensic results, the recorded results were demodulated to accurately understand the specifics of the tampering.

4.3.3. Defense Evaluation and Enhancement

Enhancing the defense capability of IECPS against deliberate attacks is crucial to protect the system from threats and maintain its safe and stable operation. Scientifically and rationally evaluating the effectiveness of defensive strategies against deliberate attack events is the foundation for enhancing defense capabilities. Following each defense against a deliberate attack, it is essential to analyze the weaknesses in the current defense system and the effectiveness of the defense strategies, providing guidance for optimizing the defense system. Specifically, defense evaluation typically combines both static and dynamic methods, dividing the process into static analysis and dynamic assessment. Static analysis mainly focuses on reviewing aspects, such as system architecture, access control policies, communication protocols, and device configurations, analyzing the strengths and weaknesses of the defense system from a configuration and planning perspective. Literature [187] analyzes the framework of the entire energy system based on the System of Systems approach. It establishes multidimensional evaluation metrics to capture future changes in the system architecture, providing theoretical support for the updating of defense systems. In [188], based on trust evaluation of security management nodes, a data-driven method was used to establish a security analysis model for communication protocols, providing an effective solution for analyzing the security of communication protocols. In [189], various configuration schemes within the integrated energy system were evaluated in detail, and the economic aspects of the configurations were also analyzed.

Dynamic evaluation mainly assesses the system's response to deliberate attacks, including load loss evaluation, the degree of protection for information integrity, among others. By analyzing the resistance capability of specific events, the vulnerabilities and issues of the existing defense system are intuitively revealed. After completing the defense evaluation, corresponding improvement measures are formulated for the existing defense system's issues, including but not limited to improving the accuracy of attack detection and localization, enhancing the targeting of redundant equipment configurations, and improving the coordination of cyber–physical restoration. Additionally, considering the uncertainty of deliberate attacks, periodic attack–defense exercises can be conducted to broaden the scope of dynamic evaluation objects. In conclusion, through continuous evaluation and improvement of the defense system against deliberate attacks, a dynamic defense system for IECPS is formed, ensuring that it possesses sufficient resistance capabilities to maintain the security and stability of energy supply in the face of real deliberate attacks.

5. Key Technologies Supporting Deliberate Attack Defense for IECPS

The deliberate attack defense system of IECPS is a critical safeguard for ensuring the safe and stable operation of IECPS and promoting its high-quality development. The construction of the comprehensive defense system against deliberate attacks heavily relies on key technological breakthroughs in areas such as theoretical foundations, system planning, operation scheduling, cyber security and defense evaluation. The key technologies of the deliberate attack defense for IECPS are shown in Figure 15.

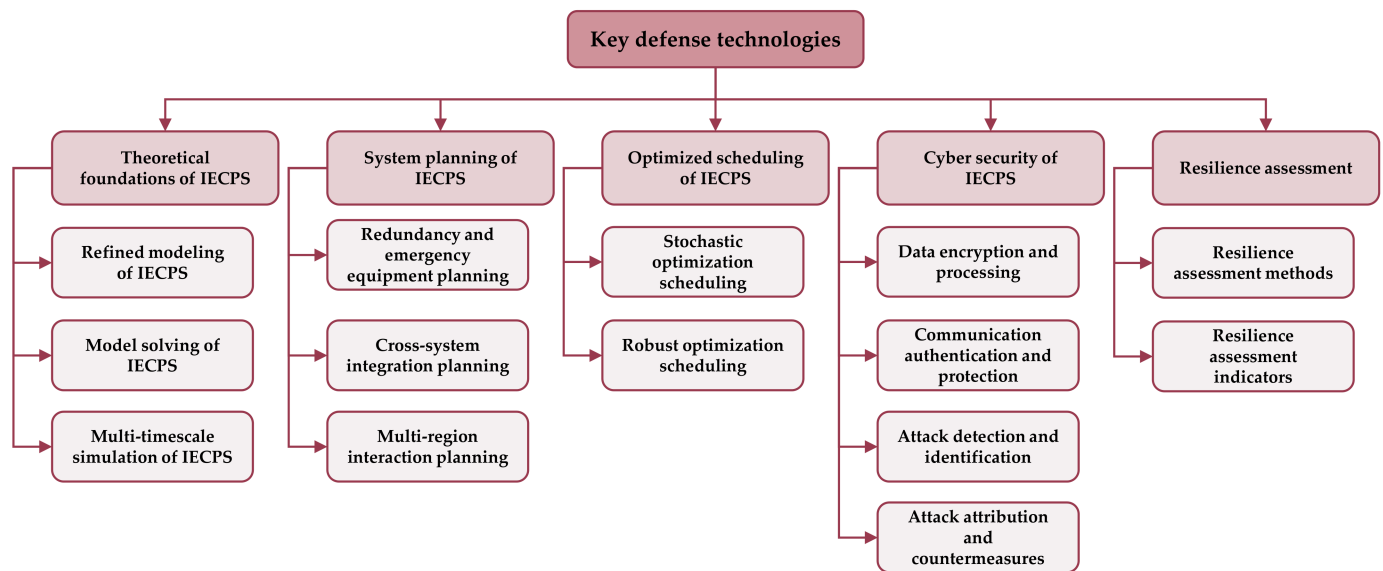


Figure 15. Key defense technologies against deliberate attacks in IECPS.

5.1. Theoretical Foundations of IECPS

A comprehensive theoretical understanding of IECPS is essential for all research and applications within this field. By systematically analyzing the coupling operation mechanisms of IECPS, we establish a refined system operation model to support research on fault propagation mechanisms and collaborative optimization within IECPS. Following the establishment of this refined model, we employ efficient model-solving methods for rapid resolution of defense optimization models, enabling real-time formulation of defense strategies. Building upon this foundation, multi-time-scale simulation technologies are utilized to achieve high-precision simulations of deliberate attack-defense processes [6]. Through elucidating the propagation mechanisms of deliberate attack impacts on system failures and the effectiveness of defense measures, this study provides scientifically executable plans for system operation and defense strategies.

5.1.1. Refined Modeling of IECPS

The modeling technology of IECPS is of great significance in understanding the system's operational mechanisms, analyzing deliberate attack behaviors, and formulating effective defense strategies. By meticulously modeling the infrastructure, energy conversion devices, and communication controls of each system, it captures the complex coupling relationships between cyber and physical networks, thereby accurately characterizing the dynamic properties between cyber flow and energy flow [190]. Based on the system's dynamic characteristics, the impact of deliberate attacks and their propagation process can be accurately simulated, while also allowing for the evaluation of the defense effectiveness of corresponding response strategies. The main distinction between IECPS and integrated energy systems lies in the former's focus on the interaction mechanisms between cyber and physical systems. In modeling, it requires separate modeling of the abnormal states of each

cyber–physical coupling component. In contrast, the latter diminishes the role of cyber systems in operational processes and is unable to display the real impact of cyberattacks on physical systems.

In addition to the detailed modeling of the system's devices, it is also crucial to develop a precise attack model. By hypothesizing the behavior of attackers based on existing case studies and deducing their actions using the IECPS operational model, the attacker's path and its impacts can be simulated. When hypothesizing attacker behaviors, it is important to not only consider traditional single attack methods but also combine them to design diversified attack models involving multiple types of cyberattacks and cyber–physical coordinated attacks, thereby creating a diverse attack model library to guide the research of defense strategies.

Moreover, the focus is on all the defense resources within IECPS that can be used to resist or mitigate deliberate attacks. By combining the operational model and attack model, the response of these defense resources is analyzed, and a corresponding defense resource response model is established. Besides depicting the response model of defense resources, a cost model for utilizing these resources must also be established. Given a limited budget, the optimal allocation of defense resources is studied to maximize the effectiveness of the defense strategy [191]. During the model-building process, to ensure that the model can be solved within a limited time, it is necessary to balance model accuracy with computational speed, thereby enabling online application of the model. This allows for quick adjustments to the system's operational state and a preemptive response to deliberate attacks.

5.1.2. Model Solving of IECPS

The IECPS deliberate attack defense optimization model is a large-scale, nonlinear, multi-stage optimization model, which is mathematically challenging to solve for a global optimum. Typically, the optimization model needs to be processed before solving. Specifically, there are three methods for solving the model: analytic methods [192], heuristic algorithms [188], and machine learning methods [193–195].

- **Analytic methods**

The analytic method involves using techniques such as linearization, convex relaxation, and duality to convert the IECPS defense optimization problem into a solvable linear programming or mixed-integer programming problem. The linearization method can transform the nonlinear equations of the gas or thermal systems into linear equations. Common linearization methods include piecewise linearization, logarithmic transformation linearization, Big-M method, and convex relaxation [196]. To convert the deliberate attack model into a single-layer model for solving, duality or Karush–Kuhn–Tucker conditions are commonly used for the transformation.

The analytic method can be specifically categorized into two approaches: unified solving and decomposition–coordination solving. Unified solving involves integrating all constraints and variables of the IECPS defense optimization problem into a single model for solution. This method faces difficulties in solving complex systems. Decomposition–coordination solving involves optimizing and solving each subsystem individually, then exchanging the results of each subsystem's solution. The results are used to iteratively update the subsystems until the optimal solution with the required precision is found. This method ensures the confidentiality of each subsystem's information during the decision-making process while achieving a global or near-global optimum for the entire system.

- **Heuristic algorithms**

Considering that some defense problems are highly complex, nonlinear, and non-convex, traditional analytic methods are difficult to model and solve, heuristic algorithms can be employed for handling them. Heuristic algorithms are optimization algorithms constructed based on intuition or experience, capable of providing a feasible solution for defense optimization within an acceptable time. Currently, commonly used heuristic algorithms are swarm intelligence algorithms, such as particle swarm optimization and ant colony optimization [193].

- **Machine learning methods**

AI methods do not focus on the type and characteristics of the problem when solving optimization problems, making them effective in solving IECPS defense optimization problems with non-linear and non-convex properties. Compared to analytic methods, AI methods can flexibly adapt to different attack scenarios without the need for model reconstruction, and they offer more efficient solution speeds. Compared to heuristic algorithms, they can handle most deliberate attack problems. However, AI methods require high-quality training data to ensure the accuracy of the solution. Although unsupervised learning methods that do not require attack cases have been developed, these methods still lack interpretability. Common machine learning methods include support vector machines, k-nearest neighbors, principal component analysis, Q-learning, and deep reinforcement learning [194,196–198].

In practical applications, the above methods can be combined based on the specific problem at hand. For instance, in robust optimization problems involving attack uncertainty, particle swarm optimization can be used to generate defense strategies, or machine learning methods can be employed to optimize attack strategies, while the remaining parts of the problem can be solved using analytical methods. This combined approach improves both the solution efficiency and the accuracy of the results.

5.1.3. Multi-Timescale Simulation of IECPS

IECPS integrates different energy sources and couples cyber networks with physical networks. It involves not only fast information transmission and electricity transmission but also slow processes such as gas flow and thermal processes. At the system level, it involves not only real-time operation scheduling but also long-term system planning. Therefore, IECPS defense against deliberate attacks exhibits typical multi-time scale characteristics. With the help of multi-time scale simulation technology, these characteristics can be modeled and solved with differentiation, enabling comprehensive analysis of deliberate attacks and system defense [170]. Figure 16 illustrates the application of multi-time scale simulation technology in the research of IECPS deliberate attack and defense.

As shown in Figure 16, multi-time scale simulation technology enables the understanding of the propagation process of deliberate attacks. The complex dynamic behaviors inherent in IECPS lead to unclear mechanisms of deliberate attacks. Particularly in the case of cyber–physical coordinated attacks, cyberattacks manifest within a very short time, while the cascading effects of physical failures operate on time scales of seconds or even minutes. By introducing multi-time scale simulation, the propagation paths of attack impacts across both cyber and physical domains can be dynamically traced, thereby optimizing attack models and providing more advanced experimental subjects for system defense [199]. Additionally, multi-time scale simulation technology provides a validation platform for long-term defense strategies, such as redundancy resource allocation and system recovery plans. Although system planning and recovery focus on longer time scales, they cannot be effectively implemented without short-term dynamic simulations. Finally, multi-time scale simulation technology is of crucial significance for the rapid response of the system.

In practical operations, deliberate attacks are often sudden and dynamic. Attackers adjust their strategies dynamically based on the system's state, and existing defense strategies are often inadequate to resist such attacks. With the assistance of multi-time scale simulation technology, attackers' behaviors can be predicted, enabling rapid response and precise intervention in the event of an attack.

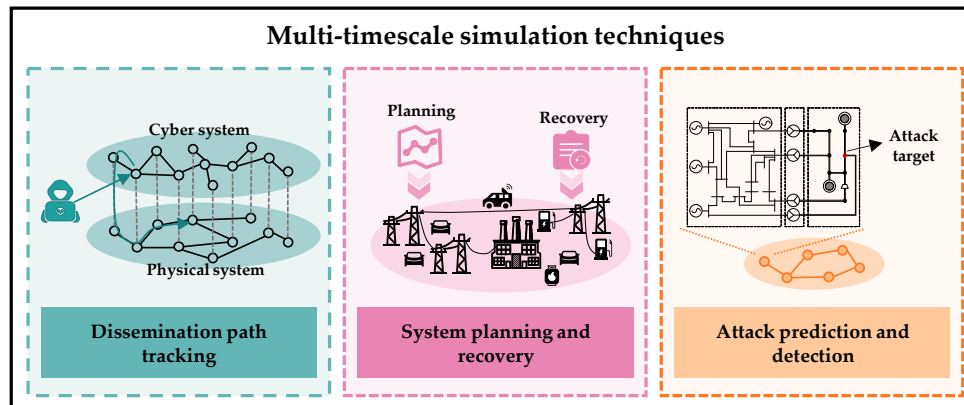


Figure 16. Application of multi-time scale simulation technology in deliberate attack defense.

5.2. System Planning of IECPS

Incorporating the impact of deliberate attacks into the planning phase of IECPS is beneficial for enhancing the system's defense capabilities against such attacks. By utilizing cross-system integration planning technology, multi-region interaction planning technology, and flexible emergency planning technology, early-stage planning of IECPS infrastructure can be conducted, proposing defensive measures to counter various types of deliberate attacks.

5.2.1. Redundancy and Emergency Equipment Planning

The planning of redundancy and emergency equipment aims to reduce the likelihood of attacks and minimize damage during an attack by strategically incorporating essential equipment. For cyber-related measures, this includes installing key data measurement devices to provide backups and enable verification. Additionally, fiber optic communication helps prevent transmission interruptions caused by power line damage. To restore networks disrupted by deliberate attacks, emergency communication vehicles are deployed. Strengthening system firewalls and intrusion detection systems further enhances the ability to resist and detect network attacks. Finally, data storage backup centers ensure the recovery of data and support traceability after an attack.

In terms of physical equipment, measures encompass deploying fault inspection drones and other mobile monitoring instruments to quickly locate faults; equipping fast isolation devices to provide equipment support for fault isolation; providing sufficient emergency repair vehicles to ensure the rapid arrival of repair personnel; setting up emergency power generation vehicles, fixed/mobile energy storage to provide short-term emergency power for system response and recovery; equipping uninterruptible power supplies and independent microgrids to ensure emergency power supply for key devices and loads; replacing critical lines with underground cables to enhance the ability to withstand extreme events.

When planning redundancy and emergency equipment, it is crucial to focus on the system's coordination and risk resistance capabilities. Equipment configuration must take into account the interactions between different systems to enhance the system's flexibility in emergency response. For various potential deliberate attacks, equipment must be capable of resisting single-point and multi-point fault propagation. Additionally, emergency equip-

ment planning must support rapid deployment and scheduling to minimize the impact duration of deliberate attacks. Furthermore, within a limited budget, priority should be given to deploying the aforementioned equipment in critical locations, thereby optimizing emergency resource allocation to maximize the defense effectiveness against deliberate attacks.

5.2.2. Cross-System Integration in Planning

With the coordinated progress of electrification and digital transformation, the integration between energy systems and cross-domain systems, such as transportation and cyber, is continuously improving [77]. Traditional energy system planning is gradually shifting towards cross-system integration planning to address the increasing demand for defense and control in energy systems. Cross-system integration planning technology aims to establish a unified information-sharing platform, applying transportation data to energy dispatching while ensuring data security. This approach, which leverages cyber systems to coordinate and optimize energy and transportation systems, not only effectively improves energy utilization efficiency but also provides a novel technological methodology for IECPS.

Specifically, the cross-system integration planning technology takes into account the significant aggregation and adjustment capabilities of EVs, which can act as a “virtual power plant” for regional energy regulation. When a deliberate attack occurs, by adjusting the charging prices or controlling the charging power of charging stations, the energy supply and demand in the region can be rapidly balanced, effectively suppressing the chain propagation of faults and preventing the further expansion of the attack’s impact. Moreover, after the coordinated planning of transportation and IECPS, IECPS can utilize shared traffic flow data to adjust the repair teams’ emergency routes, ensuring the fastest restoration of energy supply, and thereby significantly enhancing the defense capability of IECPS.

5.2.3. Multi-Region Interaction on Planning

In the process of advancing energy integration, users with similar energy consumption characteristics gradually aggregate to form regional integrated energy systems dominated by industries, commerce, and residents. Traditional regional integrated energy system planning focuses only on infrastructure within the region. However, due to similar internal resource endowments and limited adjustable resources, it is difficult to establish a stable and reliable energy defense and control system. Therefore, breaking the spatial limitations of a single region and promoting multi-region energy complementarity and coordination enables the tapping into the adjustment potential of regional integrated energy systems with different energy consumption characteristics, thereby enhancing the system’s ability to resist deliberate attacks.

The key to multi-regional interactive planning technology lies in reasonably determining the site selection and capacity configuration of regional energy stations and optimizing the layout of energy transmission pipelines between regions. Subsequently, through the unified scheduling of the cyber system, it addresses the imbalance of energy supply and demand in both time and space, achieving complementary coordination of energy. Overall, benefiting from the energy usage differences in different regional systems, multi-regional interactive planning enhances the system’s ability to respond to uncertainty, improve anti-interference performance, and enables rapid recovery characteristics. This ensures that the system possesses sufficient flexibility to maintain sustainable energy supply in the face of diversified deliberate attacks.

5.3. Optimized Scheduling of IECPS

The information control center of IECPS coordinates the unified operation of the multi-energy system based on the complementary characteristics of various energy types such as electricity, heat, and gas, as well as the principle of energy ladder utilization. This represents a significant means of enhancing energy utilization efficiency [200]. During the optimization scheduling process, the information control center can integrate the coordination capabilities of multiple energy sources and the potential of emergency resources, forming a multi-stage, multi-level defense system that gradually reduces the impact of deliberate attacks, thus providing effective support for enhancing the overall defense capability of the system. Given the highly secretive nature of deliberate attacks, their methods and capabilities of intrusion exhibit significant uncertainty. Consequently, IECPS optimization scheduling for deliberate attacks must pay particular attention to the uncertainty of such attacks. Stochastic optimization and robust optimization are two of the most commonly used methods for managing uncertainty. By employing these two scheduling techniques, it is possible to effectively address the issue of decreased defense strategy performance caused by the uncertainty of attacks. Table 4 presents a comparison of optimal scheduling studies that account for uncertainty.

Table 4. Comparison of Optimal Scheduling Studies Considering Uncertainty.

System	Methods		Multi-Stage Model	Data Driven	Ref.
	Stochastic Optimization	Robust Optimization			
Electric–Heat–Gas Integrated System	✓	✓	✓ ✓		[201] [202]
Integrated power and gas system	✓		✓		[203,204]
	✓	✓			[205]
		✓		✓	[206] [207]
Integrated heat and electric system	✓	✓	✓ ✓	✓	[208,209] [210]

5.3.1. Stochastic Optimization Scheduling

Stochastic optimization is a method that uses probability theory to handle the impacts of uncertainty. The stochastic optimization for deliberate attack defense generally includes the following key steps: firstly, defining the quantitative indicators and constraints for the defense against deliberate attacks, with the objective function usually being the expected value or chance constraint. Secondly, using probability distributions or historical data to generate possible attack scenarios. Lastly, solving the stochastic optimization model using methods such as two-stage programming or dynamic programming, resulting in defense strategies that consider uncertainty. Among these methods, two-stage programming is the most commonly used method, which is divided into pre-decision and post-adjustment, corresponding to the decision-making process before and after uncertainty occurs. However, the assumed probability distributions may contain inaccuracies in characterizing the uncertainty. Furthermore, since stochastic programming converts uncertainty models into deterministic models by generating numerous scenarios, and considering the complex operational state of IECPS, the model's solution scale can become very large, making it difficult to solve. Therefore, it is necessary to reasonably apply methods such as scenario reduction techniques and extreme scenarios to optimize the selection of deliberate attack scenarios [203]. Additionally, one can consider retaining key uncertainty factors while neglecting less significant ones, thereby reducing the number of random variables in the stochastic optimization problem. This approach diminishes the difficulty of solving and enhances solution speed and efficiency.

5.3.2. Robust Optimization Scheduling

Unlike stochastic optimization, robust optimization does not rely on specific probability distributions for uncertainty parameters such as deliberate attacks and system failures. Instead, it is an uncertainty decision-making method based on interval perturbation information. Because it does not rely on the assumption of probability distributions, it is more suitable for deliberate attack defense optimization studies with scarce historical data. Moreover, this method considers the optimal solution under the worst-case scenario as the final defense strategy, resulting in a defense strategy with high feasibility. However, by focusing on the defense strategy under the worst-case scenario, this method compromises some level of optimality. To reduce the conservatism of robust optimization scheduling, it can be mitigated using distributionally robust optimization techniques. In addition, robust optimization also faces the same model complexity issues as stochastic programming. Data-driven distributionally robust optimization can be explored as an alternative.

5.4. Cyber Security of IECPS

With the development of cyber technology, cyber systems have gained increasing significance in the operation and control of IECPS. Deliberate attacks on IECPS cyber systems have become more frequent, and the methods of attack have become more diverse. However, at its core, these attacks primarily disrupt the functionality of communication and the integrity of data. Therefore, it is essential to upgrade data encryption and processing technologies, along with communication authentication and protection technologies, to prevent damage to data integrity and communication functionality. By integrating attack detection and identification technologies, it becomes feasible to sense and issue alerts in response to deliberate attacks, thereby further strengthening the defense capabilities of IECPS. Simultaneously, using attack traceability and countermeasure technologies, deliberate attacks can be recorded, and corresponding countermeasures can be designed to prevent similar attacks from recurring.

5.4.1. Data Encryption and Processing

By leveraging wide-area measurement technology and agile control strategies, IECPS achieves safe, stable, and efficient operation. During this process, vast amounts of operational data are collected, transmitted, stored, and processed across various hierarchical levels of the system. To prevent operational data from being eavesdropped or tampered with, data encryption serves as a crucial defensive measure against potential attacks.

Data encryption refers to the process of converting plaintext data into ciphertext, which cannot be directly recognized or read, using specific encryption algorithms. During transmission or storage, unauthorized personnel cannot directly access, steal, or tamper with the encrypted data; only the recipient holding a valid key can decrypt the ciphertext back to plaintext. However, performing encryption and decryption on massive amounts of data can affect the speed of information computation and processing, greatly impacting the agility of system control, which in turn compromises the system's security and stability. To address this issue, less sensitive data can be selectively deleted, or only sensitive data can be encrypted. Additionally, encryption methods that match hardware accelerators are used to speed up the encryption process of sensitive data, thereby balancing real-time requirements and security control.

To achieve wide-area measurement and agile control in IECPS, a significant number of internet of things (IoT) and embedded devices are deployed at the terminals of the physical system. These devices, with their low power consumption and weak computing capabilities, require higher adaptability for encryption and processing technologies. Lightweight encryption technology is a data encryption method designed specifically for

resource-constrained devices, requiring very low computational power and energy consumption, and operates at high speed [211]. Common lightweight encryption algorithms include symmetric encryption, stream cipher algorithms, hash algorithms, public-key encryption algorithms, etc. By flexibly selecting the encryption algorithm based on the scenario limitations, the system's defense capabilities can be maximized.

In recent years, quantum encryption technologies based on the “uncertainty principle” and the “no-cloning theorem of single quantum” have begun to be implemented in the business scenarios of energy systems. Among them, quantum encryption methods represented by the BB84 quantum key distribution protocol have been initially piloted in small-scale trials in scenarios such as distribution automation, distribution network protection, new energy monitoring, and transmission line monitoring [67].

5.4.2. Communication Authentication and Protection

In IECPS, unified communication between different energy subsystems is becoming increasingly necessary, but it also brings many security issues, which can be categorized into signaling security, streaming media transmission security, and IP backbone network security [212]. For signaling security, the HTTP digest verification mechanism is used to ensure authentication security, while the transport layer security protection mechanism is employed to ensure the encryption of signaling. Streaming media transmission security can be achieved by using secure real-time transport protocol for encryption, ensuring the confidentiality and functionality of streaming media during transmission. As for the security of IP backbone networks, it is typically ensured using firewall technologies, demilitarized zones, and virtual network technologies. The demilitarized zone and virtual network are used to address the issue where users accessing external networks after firewall installation cannot reach internal network servers, and these methods are widely applied by grid operators. With the advancement of communication and authentication protection technologies, more effective communication protection methods, such as quantum communication technology and software-defined networking, are gradually being applied.

5.4.3. Attack Detection and Identification

Deliberate attack detection and identification are key elements in ensuring the safe operation of IECPS. Effective deliberate attack detection methods help intrusion detection systems (IDS) identify potential deliberate attacks in a timely manner, thereby strengthening the defense capabilities of IECPS against deliberate attacks. In Section 4.2.1, methods for deliberate attack detection are analyzed based on underlying principles. In practice, the aforementioned deliberate attack detection methods are integrated into the IDS. By strategically deploying IDS within IECPS, the detection algorithm's capability can be maximized. A centralized IDS uses a single sensor to monitor all traffic entering and exiting measurement devices, as well as access system logs. This helps identify internal attacks in the IECPS network and detects systemic intrusions by scanning access records and analyzing the anti-tampering signals provided by the measurement devices. Embedding IDS into the deployment of measurement instruments can significantly improve the detection accuracy and the reliability of early warnings, though it comes at a higher cost. Additionally, there are IDS deployed in cloud service platforms and distributed IDS, among others. In the future, attention should be given not only to upgrading deliberate attack detection algorithms but also to IDS deployment strategies, in order to enhance the system's defense capabilities.

5.4.4. Attack Attribution and Countermeasures

Attack tracing technology can extract and analyze deliberate attack events occurring in IECPS, providing technical support for countermeasures. In the field of cyber security,

methods such as IP tracing, log and traffic analysis, domain name system tracing, link tracing, and routing analysis are commonly used for attack tracing. However, due to the complex cyber–physical interaction mechanisms and massive operational data in IECPS, traditional traffic analysis techniques face issues of low efficiency and high analytical difficulty. At this point, big data technology and AI can be used to extract and analyze attack characteristics of the system, thereby speeding up the efficiency of attack tracing.

Attack countermeasure technology serves as a preemptive defense technique. With the increasing number of new types of attacks, passive defense technologies such as planning, detection, and scheduling struggle to provide effective protection. To address this flaw, the academic community has developed attack countermeasure technologies, such as honeypot technology. Figure 17 illustrates a schematic diagram of a honeypot technique, which depletes an attacker's attack resources by arranging a number of hosts, network services, or information that serve as decoys and entice the attacker to attack them. In addition, honeypot technology can capture the attacker's behavior, infer their intentions and motivations, and subsequently strengthen the system accordingly.

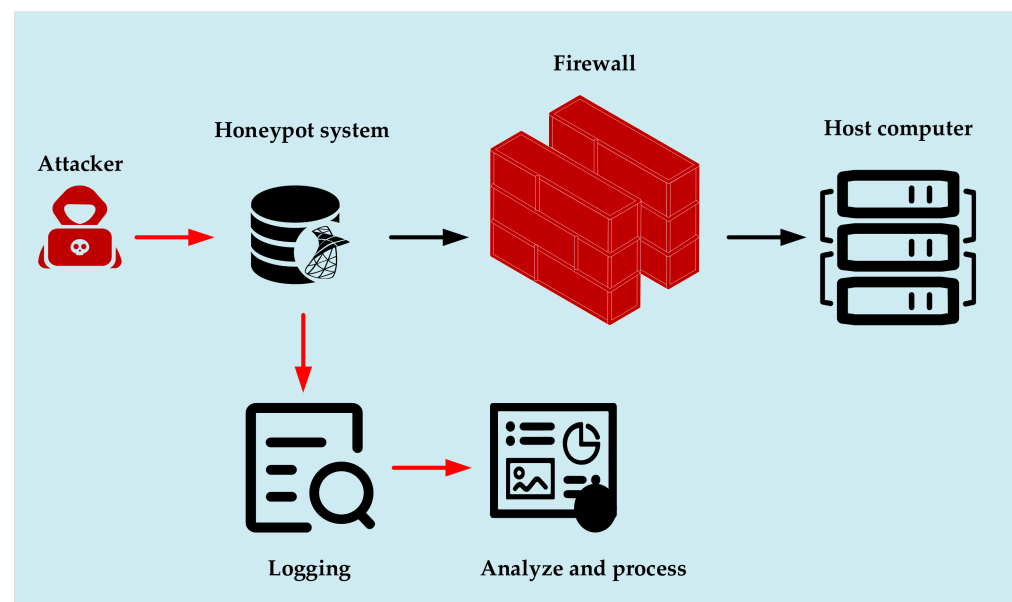


Figure 17. Schematic diagram of honeypot technology.

5.5. System Defense Assessment Technology

The concept of comprehensive energy system resilience evaluates multiple aspects, including system status, component risk, operation decision, and system recovery, taking into account operation constraints and the development process of extreme events. Thus, based on this, the system operation and recovery strategy are adjusted. It is an advanced indicator for evaluating the losses of IECPS from intentional attacks. It can also reflect the quality of the system defense strategy from the side and guide the upgrade of the defense strategy.

5.5.1. Resilience Assessment Methods

Resilience assessment methods include qualitative and quantitative assessments [213]. Qualitative assessments include questionnaire surveys [214], the analytic hierarchy process [215], etc. Such methods rely on the cognitive level of the assessment subject. The assessment results obtained by different assessment subjects vary greatly, and the objectivity of the assessment is slightly weak. In addition, the complex coupling mechanism and a

large number of uncertain factors within the integrated energy system further reduce the practicality of qualitative assessment.

Quantitative assessments mainly include statistical analysis and simulation. The statistical analysis method is to infer and analyze the system's resilience in a certain period in the future by statistically analyzing the frequency and severity of system failures in extreme events in history. For example, by statistically analyzing the historical failure data of the system, using probability density distribution fitting methods [216] or establishing Bayesian networks [217] to reasonably analyze system failures under extreme events, we can then evaluate the system resilience. This method is highly dependent on historical data, and it is difficult to ensure the accuracy of the assessment for extreme events with low probability. The simulation method establishes a disaster and system model, simulates the entire process of the system responding to extreme disasters, collects system operation status data for resilience index calculation, and evaluates the resilience of the system based on the value of the index. In [218], researchers established an earthquake fault model and a system repair model to simulate the system's resistance and recovery process under earthquake scenarios, and established robustness, rapidity, and redundancy indicators to evaluate the resilience of the integrated energy system. In [219], the authors established an electric-gas coupling system model under a hurricane scenario to evaluate the system resilience from the aspects of system operation, infrastructure failure, and economic losses. The evaluation results obtained by the simulation method are highly interpretable and easy to understand and accept. The main steps of the simulation method include fault scenario modeling, system response and recovery modeling, system operation simulation, and resilience indicator calculation and evaluation.

5.5.2. Resilience Assessment Indicators

The resilience index system is a standard for evaluating the resilience of integrated energy systems. The rationality of the selection of resilience indicators is related to the accuracy of resilience assessment. At present, system resilience indicators can be divided into two categories: resilience indicators based on system structure and resilience indicators based on system performance.

Resilience indicators based on system structure include system topology, component redundancy, resource abundance, etc. [220–223]. Resilience indicators based on system performance are mostly based on the system performance curve shown in Figure 18. This curve describes the trend of system performance changes over time before and after extreme events occur.

In the IECPS resilience assessment, it is critical to determine which indicators are used to quantify system performance. Table 5 summarizes the existing resilience indicators based on system structure and system performance.

As can be seen from the above table, although the current resilience indicators are constructed from multiple perspectives based on system characteristics, there is still a lack of discussion on information system losses. Although the damage to the information system will be reflected in the loss of the physical system, measuring the physical system alone cannot reflect the true loss of the entire IECPS. Therefore, multi-dimensional evaluation indicators are necessary.

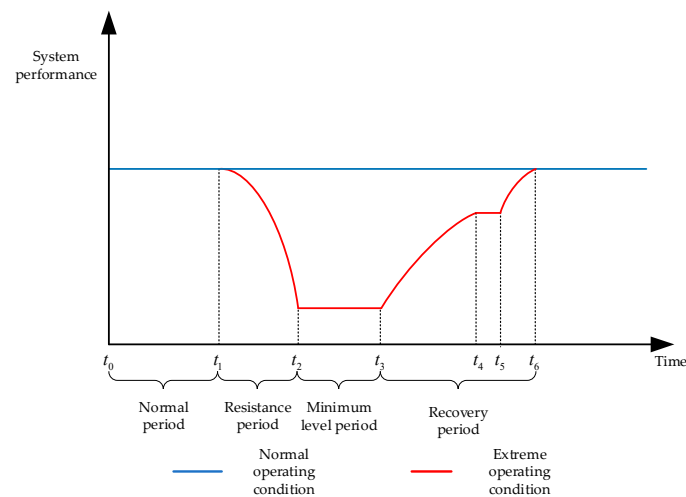


Figure 18. Comprehensive performance curves for energy system operation.

Table 5. System structure-based and system performance-based indicators.

Indicator Categories	Indicators	Evaluation Object	Ref.
System structure-based indicators	Node degree, node betweenness, weighted node degree of betweenness, connectivity	Power system	[222]
	Distribution line strength	Distribution network	[223]
	Number of common branches, number of switch operations, path redundancy ratio, equipment availability	Power system	[224]
	Component redundancy	Integrated energy system	[225]
System performance-based indicators	Load loss expectation	Integrated energy system	[219]
	Load recovery rate	Power System	[226]
	Performance curve integral area	Power system	[227]
	Maximum loss of important loads, load recovery rate	Power system	[228]
	Load loss duration	Integrated energy system	[229]

6. Issues and Challenges in the Defense Against Deliberate Attacks on IECPS

Due to the limitations of current key technologies, coupled with the complex operational mechanisms of IECPS and the high uncertainty of deliberate attacks, the full-process defense strategy, including preemptive prevention, process response, post-event recovery and summarization, faces challenges such as difficulties in modeling and solving problems, attack detection and early warning, as well as defense assessment and improvement during its implementation.

6.1. Complexity of Modeling and Solving

The difficulty in modeling deliberate attacks in IECPS mainly arises from the diversity of equipment types, significant differences in energy flow, and the heavy influence of uncertainty. IECPS includes numerous defense components and flexible devices (i.e., remote switches, EVs, combined heat and power, power-to-gas devices, etc.), and there are complex interrelationships between these components and devices. Furthermore, due to differences in layout or system configurations, even the same type of device may exhibit different responses when facing deliberate attacks. Additionally, with the involvement of cyberattacks, modeling must also account for the cyber network and the cyber–physical coupling mechanisms, further increasing the complexity of the device models.

Secondly, due to the significant dynamic differences in energy flow among different subsystems, the impact of implementing deliberate attacks and defense strategies in different systems exhibits complex spatiotemporal correlations. It is not feasible to simply understand IECPS as merely the sum of multiple subsystems, nor can the system model be simplified from a holistic analysis perspective. Only by combining multi-timescale methods to establish a dynamic operation model for IECPS can this spatiotemporal correlation be described. Compared to steady-state system models, the difficulty of modeling increases dramatically.

For complex systems like IECPS, it is challenging to comprehensively model and efficiently solve the system state using traditional model-driven methods alone. Data-driven AI methods can effectively address the challenges of complex system modeling and solving by extracting hidden information and knowledge from vast amounts of data, enabling autonomous learning and automatic modeling. However, AI-based modeling solutions face the challenge of lacking interpretability.

At present, the problems of system modeling and solving affect the whole process of deliberate attack and defense. In the pre-prevention strategy with planning as the core, the strategy has low requirements for the model's solution speed. However, the accuracy of the model itself and the accuracy of the solution method seriously affect the cost investment in the planning phase. In the case of limited defense costs, it may lead to a weaker defense system in the configuration. In the mid-event response phase, the accuracy and solution speed of the model have the greatest impact. First of all, the detection of deliberate attacks depends heavily on the accurate grasp of the system state, and models with large deviations are easy to cause missed detections and false detections. Secondly, the formulation and implementation of fault isolation and multi-source collaborative scheduling strategies are highly time-sensitive. Attackers can exploit this vulnerability to carry out multi-stage attacks and further expand the scope of the attack. Therefore, it is necessary to put forward higher requirements for the solution accuracy and speed of the model. Several strategies in the post-event recovery and summary stage are based on evaluation and analysis; the corresponding evaluation model needs to be established in this stage, and the quality of the evaluation model determines whether the defense strategy can be included in the defense strategy library, so as to respond quickly when similar attacks occur next time.

6.2. Difficulties in Attack Detection and Early Warning

IECPS plays a crucial role in achieving efficient energy collaboration and actively promotes the development of a diversified energy market. In this process, a large number of emerging producers and consumers have emerged, whose participation enhances the competitiveness of the energy market while also posing new security challenges to the system. At the same time, to improve operators' system awareness and users' energy quality, a large number of IoT devices have been widely deployed within IECPS. IoT devices play an indispensable role in enhancing the intelligence and automation of the system; however, they also open up additional intrusion channels for potential attackers, making it difficult to detect and prevent small attacks originating from system terminals in a timely and effective manner. Especially in the case of massive interconnection among producers, consumers, and IoT devices, attackers can exploit the complexity and diversity of the system to easily bypass traditional security measures.

With the large-scale integration of renewable energy, the source side is highly influenced by extreme weather, potentially resulting in significant power fluctuations in a short period. If an attacker launches a deliberate attack during this period, hiding the attack data within normal system fluctuations, the attack can easily bypass system detection. Moreover, during extreme disasters, the perception capability of IECPS diminishes significantly, and

the focus at the scheduling level shifts to disaster recovery efforts. At this point, attackers can easily carry out cyber–physical collaborative attacks. This can lead to erroneous system scheduling, thereby expanding the scope of system damage.

Whether it is due to the system's complex architecture or frequent external extreme events that make attack detection more difficult, the fundamental issue is the limited adaptability of existing attack detection algorithms to unknown attacks. Although some AI algorithms can dynamically adjust model parameters to counter unknown attacks, existing research has proven that attackers can manipulate the construction, training, and deployment processes of AI detection algorithms through backdoor attacks, thereby decreasing the probability of detecting deliberate attacks and faulty data. Compared to directly attacking the physical power grid system, embedding backdoors into the model constitutes a more covert form of attack. By altering the algorithm's application in business decision-making systems, this behavior can cause far more severe consequences [230,231].

The challenges of attack detection and early warning reduce the speed and intensity of the execution of response strategies during the incident. On the one hand, diverse attack patterns and complex system characteristics make attack detection increasingly difficult. In order to avoid the occurrence of false detection, the existing detection methods cannot eliminate all malicious attacks. On the other hand, with the increase in uncertainties, the system has to set up multiple links to verify the normal operation of the system, which slows down the speed of the system's early warning. In addition, the backwardness of attack detection technology will also affect the accuracy of attack source tracing and analysis, and some advanced combined attacks may be completely ignored.

6.3. Obstacles in Defense Evaluation and Improvement

Scientifically and reasonably evaluating the system's ability to resist deliberate attacks is fundamental to enhancing the defense capability of IECPS. It offers quantifiable standards for system design, operation and maintenance management, as well as the formulation of efficient defense strategies. However, most current defense evaluation methods use the reduction in system losses as the evaluation criterion for the enhancement of defense capability. While these methods can accurately depict the defense capability of a single energy system, the complex coupled dynamics of IECPS cannot be accurately captured by the reduction in system losses when the defense capability of IECPS is being assessed.

Firstly, there are significant dynamic characteristic differences between various energy systems, and their losses manifest differently in terms of time and space. For example, the response speed of the power system is typically within seconds or even milliseconds, whereas thermal and gas systems undergo dynamic changes typically on a scale of minutes. This dynamic difference results in asynchronous responses and recovery processes among different energy subsystems when implementing defense measures and facing attacks, making the accurate quantification of the impacts of these disturbance events highly complex at the physical layer.

The high coupling between the IECPS cyber network and the physical network further increases the complexity of the evaluation. The disruption of the cyber system affects the system's perception and control capabilities, subsequently impacting the operation of the physical system through the cyber–physical coupling mechanism. Existing evaluation methods often overlook the impact of cyber system losses on the overall system; instead, they use the losses in the physical system as the evaluation criterion for the entire system, leading to significant discrepancies in the evaluation results.

In addition, the stealth and unpredictability of deliberate attacks further complicate defense evaluation. In actual defense processes, there is often a scarcity of sufficient and complete attack event data, prompting the use of simulations based on hypothetical

attack scenarios. These hypothetical defense enhancement strategies can theoretically offer effective evaluation methods and improvement strategies for system defense, but validating them in real experimental environments proves challenging, thereby limiting the development of defense evaluation and enhancement technologies.

The obstacles in defense evaluation and improvement are integral to the entire process of formulating defense strategies. First, all defense strategies involving modeling cannot be separated from evaluation. Evaluation is not merely a process of validating results; it directly determines the effectiveness and optimization direction of defense strategies. Evaluation metrics typically represent the goals of defense optimization, and they must be scientific and rational. If unscientific evaluation metrics or methods are used, the resulting defense strategies may fail to meet the system's security requirements in practice and may even lead to unnecessary resource wastage. Furthermore, when evaluating the superiority of detection methods, multiple comprehensive indicators are typically required. For example, in attack detection methods, it is important not only to consider detection accuracy but also to account for detection speed, false positive rates, false negative rates, and other performance dimensions. The trade-offs and choices between these metrics are also part of defense evaluation. Therefore, defense evaluation is not just a summary of the results of defense strategies, but also an important basis for strategy improvement and adjustment.

7. Conclusions

As a new energy utilization model, IECPS demonstrates significant advantages in energy conservation and promoting the integration of renewable energy. During the process of multi-energy integration, the complex interaction mechanisms among subsystems create opportunities for fault propagation across systems. In addition to the threat posed by physical network integration to system security and stability, the high degree of coupling between cyber networks and physical networks expands the system's network boundaries, thereby increasing the risk of network attacks.

Improving the intentional attack defense capability of IECPS is the basis for ensuring the safe and stable operation of the system. It is crucial for promoting the development of IECPS and is one of the key directions in the research of multi-energy convergence. This paper starts with the intrusion paths of attacks, reviewing the attack principles of deliberate attacks and modeling methods for various types of attacks. Based on this, the defense strategies for the three stages of deliberate attacks—pre-attack, during attack, and post-attack—are summarized. In the context of deliberate attacks, achieving full-stage defense strategies relies on the support of key technologies such as theoretical foundations, system planning, optimization scheduling, and cyber security. With the help of these key technologies, the system's defense capabilities against deliberate attacks can be strengthened by reasonably planning the system architecture, predicting key risks, and designing appropriate resistance strategies.

It is important to note that technological limitations, inherent system uncertainties, and the unpredictability of deliberate attacks pose significant challenges to improving IECPS defense capabilities. These challenges encompass difficulties in system modeling and resolution, attack detection and early warning, as well as defense evaluation and enhancement. To facilitate the substantial development of IECPS, researchers must actively engage in relevant research and overcome these challenges and propose more effective defense strategies against deliberate attacks. Specifically, it needs to happen in the following ways.

- Advanced attack strategies. The development of more threatening attack strategies can clarify system weaknesses and vulnerabilities, and help update and iterate the defense

strategy. Nowadays, in addition to collaborating to develop based on several existing typical attack types, we should focus on the development of advanced cyberattack strategies against AI technology, which is applied in large numbers. Moreover, further research on multi-stage attack strategies that match real-world attack logic is needed, as this area of research is currently relatively weak.

- **Efficient data processing.** Combining traditional modeling methods with machine learning technology, we can develop a modeling method that combines both solution speed and solution accuracy to achieve high-precision digital reconstruction of IECPS. At the same time, the agility of system perception is improved with the help of big data technology to create IECPS with fast response capability and strong adaptability.
- **Reliable privacy protection.** In recent years, advanced persistent threat organizations and various cyber ransom syndicates have been targeting IECPS, and it is essential to strengthen the protection of data and information to prevent privacy leakage. The superior performance of quantum technology in data encryption and data transmission is expected to resist the intrusion of advanced persistent threat organizations and ransom groups into IECPS.
- **Advanced system planning.** At present, IECPS are still under gradual construction, but the development of various types of technology is very rapid. Only with advanced strategic planning can we avoid the problem of equipment compatibility that cannot be achieved during the construction of the subsequent security system. Whether to incorporate transportation into the energy system planning, as well as how to ensure the safety of the entire system after the incorporation of transportation into energy planning is topics that need to be explored.
- **Reasonable emergency response mechanism.** We should face the demand of users for rapid restoration of energy supply under malicious attacks, study the system reconfiguration and load restoration strategy of multi-energy synergy, and study the new technology of system restoration with the participation of resources, such as flex-direct, micro-grid, and energy storage. We should consider the emergency response mechanism in extreme situations, such as unsound pipeline networks and unavailable facilities, and improve the ability of IECPS to cope with malicious attacks.
- **Scientific assessment system.** The establishment of a scientific assessment system is the key to ensuring the rational formulation of system defense strategies. A multi-stage, multi-dimensional assessment system is not only conducive to accurately assessing the loss of the system but also can reflect whether the defense strategy is good or bad.
- **Advanced equipment development.** While information-based and intelligent equipment provides easy access to malicious attacks, it is undeniable that this advanced equipment maximizes the chances of stopping attacks. The development of more secure monitoring equipment can significantly reduce the probability of system attacks, while the development of equipment such as energy storage, electric vehicles, and emergency response devices provides regulating resources to mitigate the impact of attacks.
- **Stabilized energy markets.** The energy market serves as the foundation for the existence and operation of IECPS. Disruptions in the energy market will inevitably introduce uncertainties into the operation of IECPS, and attackers can potentially destabilize its safe and stable functioning by manipulating the market. Conversely, the energy market also possesses regulatory characteristics akin to those of the transportation system. Therefore, it is crucial to establish appropriate regulatory and operational frameworks to ensure that energy markets have a positive and stabilizing impact on energy systems.

- Practical energy projects. Future research also relies on a program of actual engineering projects. Each country should vigorously support the construction of relevant pilot projects to provide financial support for the construction of the safety system of IECPS, to provide research cases and accumulate technical experience. The combination of theoretical research and theoretical application will be accelerated by means of engineering applications.

Author Contributions: Project administration, writing—review and editing, funding acquisition, T.Z.; writing—original draft preparation, X.T.; writing—review and editing, C.L. and B.Z.; conceptualization, Y.G.; investigation, R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Science Foundation of China (No. 52377115, 51907097).

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

IECPS	integrated energy cyber–physical system
CCPA	coordinated cyber–physical attack
APT	advanced persistent threat
GPS	global positioning system
RA	replay attack
MITM	man-in-the-middle attack
FDIA	false data injection attack
TSA	time synchronization attack
DoS	denial of service attack
CCA	coordinated cyberattack
AGC	automatic generation control
IED	intelligent electronic device
FTU	feeder terminal unit
RTU	remote terminal unit
DTU	data transfer unit
AC	alternating current
LR	load redistribution attack
DC	direct current
PMU	phasor measurement unit
DDoS	distribution denial of service
EV	electric vehicle
AI	artificial intelligence
BDD	bad data detection
KF	Kalman filter
MTD	moving target defense
GLR	generalized likelihood ratio
QCD	quickest change detection
CUSUM	cumulative sum test
G2V	grid-to-vehicle
V2G	vehicle-to-grid
V2B	vehicle-to-building
IoT	internet of things
IP	internet protocol address
HTTP	hypertext transfer protocol
IDS	intrusion detection system

References

1. Yang, J.; Zhang, N.; Wang, Y.; Kang, C. Multi-energy system towards renewable energy accommodation: Review and prospect. *Autom. Electr. Power Syst.* **2018**, *42*, 11–24.
2. Zhang, W.; Zhang, C.; Li, J.; Zhu, L.; Cao, S.; Huang, W. Multi-resource collaborative service restoration of a distribution network with decentralized hierarchical droop control. *Prot. Control Mod. Power Syst.* **2024**, *9*, 19–37. [\[CrossRef\]](#)
3. Lin, Y.; Luo, H.; Chen, Y.; Yang, Q.; Zhou, J.; Chen, X. Enhancing participation of widespread distributed energy storage systems in frequency regulation through partitioning-based control. *Prot. Control Mod. Power Syst.* **2025**, *10*, 76–89. [\[CrossRef\]](#)
4. Lin, J. Risk Assessment of Cyber-Attacks in Integrated Energy System. Master's Thesis, Guangxi University, Nanning, China, 2021.
5. Zhang, G.; Zhong, H.; Tan, Z.; Cheng, T.; Xia, Q.; Kang, C. Texas electric power crisis of 2021 warns of a new blackout mechanism. *CSEE J. Power Energy Syst.* **2022**, *8*, 1–9.
6. Xin, B.; Li, M.; He, J.; He, J.; Sun, W. Research on security defense system of new power system. *Proc. CSEE* **2023**, *43*, 5723–5732.
7. Tang, Y.; Wang, Q.; Ni, M.; Liang, Y. Analysis of cyber attacks in cyber physical power system. *Autom. Electr. Power Syst.* **2016**, *40*, 148–151.
8. Zang, T.; Wang, Z.; Wei, X.; Zhou, Y.; Wu, J.; Zhou, B. Current status and perspective of vulnerability assessment of cyber-physical power systems based on complex network theory. *Energies* **2023**, *16*, 6509. [\[CrossRef\]](#)
9. Jang, K.B.; Baek, C.H.; Woo, T.H. Analysis of cyber nuclear terrorism by DTrack consequences in the civilian nuclear power plant. *J. Nucl. Sci. Technol.* **2022**, *59*, 207–215. [\[CrossRef\]](#)
10. Ransomware Operators Demand \$14 Million from Power Company. Available online: <https://www.securityweek.com/ransomware-operators-demand-14-million-power-company/> (accessed on 16 February 2025).
11. Energy Company EDP Confirms Cyberattack, Ragnar Locker Ransomware Blamed. Available online: <https://www.zdnet.com/article/edp-energy-confirms-cyberattack-ragnar-locker-ransomware-blamed/> (accessed on 16 February 2025).
12. America's Largest Oil Pipeline Hit by Cyberattack—Multiple States Declared in State of Emergency. Available online: <https://www.bbc.com/zhongwen/simp/world-57054720> (accessed on 16 February 2025).
13. Industroyer2: Industroyer Reloaded. Available online: <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/> (accessed on 16 February 2025).
14. Cyber Incident Victim: Acea. Available online: <https://www.csidb.net/csldb/incidents/39d3dade-5940-4110-8c1e-50a6c66528be/> (accessed on 17 February 2025).
15. Tang, Y.; Chen, Q.; Li, M.; Wang, Q.; Ni, M.; Liang, Y. Overview on cyber-attacks against cyber physical power system. *Autom. Electr. Power Syst.* **2016**, *40*, 59–69.
16. Tian, E.; Peng, C. Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks. *IEEE Trans. Cybern.* **2020**, *50*, 4610–4618. [\[CrossRef\]](#)
17. Tadepalli, P.S.; Pullaguram, D. Distributed control microgrids: Cyber-attack models, impacts and remedial strategies. *IEEE Trans. Signal Inf. Process. Netw.* **2022**, *8*, 1008–1023. [\[CrossRef\]](#)
18. Ahmed, C.M.; Palleti, V.R.; Mishra, V.K. A practical physical watermarking approach to detect replay attacks in a CPS. *J. Process Control* **2022**, *116*, 136–146. [\[CrossRef\]](#)
19. Deb Roy, S.; Sharma, A.; Chakrabarti, S.; Debbarma, S. Securing power system data in motion by timestamped digital text watermarking. *IEEE Trans. Smart Grid* **2024**, *15*, 4974–4985. [\[CrossRef\]](#)
20. Narang, J.K.; Bag, B. Deep learning-based integrated attack detection framework to protect distance relays against cyberattacks. *Electr. Power Syst. Res.* **2024**, *231*, 110346. [\[CrossRef\]](#)
21. Raoof, A.; Lung, H.; Matrawy, A. Securing RPL using network coding: The chained secure mode (CSM). *IEEE Internet Things J.* **2022**, *9*, 4888–4898. [\[CrossRef\]](#)
22. Wang, Y.; Chen, C.; Zhang, S.; Liu, Y.; Huang, C.; Du, Y. A Tri-level programming-based frequency regulation market equilibrium under cyber attacks. *Prot. Control Mod. Power Syst.* **2023**, *8*, 55. [\[CrossRef\]](#)
23. Cheng, G.; Lin, Y.; Zhao, J.; Yan, J. A highly discriminative detector against false data injection attacks in AC state estimation. *IEEE Trans. Smart Grid* **2022**, *13*, 2318–2330. [\[CrossRef\]](#)
24. Jena, P.K.; Ghosh, S.; Koley, E.; Manohar, M. An ensemble classifier based scheme for detection of false data attacks aiming at disruption of electricity market operation. *J. Netw. Syst. Manag.* **2021**, *29*, 43. [\[CrossRef\]](#)
25. Konstantinou, C.; Maniatakis, M. A case study on implementing false data injection attacks against nonlinear state estimation. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, Vienna, Austria, 28 October 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 81–92.
26. Zhang, Z.; Huang, S.; Liu, F.; Mei, S. Pattern analysis of topological attacks in cyber-physical power systems considering cascading outages. *IEEE Access* **2020**, *8*, 134257–134267. [\[CrossRef\]](#)
27. Yang, H.; He, X.; Wang, Z.; Qiu, R.C.; Ai, Q. Blind false data injection attacks against state estimation based on matrix reconstruction. *IEEE Trans. Smart Grid* **2022**, *13*, 3174–3187. [\[CrossRef\]](#)

28. Li, X.; Wang, Y.; Lu, Z. Graph-based detection for false data injection attacks in power grid. *Energy* **2023**, *263*, 125865. [\[CrossRef\]](#)
29. Musleh, A.S.; Chen, G.; Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid* **2020**, *11*, 2218–2234. [\[CrossRef\]](#)
30. Tan, R.; Nguyen, H.H.; Foo, E.Y.S.; Dong, X.; Yau, D.K.Y.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Optimal false data injection attack against automatic generation control in power grids. In Proceedings of the 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, 11–14 April 2016; pp. 1–10.
31. Musleh, A.S.; Chen, G.; Dong, Z.Y.; Wang, C.; Chen, S. Attack detection in automatic generation control systems using LSTM-based stacked autoencoders. *IEEE Trans. Ind. Inform.* **2023**, *19*, 153–165. [\[CrossRef\]](#)
32. Ghiasi, M.; Niknam, T.; Wang, Z.; Mehrandezh, M.; Dehghani, M.; Ghadimi, N. 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.* **2023**, *215*, 108975. [\[CrossRef\]](#)
33. Kumar, M.; Prasad, S.; Ansari, M.R.; Mohapatra, B. Resonance attacks detection and mitigation control scheme on frequency regulation in multi-area smart grid. *Int. J. Control* **2023**, *96*, 2212–2229. [\[CrossRef\]](#)
34. Yuan, Y.; Li, Z.; Ren, K. Modeling load redistribution attacks in power systems. *IEEE Trans. Smart Grid* **2011**, *2*, 382–390. [\[CrossRef\]](#)
35. Liu, X.; Bao, Z.; Lu, D.; Li, Z. Modeling of local false data injection attacks with reduced network information. *IEEE Trans. Smart Grid* **2015**, *6*, 1686–1696. [\[CrossRef\]](#)
36. Yuan, Y.; Li, Z.; Ren, K. Quantitative analysis of load redistribution attacks in power systems. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1731–1738. [\[CrossRef\]](#)
37. Ruan, J.; Yang, C.; Wang, Q.; Wang, S.; Liang, G.; Zhao, J.; Qiu, J. Assessment of spatiotemporally coordinated cyberattacks on renewable energy forecasting in smart energy system. *Appl. Energy* **2023**, *347*, 121470. [\[CrossRef\]](#)
38. Ruan, J.; Wang, Q.; Chen, S.; Lyu, H.; Liang, G.; Zhao, J.; Dong, Z.Y. On vulnerability of renewable energy forecasting: Adversarial learning attacks. *IEEE Trans. Ind. Inform.* **2024**, *20*, 3650–3663. [\[CrossRef\]](#)
39. Chen, F.; Shi, J.; Liu, H.; Wang, R.; Zhao, M.; Liu, D. Reliability evaluation of power generation and transmission system considering load redistribution attack and defense of vulnerable line. *Autom. Electr. Power Syst.* **2022**, *46*, 65–72.
40. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. A framework for cyber-topology attacks: Line-switching and new attack scenarios. *IEEE Trans. Smart Grid* **2019**, *10*, 1704–1712. [\[CrossRef\]](#)
41. Wang, S.; Ding, Z.; Wu, J.; Qiu, A. False data injection attack scheme of electricity market based on topology tampering. *Electr. Power Autom. Equip.* **2021**, *41*, 147–152.
42. Liu, X.; Li, Z.; Liu, X.; Li, Z. Masking transmission line outages via false data injection attacks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1592–1602. [\[CrossRef\]](#)
43. He, Z.; Gao, S.; Wei, X.; Zang, T.; Lei, J. Research on offensive and defensive game model of false topology attack based on collaborative tampering with branch and protection. *Power Syst. Technol.* **2022**, *46*, 4346–4355.
44. Liang, G.; Weller, S.R.; Luo, F.; Zhao, J.; Dong, Z.Y. Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism. *IEEE Trans. Smart Grid* **2018**, *9*, 3820–3829. [\[CrossRef\]](#)
45. Zhang, Z.; Gong, S.; Dimitrovski, A.D.; Li, H. Time synchronization attack in smart grid: Impact and analysis. *IEEE Trans. Smart Grid* **2013**, *4*, 87–98. [\[CrossRef\]](#)
46. Shereen, E.; Delcourt, M.; Barreto, S.; Dán, G.; Le Boudec, J.-Y.; Paolone, M. Feasibility of time-synchronization attacks against PMU-based state estimation. *IEEE Trans. Instrum. Meas.* **2020**, *69*, 3412–3427. [\[CrossRef\]](#)
47. Wang, Q.; Li, M.; Tang, Y.; Ni, M. A review on research of cyber-attacks and defense in cyber physical power systems part one modelling and evaluation. *Autom. Electr. Power Syst.* **2019**, *43*, 9–21.
48. Li, Y.; Huang, R.; Ma, L. Hierarchical-attention-based defense method for load frequency control system against DoS attack. *IEEE Internet Things J.* **2021**, *8*, 15522–15530. [\[CrossRef\]](#)
49. Zhang, X.; Liu, X.; Ding, T.; Wang, P. On resilience and distributed fixed-time control of mtdc systems under dos attacks. *IEEE Trans. Autom. Sci. Eng.* **2023**, *20*, 2569–2580. [\[CrossRef\]](#)
50. Zhang, Y.; Xie, X.; Fu, W.; Chen, X.; Hu, S.; Zhang, L.; Xia, Y. An optimal combining attack strategy against economic dispatch of integrated energy system. *IEEE Trans. Circuits Syst. II Express Briefs* **2023**, *70*, 246–250. [\[CrossRef\]](#)
51. Mohan, A.M.; Meskin, N.; Mehrjerdi, H. A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems. *Energies* **2020**, *13*, 3860. [\[CrossRef\]](#)
52. Demir, K.; Nayyer, F.; Suri, N. MPTCP-H: A DDoS attack resilient transport protocol to secure wide area measurement systems. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 84–101. [\[CrossRef\]](#)
53. Kim, Y.; Hakak, S.; Ghorbani, A. Detecting distributed denial-of-service (DDoS) attacks that generate false authentications on electric vehicle (EV) charging infrastructure. *Comput. Secur.* **2024**, *144*, 103989. [\[CrossRef\]](#)
54. Tawfiq, M. Modeling Time-Varying Wide-Scale Distributed Denial of Service Attacks on Electric Vehicle Charging Stations. *Ain Shams Eng. J.* **2024**, *15*, 102860.

55. Yan, B.; Yao, P.; Yang, T.; Zhou, B.; Yang, Q. Game-theoretical model for dynamic defense resource allocation in cyber-physical power systems under distributed denial of service attacks. *J. Mod. Power Syst. Clean Energy* **2024**, *12*, 41–51. [\[CrossRef\]](#)
56. Tawfiq, A.; Abdulaziz, A. A comprehensive survey of cyberattacks on EVs: Research domains, attacks, defensive mechanisms, and verification methods. *Def. Technol.* **2024**, *42*, 31–58.
57. Feng, Y.; Huang, R.; Zhao, W.; Yin, P.; Li, Y. A survey on coordinated attacks against cyber-physical power systems: Attack, detection, and defense methods. *Electr. Power Syst. Res.* **2025**, *241*, 111286. [\[CrossRef\]](#)
58. Xiahou, K.; Xu, X.; Huang, D.; Du, W.; Li, M. Sliding-Mode Perturbation Observer-Based Delay-Independent Active Mitigation for AGC systems against false data injection and random time-delay attacks. *IEEE Trans. Ind. Cyber-Phys. Syst.* **2024**, *2*, 446–458. [\[CrossRef\]](#)
59. Zadsar, M.; Abazari, A.; Ameli, A.; Yan, J.; Ghafouri, M. Prevention and detection of coordinated false data injection attacks on integrated power and gas systems. *IEEE Trans. Power Syst.* **2023**, *38*, 4252–4268. [\[CrossRef\]](#)
60. Zhou, B.; Ming, X.; Zang, T.; Zhang, Y.; Chen, Y.; Zhao, W. Loss assessment and vulnerability analysis of an integrated electricity natural gas system under load redistribution attack. *Adv. Eng. Sci.* **2023**, *55*, 3–13.
61. Gu, W.; Ding, S.; Lu, S.; Zhao, P.; Zou, D.; Qiu, Y.; Yu, R.; Sheng, L. Coordinated heat and power cyber-attacks with time window matching strategy. *IEEE Trans. Smart Grid* **2023**, *14*, 2747–2761. [\[CrossRef\]](#)
62. Zhang, H.; Chen, Z.; Yu, C.; Yue, D.; Xie, X.; Hancke, G.P. Event-trigger-based resilient distributed energy management against FDI and DoS attack of cyber-physical system of smart grid. *IEEE Trans. Syst. Man Cybern. Syst.* **2024**, *54*, 3220–3230. [\[CrossRef\]](#)
63. Maiti, S.; Balabhaskara, A.; Adhikary, S.; Koley, I.; Dey, S. Targeted attack synthesis for smart grid vulnerability analysis. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Copenhagen, Denmark, 26–30 November 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 2576–2590.
64. Xia, Y.; Xu, Y.; Mondal, S.; Gupta, A.K. A transfer learning-based method for cyber-attack tolerance in distributed control of microgrids. *IEEE Trans. Smart Grid* **2024**, *15*, 1258–1270. [\[CrossRef\]](#)
65. Li, H.; Lu, R.; Zhou, L.; Yang, B.; Shen, X. An efficient merkle-tree-based authentication scheme for smart grid. *IEEE Syst. J.* **2014**, *8*, 655–663. [\[CrossRef\]](#)
66. Kim, J.; Tong, L. On topology attack of a smart grid: Undetectable attacks and countermeasures. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1294–1305. [\[CrossRef\]](#)
67. Yang, T.; Xu, Z.; Zhao, J.; Zhai, F. Review on research of attack and defense methods for digitalized new power system. *Autom. Electr. Power Syst.* **2024**, *48*, 112–126.
68. Cao, P.; Ji, Y.; Ding, M.; Ni, L.; Ma, Y.; Jin, L. Research on the impact of graphite fiber attached insulator. In Proceedings of the 2022 IEEE 5th International Electrical and Energy Conference (CIEEC), Nanjing, China, 27–29 May 2022; pp. 1704–1709.
69. Wu, Y.; Chen, Z.; Dang, J.; Chen, Y.; Zhao, X.; Zha, L. Allocation of defensive and restorative resources in electric power system against consecutive multi-target attacks. *Reliab. Eng. Syst. Saf.* **2022**, *219*, 108199. [\[CrossRef\]](#)
70. Karabiber, A. Detecting and pricing nontechnical losses by using utility power meters in electricity distribution grids. *J. Electr. Eng. Technol.* **2019**, *14*, 1933–1942. [\[CrossRef\]](#)
71. Li, P.; Fu, J.; Xie, K.; Hu, B.; Wang, Y.; Shao, C.; Sun, Y.; Huang, W. A Defense planning model for a power system against coordinated cyber-physical attack. *Prot. Control Mod. Power Syst.* **2024**, *9*, 84–95. [\[CrossRef\]](#)
72. Tian, J.; Wang, B.; Li, T.; Shang, F.; Cao, K. Coordinated cyber-physical attacks considering dos attacks in power systems. *Int. J. Robust Nonlinear Control* **2020**, *30*, 4345–4358. [\[CrossRef\]](#)
73. Zhang, Z.; Deng, R.; Tian, Y.; Cheng, P.; Ma, J. SPMA: Stealthy physics-manipulated attack and countermeasures in cyber-physical smart grid. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 581–596. [\[CrossRef\]](#)
74. Li, S.; Shi, L. A tri-level optimization strategy incorporating wind power against coordinated cyber-physical attacks. *IET Gener. Transm. Distrib.* **2023**, *17*, 2228–2248. [\[CrossRef\]](#)
75. Xiang, Y.; Wang, L.; Liu, N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electr. Power Syst. Res.* **2017**, *149*, 156–168. [\[CrossRef\]](#)
76. Ren, H.; Jiang, Z.; Wu, Q.; Li, Q.; Lv, H. Optimal planning of an economic and resilient district integrated energy system considering renewable energy uncertainty and demand response under natural disasters. *Energy* **2023**, *277*, 127644. [\[CrossRef\]](#)
77. Ren, H.; Zhang, Y.; Wu, Q.; Li, Q. Research review on planning and operation dispatch of integrated energy system for resilience enhancement. *Autom. Electr. Power Syst.* **2024**, 1–16.
78. Adefarati, T.; Bansal, R.C. Reliability assessment of distribution system with the integration of renewable distributed generation. *Appl. Energy* **2017**, *185*, 158–171. [\[CrossRef\]](#)
79. Gharehveran, S.S.; Ghassemzadeh, S.; Rostami, N. Two-stage resilience-constrained planning of coupled multi-energy microgrids in the presence of battery energy storages. *Sustain. Cities Soc.* **2022**, *83*, 103952. [\[CrossRef\]](#)
80. Wang, J.-J.; Fu, C.; Yang, K.; Zhang, X.-T.; Shi, G.; Zhai, J. Reliability and availability analysis of redundant bchp (building cooling, heating and power system). *Energy* **2013**, *61*, 531–540. [\[CrossRef\]](#)

81. Nazemi, M.; Moeini-Aghtaie, M.; Fotuhi-Firuzabad, M.; Dehghanian, P. Energy storage planning for enhanced resilience of power distribution networks against earthquakes. *IEEE Trans. Sustain. Energy* **2020**, *11*, 795–806. [\[CrossRef\]](#)
82. Abdulrazzaq Oraibi, W.; Mohammadi-Ivatloo, B.; Hosseini, S.H.; Abapour, M. Multi microgrid framework for resilience enhancement considering mobile energy storage systems and parking lots. *Appl. Sci.* **2023**, *13*, 1285. [\[CrossRef\]](#)
83. Lei, S.; Wang, J.; Chen, C.; Hou, Y. Mobile emergency generator pre-positioning and real-time allocation for resilient response to natural disasters. *IEEE Trans. Smart Grid* **2018**, *9*, 2030–2041. [\[CrossRef\]](#)
84. Flôr, V.B.B.; Filho, M.B.D.C.; Souza, J.C.S.; Vergara, P.P. Critical data visualization to enhance protection schemes for state estimation. *IEEE Trans. Smart Grid* **2023**, *14*, 1249–1261. [\[CrossRef\]](#)
85. He, X.; Tu, C.; Yu, L. Measurements processing method of distribution network state estimation and anti false data injection attack strategy. *High Volt. Eng.* **2021**, *47*, 2342–2349.
86. Huang, C.; Hong, M.; Fu, S.; Deng, S. Distributed state estimation of active distribution network considering false data injection attack. *Electr. Power Eng. Technol.* **2022**, *41*, 22–31.
87. Shafie, A.E.; Chihaoui, H.; Hamila, R.; Al-Dhahir, N.; Gastli, A.; Ben-Brahim, L. Impact of passive and active security attacks on MIMO smart grid communications. *IEEE Syst. J.* **2019**, *13*, 2873–2876. [\[CrossRef\]](#)
88. Derhab, A.; Guerroumi, M.; Belaoued, M.; Cheikhrouhou, O. BMC-SDN: Blockchain-based multicontroller architecture for secure software-defined networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9984666. [\[CrossRef\]](#)
89. Yang, W.; Wan, Y.; He, J.; Cao, Y. Security vulnerabilities and countermeasures for time synchronization in TSCH networks. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1954121. [\[CrossRef\]](#)
90. Cao, P.; Liu, M. PMU placement method based on improved integer programming method combined with zero injection buses. *Power Syst. Prot. Control* **2021**, *49*, 143–150.
91. Zhou, S.; Liu, X.; Xiong, Z.; Wang, X.; Jiang, C.; Zhang, S. Line Hardening and energy storage system configuration strategies for resilience enhancement of a hybrid AC-DC distribution system. *J. Shanghai Jiaotong Univ.* **2021**, *55*, 1619.
92. Zhang, H.; Ma, S.; Chen, X.; Gong, X.; Wei, K. Distribution network energy storage planning ensuring uninterrupted power supply for critical loads. *Power Syst. Technol.* **2021**, *45*, 259–268.
93. Said, D.; Elloumi, M.; Khoukhi, L. Cyber-attack on P2P energy transaction between connected electric vehicles: A false data injection detection based machine learning model. *IEEE Access* **2022**, *10*, 63640–63647. [\[CrossRef\]](#)
94. Jafari, M.; Kavousi-Fard, A.; Sheikh, M.; Jin, T.; Karimi, M. A copula-based secured intelligent dynamic-static energy community transportation system for smart cities. *Sustain. Cities Soc.* **2024**, *107*, 105432. [\[CrossRef\]](#)
95. Xu, T.; Shao, C.; Shahidepour, M.; Wang, X. Coordinated planning strategies of power systems and energy transportation networks for resilience enhancement. *IEEE Trans. Sustain. Energy* **2023**, *14*, 1217–1229. [\[CrossRef\]](#)
96. 14th Five-Year Plan for Energy in Lin-Gang Special Area. Available online: <https://en.lingang.gov.cn/html/website/lg/English/about/14th/Industrial%20Development/1668586084997582850.html> (accessed on 20 January 2025).
97. Huang, G.; Li, G.; Xiao, Y.; Bie, Z.; Sun, S. Optimal Placement for Integrated Electricity and Gas Energy System Considering Natural Disasters and Man-made Attacks. *Power Syst. Technol.* **2021**, *45*, 959–970.
98. Kumar, R.; Mishra, S.K.; Mohanta, D.K. An integrated development environment based situational awareness for operational reliability evaluation in wind energy systems incorporating uncertainties. *Electr. Power Syst. Res.* **2024**, *233*, 110467. [\[CrossRef\]](#)
99. Lv, X.; Yang, X.; An, L.; Lin, Z. Multi-fault repair and recovery strategy for local energy internet integrated with transportation network. *Electr. Power Autom. Equip.* **2020**, *40*, 32–39.
100. Zhang, H.; Liu, Y. Comprehensive assessment of extreme ice disaster affecting power system operation available. *Proc. CSEE* **2011**, *31*, 52–58.
101. Hu, X.; Zhang, H.; Ma, D.; Wang, R. Situation awareness method using spectral analysis of random matrix for integrated energy system. *ISA Trans.* **2020**, *99*, 240–251. [\[CrossRef\]](#)
102. Liu, Y.; Hazarika, H.; Kanaya, H.; Takiguchi, O.; Murai, M.; Hidayat, M.N.; Kochi, Y. Design and deployment of an iot-based landslide early warning system. In Proceedings of the 2022 International Conference and Utility Exhibition on Energy, Environment and Climate Change (ICUE), Pattaya, Thailand, 26–28 October 2022; pp. 1–7.
103. Zhu, J.; Dai, C.; Yang, H.; Shan, Y.; Ren, J.; Liu, Y.; Li, J.; Chen, W.; Liang, J.; Ling, S. Intellisense bio-ionotronics battery for early warning of geological seepage. *ACS Sens.* **2023**, *8*, 2731–2739. [\[CrossRef\]](#) [\[PubMed\]](#)
104. Zhang, Y.; Ding, Z.; Xie, S. Construction of experimental platform for resilience enhancement of energy-transport-information integrated systems. *Exp. Technol. Manag.* **2023**, *40*, 7–13.
105. Wu, Y.; Xue, Y.; Xie, Y.; Wang, H.; Duan, R.; Huang, W. Space-time impact of typhoon and rainstorm on power grid fault probability. *Autom. Electr. Power Syst.* **2016**, *40*, 20–29+83.
106. Du, S.; Guo, C.; Yu, X.; Zhao, F.; Xin, H.; Fang, Y. Review and prospect of resilient distribution network under typhoon disaster. *Electr. Power Autom. Equip.* **2022**, *42*, 176–186+209.
107. Shahgholian, G.; Moradian, M.; Fathollahi, A. Droop Control Strategy in inverter-based microgrids: A brief review on analysis and application in islanded mode of operation. *IET Renew. Power Gener.* **2025**, *19*, e13186. [\[CrossRef\]](#)

108. Najafi Tari, A.; Sepasian, M.S.; Tourandaz Kenari, M. Resilience assessment and improvement of distribution networks against extreme weather events. *Int. J. Electr. Power Energy Syst.* **2021**, *125*, 106414. [\[CrossRef\]](#)
109. Chen, B.; Wu, Q.H.; Li, M.; Xiahou, K. Detection of false data injection attacks on power systems using graph edge-conditioned convolutional networks. *Prot. Control Mod. Power Syst.* **2023**, *8*, 16. [\[CrossRef\]](#)
110. Reda, H.T.; Anwar, A.; Mahmood, A.N.; Tari, Z. A taxonomy of cyber defence strategies against false data attacks in smart grids. *ACM Comput. Surv.* **2023**, *55*, 331:1–331:37. [\[CrossRef\]](#)
111. Liu, T.; Gu, Y.; Wang, D.; Gui, Y.; Guan, X. A novel method to detect bad data injection attack in smart grid. In Proceedings of the 2013 Proceedings IEEE INFOCOM 2013, Turin, Italy, 14–19 April 2013; pp. 3423–3428.
112. Zhao, J.; Gómez-Expósito, A.; Netto, M.; Mili, L.; Abur, A.; Terzija, V.; Kamwa, I.; Pal, B.; Singh, A.K.; Qi, J.; et al. Power system dynamic state estimation: Motivations, definitions, methodologies, and future work. *IEEE Trans. Power Syst.* **2019**, *34*, 3188–3198. [\[CrossRef\]](#)
113. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of faults and attacks including false data injection attack in smart grid using kalman filter. *IEEE Trans. Control Netw. Syst.* **2014**, *1*, 370–379. [\[CrossRef\]](#)
114. He, Y.; Zhou, C.; Zheng, N.; Zhang, W.; Xie, Y. Detection method against false data injection attack based on extended kalman filter. *Electric Power* **2017**, *50*, 35–40.
115. He, D.; Xu, C.; Lou, X. Data attack detection of connected vehicle systems based on adaptive kalman filtering. *J. Zhejiang Univ. Technol.* **2021**, *49*, 178–185.
116. Liu, X.; Chang, P.; Sun, Q. Grid false data injection attacks detection based on xgboost and unscented kalman filter adaptive hybrid prediction. *Proc. CSEE* **2021**, *41*, 5462–5476.
117. Chen, B.; Li, H.; Li, B. Application research on pseudo measurement modeling and AUKF in FDIAs identification of distribution network. *Power Syst. Technol.* **2019**, *43*, 3226–3236.
118. Liu, C.; Wu, J.; Long, C.; Kundur, D. Reactance perturbation for detecting and identifying FDI attacks in power system state estimation. *IEEE J. Sel. Top. Signal Process.* **2018**, *12*, 763–776. [\[CrossRef\]](#)
119. Zhang, Z.; Deng, R.; Yau, D.K.Y.; Cheng, P.; Chen, J. Analysis of moving target defense against false data injection attacks on power grid. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2320–2335. [\[CrossRef\]](#)
120. Zhang, H.; Liu, B.; Liu, X.; Pahwa, A.; Wu, H. Voltage stability constrained moving target defense against net load redistribution attacks. *IEEE Trans. Smart Grid* **2022**, *13*, 3748–3759. [\[CrossRef\]](#)
121. Lakshminarayana, S.; Belmega, E.V.; Poor, H.V. Moving-target defense against cyber-physical attacks in power grids via game theory. *IEEE Trans. Smart Grid* **2021**, *12*, 5244–5257. [\[CrossRef\]](#)
122. Kosut, O.; Jia, L.; Thomas, R.; Tong, L. Malicious data attacks on the smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 645–658. [\[CrossRef\]](#)
123. Wei, S.; Xu, J.; Wu, Z.; Hu, Q.; Yu, X. A false data injection attack detection strategy for unbalanced distribution networks state estimation. *IEEE Trans. Smart Grid* **2023**, *14*, 3992–4006. [\[CrossRef\]](#)
124. Tang, B.; Yan, J.; Kay, S.; He, H. Detection of false data injection attacks in smart grid under colored gaussian noise. In Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 17–19 October 2016; pp. 172–179.
125. Liu, X.; Guan, Y.; Kim, S.W. Bayesian test for detecting false data injection in wireless relay networks. *IEEE Commun. Lett.* **2018**, *22*, 380–383. [\[CrossRef\]](#)
126. Mangalwedekar, S.; Bansode, P.; Kazi, F.; Singh, N. A bayesian game-theoretic defense strategy for false data injection attacks in smart grid. In Proceedings of the 2017 14th IEEE India Council International Conference (INDICON), Roorkee, India, 15–17 December 2017; pp. 1–6.
127. Khan, M.A.; Nasralla, M.M.; Umar, M.M.; Khan, S.; Choudhury, N. An efficient multilevel probabilistic model for abnormal traffic detection in wireless sensor networks. *Sensors* **2022**, *22*, 410. [\[CrossRef\]](#) [\[PubMed\]](#)
128. Chen, L.; Li, S.; Wang, X. Quickest fault detection in photovoltaic systems. *IEEE Trans. Smart Grid* **2018**, *9*, 1835–1847. [\[CrossRef\]](#)
129. Rovatsos, G.; Jiang, X.; Domínguez-García, A.D.; Veeravalli, V.V. Statistical power system line outage detection under transient dynamics. *IEEE Trans. Signal Process.* **2017**, *65*, 2787–2797. [\[CrossRef\]](#)
130. Huang, Y.; Li, H.; Campbell, K.; Zhu, H. Defending false data injection attack on smart grid network using adaptive CUSUM test. In Proceedings of the 2011 45th Annual Conference on Information Sciences and Systems, Baltimore, MD, USA, 23–25 March 2011; pp. 1–6.
131. Li, S.; Yilmaz, Y.; Wang, X. Quickest detection of false data injection attack in wide-area smart grids. *IEEE Trans. on Smart Grid* **2015**, *6*, 2725–2735. [\[CrossRef\]](#)
132. Nath, S.; Akingeneye, I.; Wu, J.; Han, Z. Quickest detection of false data injection attacks in smart grid with dynamic models. *IEEE J. Emerg. Sel. Top. Power Electron.* **2022**, *10*, 1292–1302. [\[CrossRef\]](#)
133. Hussain, S.; Hussain, S.M.S.; Hemmati, M.; Iqbal, A.; Alammari, R.; Zanero, S.; Ragaini, E.; Gruosso, G. A novel hybrid cybersecurity scheme against false data injection attacks in automated power systems. *Prot. Control Mod. Power Syst.* **2023**, *8*, 37. [\[CrossRef\]](#)

134. Ozay, M.; Esnaola, I.; Yarman Vural, F.T.; Kulkarni, S.R.; Vincent Poor, H. Smarter security in the smart grid. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 312–317.
135. Yang, Z.; Liu, H.; Bi, T.; Yang, Q. PMU bad data detection method based on long short-term memory network. *Power Syst. Prot. Control* **2020**, *48*, 1–9.
136. He, Y.; Mendis, G.J.; Wei, J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Trans. Smart Grid* **2017**, *8*, 2505–2516. [\[CrossRef\]](#)
137. Yu, J.; Hou, Y.; Li, V. Online false data injection attack detection with wavelet transform and deep neural networks. *IEEE Trans. Industr. Inform.* **2018**, *14*, 3271–3280. [\[CrossRef\]](#)
138. Hu, C.; Yan, J.; Wang, C. Advanced cyber-physical attack classification with extreme gradient boosting for smart transmission grids. In Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019.
139. Zhang, B.; Liu, X.; Yu, Z.; Wang, W.; Jin, Q.; Li, W. Review on artificial intelligence-based network attack detection in power systems. *High Volt. Eng.* **2022**, *48*, 4413–4426.
140. Khalid, H.M.; Peng, J.C.-H. A bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks. *IEEE Trans. Smart Grid* **2016**, *7*, 2026–2037. [\[CrossRef\]](#)
141. Wang, X. Research on Malicious Data Attacks and Recognition in Energy Internet. Master's Thesis, North China Electric Power University, Beijing, China, 2023.
142. Qi, R.; Rasband, C.; Zheng, J.; Longoria, R. Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning. *Information* **2021**, *12*, 328. [\[CrossRef\]](#)
143. Wang, P.; Govindarasu, M.; Ashok, A.; Sridhar, S.; McKinnon, D. Data-driven anomaly detection for power system generation control. In Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW), New Orleans, LA, USA, 18–21 November 2017; pp. 1082–1089.
144. Zhang, Y.; Wang, J.; Chen, B. Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach. *IEEE Trans. Smart Grid* **2021**, *12*, 623–634. [\[CrossRef\]](#)
145. Mohammadpourfard, M.; Sami, A.; Seifi, A.R. A statistical unsupervised method against false data injection attacks: A visualization-based approach. *Expert Syst. Appl.* **2017**, *84*, 242–261. [\[CrossRef\]](#)
146. Zhang, Y.; Yan, J. Domain-adversarial transfer learning for robust intrusion detection in the smart grid. In Proceedings of the 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, China, 21–23 October 2019; pp. 1–6.
147. Konstantinou, C.; Maniatakos, M. A data-based detection method against false data injection attacks. *IEEE Des. Test* **2020**, *37*, 67–74. [\[CrossRef\]](#)
148. Zhao, Y.; Li, Z.; Ju, P.; Wang, C. Resilience of power system with integrated energy in context of low-carbon energy transition: Review and prospects. *Electr. Power Autom. Equip.* **2021**, *41*, 13–23+47.
149. Hategekimana, P.; Ferre, A.J.; Bernuz, J.M.R.; Ntagwirumugara, E. Fault detecting and isolating schemes in a low-voltage DC microgrid network from a remote village. *Energies* **2022**, *15*, 4460. [\[CrossRef\]](#)
150. Zhang, G.; Tong, X.; Hong, Q.; Lu, X.; Booth, C.D. A novel fault isolation scheme in power system with dynamic topology using wide-area information. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2399–2410. [\[CrossRef\]](#)
151. Esfahani, A.G.; Fani, B.; Delshad, M.; Saghafi, H. A three-stage multi-agent-based peer-to-peer method for fault isolation of high distributed generation penetrated distribution networks. *IET Renew. Power Gener.* **2023**, *17*, 1255–1266. [\[CrossRef\]](#)
152. Lv, W.; Zheng, T.; Yang, Y.; Li, R.; Sun, S. Novel fault isolation scheme under protection failure in MVDC distribution networks without DC circuit breakers. *Int. J. Electr. Power Energy Syst.* **2023**, *148*, 108901. [\[CrossRef\]](#)
153. Peng, K.; Zhang, C.; Xu, B.; Chen, Y.; Cheng, J.; Zhao, X. Key issues of fault analysis on distribution system with high-density distributed generations. *Autom. Electr. Power Syst.* **2017**, *41*, 184–192.
154. Chen, Y.; Wen, J.; Chen, T.; Ojas, P. Bayesian networks for whole building level fault diagnosis and isolation. In Proceedings of the 2018 5th International High Performance Buildings Conference, Purdue, West Lafayette, IN, USA, 9–12 July 2018; pp. 1–10.
155. Chen, Y.; Wen, J.; Pradhan, O.; Lo, L.J.; Wu, T. Using discrete bayesian networks for diagnosing and isolating cross-level faults in HVAC systems. *Appl. Energy* **2022**, *327*, 120050. [\[CrossRef\]](#)
156. Wang, Z.; Wang, L.; Tan, Y.; Yuan, J.; Li, X. Fault diagnosis using fused reference model and bayesian network for building energy systems. *J. Build. Eng.* **2021**, *34*, 101957. [\[CrossRef\]](#)
157. Kiluk, S. Algorithmic acquisition of diagnostic patterns in district heating billing system. *Appl. Energy* **2012**, *91*, 146–155. [\[CrossRef\]](#)
158. Månsson, S.; Kallioniemi, P.O.J.; Sernhed, K.; Thern, M. A machine learning approach to fault detection in district heating substations. *Energy Procedia* **2018**, *149*, 226–235. [\[CrossRef\]](#)
159. Li, M.; Deng, W.; Xiahou, K.; Ji, T.; Wu, Q. A data-driven method for fault detection and isolation of the integrated energy-based district heating system. *IEEE Access* **2020**, *8*, 23787–23801. [\[CrossRef\]](#)

160. Huang, J.; Ghalamsiah, N.; Patharkar, A.; Pradhan, O.; Chu, M.; Wu, T.; Wen, J.; O'Neill, Z.; Selcuk Candan, K. An entropy-based causality framework for cross-level faults diagnosis and isolation in building HVAC systems. *Energy Build.* **2024**, *317*, 114378. [\[CrossRef\]](#)
161. Dong, G.; He, C.; Liu, X.; Nan, L.; Liu, T.; Zhang, Y. Coordinated recovery method of post-disaster distribution network cyber-physical system considering network reconstruction and emergency resources. *Electr. Power Autom. Equip.* **2024**, *44*, 106–113.
162. Szott, M.; Werminiński, S.; Jarnut, M.; Kaniewski, J.; Benysek, G. Battery energy storage system for emergency supply and improved reliability of power networks. *Energies* **2021**, *14*, 720. [\[CrossRef\]](#)
163. Zhou, B.; Wu, J.; Zang, T.; Cai, Y.; Sun, B.; Qiu, Y. Emergency dispatch approach for power systems with hybrid energy considering thermal power unit ramping. *Energies* **2023**, *16*, 4213. [\[CrossRef\]](#)
164. Hou, H.; Tang, J.; Zhang, Z.; Wu, X.; Wei, R.; Wang, L.; He, H. Stochastic pre-disaster planning and post-disaster restoration to enhance distribution system resilience during typhoons. *Energy Convers. Econ.* **2023**, *4*, 346–363. [\[CrossRef\]](#)
165. Malek, A.F.; Mokhlis, H.; Mansor, N.N.; Jamian, J.J.; Wang, L.; Muhammad, M.A. Power distribution system outage management using improved resilience metrics for smart grid applications. *Energies* **2023**, *16*, 3953. [\[CrossRef\]](#)
166. Bustamante, R.; Mosqueda, G.; Kim, M. Enhanced seismic protection system for an emergency diesel generator unit. *Energies* **2022**, *15*, 1728. [\[CrossRef\]](#)
167. Zhou, D. China's energy emergency management system and capacity building. *Jiang-Huai Trib.* **2020**, 27–32. [\[CrossRef\]](#)
168. Ge, H.; Li, J.; Liu, H.; Cao, Y.; Yang, Z.; Yan, J. Assessing and boosting the resilience of a distribution system under extreme weather. In Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019.
169. Ameli, H.; Qadrdan, M.; Strbac, G. Value of gas network infrastructure flexibility in supporting cost effective operation of power systems. *Appl. Energy* **2017**, *202*, 571–580. [\[CrossRef\]](#)
170. Bao, Z.; Ye, Y.; Wu, L. Multi-timescale coordinated schedule of interdependent electricity-natural gas systems considering electricity grid steady-state and gas network dynamics. *Int. J. Electr. Power Energy Syst.* **2020**, *118*, 105763. [\[CrossRef\]](#)
171. Zhang, Z.; Zhou, K.; Yang, S. A post-disaster load supply restoration model for urban integrated energy systems based on multi-energy coordination. *Energy* **2024**, *303*, 132008. [\[CrossRef\]](#)
172. Wang, T.; Wang, Y.; Yu, H.; Tang, Y.; Gu, W.; Lu, Y.; Han, J. Resilience resources scheduling for new distribution system with high proportions of renewables. *Renew. Energy Resour.* **2022**, *40*, 1249–1256.
173. Wang, J.; Ge, H.; Yang, Y.; Pan, Z.; Liu, Y.; Zhao, H. Collaborative service restoration with network reconfiguration for resilience enhancement in integrated electric and heating systems. *Electronics* **2023**, *12*, 3792. [\[CrossRef\]](#)
174. Wang, Z.; Ding, T.; Jia, W.; Huang, C.; Mu, C.; Qu, M.; Shahidehpour, M.; Yang, Y.; Blaabjerg, F.; Li, L.; et al. Multi-stage stochastic programming for resilient integrated electricity and natural gas distribution systems against typhoon natural disaster attacks. *Renew. Sustain. Energy Rev.* **2022**, *159*, 111784. [\[CrossRef\]](#)
175. Jia, L.; Pannala, S.; Kandaperumal, G.; Srivastava, A. Coordinating energy resources in an islanded microgrid for economic and resilient operation. *IEEE Trans. Ind. Appl.* **2022**, *58*, 3054–3063. [\[CrossRef\]](#)
176. Brown, M.A.; Soni, A. Expert perceptions of enhancing grid resilience with electric vehicles in the united states. *Energy Res. Soc. Sci.* **2019**, *57*, 101241. [\[CrossRef\]](#)
177. Wei, J.; Gao, X.; Cheng, P.; Fu, W.; Zeng, H. Coordinated post-disaster recovery and assessment method for integrated electricity-gas-transportation system. *IEEE Access* **2023**, *11*, 11685–11699. [\[CrossRef\]](#)
178. Zhao, P.; Li, S.; Hu, P.J.-H.; Cao, Z.; Gu, C.; Xie, D.; Zeng, D.D. Coordinated cyber security enhancement for grid-transportation systems with social engagement. *IEEE Trans. Emerg. Top. Comput. Intell.* **2022**, *8*, 3199–3213. [\[CrossRef\]](#)
179. Zang, T.; Liu, Y.; Wang, S.; Xiao, Y.; Wang, Z.; Zhou, B. Multi-period maintenance and restoration collaborative strategy for cyber physical distribution system considering fault propagation effect. *Electr. Power Autom. Equip.* **2024**, *44*, 247–256.
180. Pang, K.; Wang, Y.; Wen, F.; Wang, C.; Zhao, J.; Liu, Y. Cyber-physical collaborative restoration strategy for power transmission system with communication failures. *Autom. Electr. Power Syst.* **2021**, *45*, 58–67.
181. Ti, B.; Zhang, C.; Liu, J.; Wu, Z.; Huang, Z. Cyber-physical collaborative restoration strategy for power transmission system considering maintenance scheduling. *CSEE J. Power Energy Syst.* **2024**, *10*, 1331–1341.
182. Liu, Y.; Feng, H.; Hatziargyriou, N.D. Multi-stage collaborative resilient enhancement strategy for coupling faults in distribution cyber physical systems. *Appl. Energy* **2023**, *348*, 121560. [\[CrossRef\]](#)
183. Liu, X.; Ding, L.; Zhen, T.; Wu, J.; Li, Y. Analysis of cyber attack traceback techniques from the perspective of network forensics. *J. Softw.* **2021**, *32*, 194–217.
184. Nizam, S.A.S.; Ibrahim, Z.-A.; Rahim, F.A.; Fadzil, H.S.; Abdullah, H.I.M.; Mustaffa, M.Z. Forensic analysis on false data injection attack on IoT environment. *Int. J. Adv. Comput. Sci. Appl. IJACSA* **2021**, *12*, 265–271. [\[CrossRef\]](#)
185. Dosiek, L. Extracting electrical network frequency from digital recordings using frequency demodulation. *IEEE Signal Process. Lett.* **2015**, *22*, 691–695. [\[CrossRef\]](#)

186. Berjawi, A.E.H.; Walker, S.L.; Patsios, C.; Hosseini, S.H.R. An evaluation framework for future integrated energy systems: A whole energy systems approach. *Renew. Sustain. Energy Rev.* **2021**, *145*, 111163. [\[CrossRef\]](#)
187. Huang, X. A data-driven WSN security threat analysis model based on cognitive computing. *J. Sens.* **2022**, *2022*, 5013905. [\[CrossRef\]](#)
188. Ma, H.; Wang, Y.; He, M. Collaborative optimization scheduling of resilience and economic oriented islanded integrated energy system under low carbon transition. *Sustainability* **2023**, *15*, 15663. [\[CrossRef\]](#)
189. De La Torre Parra, G.; Rad, P.; Choo, K.-K.R. Implementation of deep packet inspection in smart grids and industrial internet of things: Challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 32–46. [\[CrossRef\]](#)
190. Cui, Y.; Zhang, H.; Zhong, W. Day-ahead scheduling considering participation of price-based demand response and CSP plant in wind power accommodation. *Power Syst. Technol.* **2020**, *44*, 183–191.
191. Dong, Y.; Wang, Q.; Cao, J. Identification of false data injection attacks in power grid based on oversampling and cascade machine learning. *Autom. Electr. Power Syst.* **2023**, *47*, 179–188.
192. Correa-posada, C.; Sánchez-martín, P. Integrated power and natural gas model for energy adequacy in short-term operation. *IEEE Trans. Power Syst.* **2015**, *30*, 3347–3355. [\[CrossRef\]](#)
193. Anand, H.; Narang, N.; Dhillon, J. Multi-objective combined heat and power unit commitment using particle swarm optimization. *Energy* **2019**, *172*, 794–807. [\[CrossRef\]](#)
194. Zhou, S.; Hu, Z.; Gu, W. Combined heat and power system intelligent economic dispatch: A deep reinforcement learning approach. *Int. J. Electr. Power Energy Syst.* **2020**, *120*, 106016. [\[CrossRef\]](#)
195. Qu, K.; Zhang, X.; Yu, T. Knowledge transfer based Q-learning algorithm for optimal dispatch of multi-energy system. *Autom. Electr. Power Syst.* **2017**, *41*, 18–25.
196. Liu, F.; Bie, Z.; Wang, X. Day-ahead dispatch of integrated electricity and natural gas system considering reserve scheduling and renewable uncertainties. *IEEE Trans. Sustain. Energy* **2019**, *10*, 646–658. [\[CrossRef\]](#)
197. Zhang, B.; Hu, W.; Cao, D. Deep reinforcement learning-based approach for optimizing energy conversion in integrated electrical and heating system with renewable energy. *Energy Convers. Manag.* **2019**, *202*, 112199. [\[CrossRef\]](#)
198. Ye, Y.; Qiu, D.; Wu, X. Model-free real-time autonomous control for a residential multi-energy system using deep reinforcement learning. *IEEE Trans. Smart Grid* **2020**, *11*, 3068–3082. [\[CrossRef\]](#)
199. Chen, H.; Kou, Y.; Zhou, L. Collaborative optimal dispatching mode and mechanism of watershed-type wind-solar-water multi-energy complementary bases for clean energy absorption. *Electr. Power Autom. Equip.* **2019**, *39*, 61–70.
200. Li, J.; Zhu, M.; Lu, Y.; Huang, Y.; Wu, T. Review on optimal scheduling of integrated energy systems. *Power Syst. Technol.* **2021**, *45*, 2256–2272.
201. Zeng, Q.; Fang, J.; Chen, Z.; Conejo, A.J. A two-stage stochastic programming approach for operating multi-energy systems. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017; pp. 1–6.
202. Guo, Z.; Li, G.; Zhou, M.; Feng, W. Two-stage robust optimal scheduling of regional integrated energy system considering network constraints and uncertainties in source and load. *Power Syst. Technol.* **2019**, *43*, 3090–3100.
203. Alabdulwahab, A.; Abusorrah, A.; Zhang, X.; Shahidehpour, M. Coordination of interdependent natural gas and electricity infrastructures for firming the variability of wind energy in stochastic day-ahead scheduling. *IEEE Trans. Sustain. Energy* **2015**, *6*, 606–615. [\[CrossRef\]](#)
204. Qadrdan, M.; Wu, J.; Jenkins, N.; Ekanayake, J. Operating strategies for a GB integrated gas and electricity network considering the uncertainty in wind power forecasts. *IEEE Trans. Sustain. Energy* **2014**, *5*, 128–138. [\[CrossRef\]](#)
205. Li, Y.; Liu, W.; Shahidehpour, M.; Wen, F.; Wang, K.; Huang, Y. Optimal operation strategy for integrated natural gas generating unit and power-to-gas conversion facilities. *IEEE Trans. Sustain. Energy* **2018**, *9*, 1870–1879. [\[CrossRef\]](#)
206. Wu, G.; Liu, J.; Xiang, Y.; Sheng, X.; Ma, Y. Day-ahead optimal scheduling of integrated electricity and natural gas system with medium- and long-term electricity contract decomposition and wind power uncertainties. *Electr. Power Autom. Equip.* **2019**, *39*, 246–253.
207. Wang, C.; Gao, R.; Wei, W.; Shafie-khah, M.; Bi, T.; Catalão, J.P.S. Risk-based distributionally robust optimal gas-power flow with wasserstein distance. *IEEE Trans. Power Syst.* **2019**, *34*, 2190–2204. [\[CrossRef\]](#)
208. Mitridati, L.; Pinson, P. Optimal coupling of heat and electricity systems: A stochastic hierarchical approach. In Proceedings of the 2016 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Beijing, China, 16–20 October 2016; pp. 1–6.
209. Good, N.; Karangelos, E.; Navarro, A.; Mancarella, P. Optimization Under Uncertainty of Thermal Storage-Based Flexible Demand Response With Quantification of Residential Users' Discomfort. *IEEE Trans. Smart Grid* **2015**, *6*, 2333–2342. [\[CrossRef\]](#)
210. Shui, Y.; Liu, J.; Gao, H.; Huang, S.; Jiang, Z. A distributionally robust coordinated dispatch model for integrated electricity and heating systems considering uncertainty of wind power. *Proc. CSEE* **2018**, *38*, 7235–7247+7450.

211. Noor, M.; Jolan, R. A systematic review of ultra-lightweight encryption algorithms. *Int. J. Nonlinear Anal. Appl.* **2022**, *13*, 3825–3851.
212. Zhu, L.; Peng, L.; Han, H.; Bao, X.; Gang, W.; Hou, Z.; Xu, M. Research on the Security of Unified Communications System's Applications in the Power System. In Proceedings of the 2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), Changsha, China, 26–29 November 2015; pp. 2475–2479.
213. Sun, W.; Sun, H.; He, J.; Tu, J.; Zhang, G. Review of power system resilience assessment techniques for severe natural disasters. *Power Syst. Technol.* **2024**, *48*, 129–139.
214. Quan, M.; Chen, Y. Analysis of evaluation system & mode of overseas resilient city. *Hous. Sci.* **2019**, *39*, 1–6.
215. Chen, X.; Fan, Y.; Gong, X. Study on comprehensive evaluation index system for disaster prevention of urban ice-resistant secure power grid. *Power Syst. Technol.* **2019**, *43*, 3808–3815.
216. Wang, J.; Yao, J.; Liu, Z.; Ouyang, J.; Xiong, X. Fault statistical analysis and probability distribution fitting for a power distribution network in adverse weather conditions. *Power Syst. Prot. Control* **2022**, *50*, 143–153.
217. Li, Y.; Wang, Z.; Zhao, Q. Distributed fault section location for ADN based on bayesian complete analytic model and multi-factor dimension reduction. *Power Syst. Technol.* **2021**, *45*, 3917–3925.
218. Li, X.; Sun, T.; Hou, K.; Jiang, T.; Chen, H.; Li, G.; Jia, H. Evaluating resilience of island integrated energy systems with earthquake. *Proc. CSEE* **2020**, *40*, 5476–5493.
219. Zhang, H.; Wang, P.; Yao, S.; Liu, X.; Zhao, T. Resilience assessment of interdependent energy systems under hurricanes. *IEEE Trans. Power Syst.* **2020**, *35*, 3682–3694. [[CrossRef](#)]
220. Peng, H.; Hu, L.; Tan, M.; Li, J.; Su, Y. Decision-making method for electricity-gas region integrated energy system security correction based on deep reinforcement learning. *Power Syst. Technol.* **2024**, *48*, 1019–1029.
221. Chen, L.; Deng, X.; Chen, H.; Shi, J. Review of the assessment and improvement of power system resilience. *Power Syst. Prot. Control* **2022**, *50*, 11–22.
222. Zhao, Q.; Du, Y.; Zhang, T. Resilience index system and comprehensive assessment method for distribution network considering multi-energy coordination. *Inter. Journal Elect. Power Energy Syst.* **2021**, *133*, 107211. [[CrossRef](#)]
223. Bajpai, P.; Chanda, S.; Srivastava, A. A novel metric to quantify and enable resilient distribution system using graph theory and Choquet integral. *IEEE Trans. Smart Grid* **2018**, *9*, 2918–2929. [[CrossRef](#)]
224. Peng, H.; Li, C.; Liu, J.; Su, Y.; Tan, M. Resilience assessment of electricity-gas regional integrated energy system based on heterogeneous interdependent network. *Power Syst. Technol.* **2021**, *45*, 2811–2820.
225. Wang, H.; Hou, K.; Liu, X.; Yu, X.; Jia, H.; Du, J. Resilience enhancement method for electricity-gas interconnection system based on global sensitivity analysis. *Autom. Electr. Power Syst.* **2023**, *47*, 59–67.
226. Nan, C.; Sansavini, G. A quantitative method for assessing resilience of interdependent infrastructures. *Reliab. Eng. Syst. Safe.* **2017**, *157*, 35–53. [[CrossRef](#)]
227. Bie, C.; Lin, C.; Li, G.; Qiu, A. Development and prospect of resilient power system in the context of energy transition. *Proc. CSEE* **2020**, *40*, 2735–2745.
228. Huang, W.; Wu, J.; Guo, Z. Power grid resilience assessment and differentiated planning against typhoon disasters. *Autom. Electr. Power Syst.* **2023**, *47*, 84–91.
229. Huang, Y. Resilience Assessment and Improvement Strategy Analysis of Multi-Agent and Decentralized Decisionmaking Energy Interconnection System. Master's Thesis, North China Electric Power University, Beijing, China, 2022.
230. Cui, H.; Xue, T.; Wang, Q.; Tang, Y. The Poisoning Attack and Detection Schemes for AI Algorithms in Power Systems. *Power Syst. Technol.* **2024**, *48*, 5024–5033.
231. Zhou, B.; Cai, Y.; Zang, T.; Wu, J.; Li, X.; Dong, S. Reliability optimization method for gas-electric integrated energy systems considering cyber-physical interactions. *Energies* **2023**, *16*, 5187. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.