energies

MDPI

Review

Current Status and Perspective of Vulnerability Assessment of Cyber-Physical Power Systems Based on Complex Network Theory

Tianlei Zang [1,2], Zian Wang [1,2], Xiaoguang Wei [3,*], Yi Zhou [1,2], Jiale Wu [1,2] and Buxiang Zhou [1,2]

[1] College of Electrical Engineering, Sichuan University, Chengdu 610065, China
[2] Intelligent Electric Power Grid Key Laboratory of Sichuan Province, Sichuan University, Chengdu 610065, China
[3] School of Electrical Engineering, Southwest Jiaotong University, Chengdu 611756, China
* Correspondence: wei_xiaoguang@126.com

Abstract: The increasing factors of uncertainty faced by the system are due to the deep coupling of the electric power cyber network and the physical network. Consequently, ensuring the efficient, secure, and stable operation of the cyber–physical power system (CPPS) has become a key concern. To achieve this, vulnerability assessment plays a crucial role, as it identifies and protects the vulnerable points of the system. The application of complex network theory to assess the vulnerability of CPPSs has garnered significant attention from scholars. This paper delves into the research connotation of vulnerability assessment for CPPSs, starting with the origin, definition, and classification of vulnerability. Subsequently, the assessment framework of vulnerability based on complex network theory is presented, and the status of current domestic and international research in this field is summarized. Furthermore, the interrelationship between system vulnerability and cascading failures is analyzed from the perspective of complex network theory. In conclusion, the ideas of CPPS coupling modeling in vulnerability assessment are summarized, the concept of situation awareness is introduced, and a prospective approach for dynamic vulnerability assessment is proposed. This approach is based on situation awareness combined with complex network theory. Security protection and optimal operation of CPPSs based on vulnerability assessment are also discussed, along with the assessment of vulnerability within integrated energy cyber–physical systems (IECPSs).

Keywords: vulnerability assessment; cyber–physical power systems; complex network theory; cascading failures

Citation: 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. https://doi.org/10.3390/en16186509

Academic Editor: Mohamed Benbouzid

Received: 22 August 2023
Revised: 5 September 2023
Accepted: 7 September 2023
Published: 9 September 2023

1. Introduction

1.1. Motivation

In recent years, a gradual deepening of the transformation of energy production and consumption from fossil energy to clean energy has been observed. This has led to a continuous increase in the proportion of new energy generation, including centralized and distributed solar and wind energy connected to the grid on a large scale. Additionally, there has been a growing expansion of electricity demand due to the gradual increase in the proportion of user-level electricity replacement consumption. This includes electrification of rail transportation, green ports, civil cooling and heat pumps, and other similar applications. Moreover, there has been a rise in the number of prosumers [1,2], who contribute to the grid through the development of traditional user microgeneration facilities such as on-house solar panels and microwind turbines. This, along with an increase in user autonomy in electricity consumption, further complicates the adaptation of the grid that was originally built on the vertical operation principle to accommodate the ongoing energy transition. Simultaneously, the emergence of smart grids [3] has been facilitated by the development of wireless sensing technology, communication technology, and internet

technology. In contrast to the traditional grid, the smart grid showcases a high degree of integration of energy, information, service, and value flows [4,5]. Therefore, a transformation is underway, gradually turning the smart grid into a multidimensional heterogeneous complex system, wherein the integration of the power physical system and cyber system gives rise to a cyber–physical power system [6]. Relying on advanced communication technology, CPPS aims to enhance the operational efficiency and reliability of the power system. However, this high degree of physical cyber coupling creates conditions that allow faults to propagate across the system, rendering the grid vulnerable to cascading failures during extreme conditions and leading to increased susceptibility [7]. Moreover, in the context of the rapid development of the global energy internet, grid interconnection has emerged as the future trajectory for power grids worldwide. Although grid interconnection facilitates the implementation of global integrated development strategies and fosters a global economic community of shared destiny, the extensive interconnection simultaneously imposes greater demands on grid operations and has the potential to amplify the overall or local vulnerability of the grid.

As a matter of fact, all research subjects essentially possess some degree of vulnerability, ranging from individuals and organizations to large systems, each having their own vulnerabilities (critical points). These vulnerabilities, when targeted and exploited, result in various degrees of adverse impact (e.g., performance degradation, structural damage, and loss of function). As a result, identifying the vulnerability of research subjects (i.e., vulnerability assessment) has found extensive application across diverse disciplines in social and natural sciences, including politics and the economy [8,9], ecology and the environment [10,11], information security [12,13], and transportation [14,15].

1.2. Necessity

In recent years, significant changes in the power supply landscape worldwide have introduced a variety of threats that pose risks to the safe and stable operation of the power system. Traditional natural disasters such as lightning strikes, floods, earthquakes, and snowstorms, along with occasional accidents involving component failures, protection failures, and personnel malfunctions, continue to pose challenges. However, new threats are progressively emerging, such as malicious attacks on the power grid, including terrorist attacks and cyberattacks [16–18]. These new threats exploit the system's most vulnerable aspects, leading to cascading failures and widespread outages. In such cases, the damaged components prove difficult to repair within a short timeframe, sometimes resulting in prolonged power outage situations. The consequences extend beyond the power system alone, affecting other critical infrastructure such as water treatment, transportation, and health services, leading to severe harm to the entire society. For instance, the 2003 U.S. blackout affected 50 million people and resulted in a loss of 62 million kilowatts of load, leading to socioeconomic losses of up to USD 10 billion [19]. The 2010 Iranian nuclear power plant seismic network virus incident demonstrated how cyberattacks can cause the failure of CPPS [20]. In 2011, the southwestern United States and northern Mexico experienced a 12 h blackout due to line overloads, incurring a direct economic loss of USD 118 million [21]. In 2012, a line trip in the Indian grid led to grid oscillations and a massive outage affecting more than 600 million people [22]. The 2015 Ukraine blackout, caused by a cyberattack, resulted from hackers sending phishing emails to power company employees, ultimately leading to the failure of 30 substations and a massive power outage affecting one and a half million Ukrainian residents [23]. Moreover, in 2016, the impact of a strong typhoon caused a large number of off-grid turbines in the South Australian grid to fail, resulting in a network-wide collapse and a load loss of 1.83 million kW [24]. On 7 March 2019, a cyberattack on Venezuela's largest hydroelectric power plant, Simón Bolívar, triggered a major blackout in 22 states, including the capital city of Caracas. After restoring 40% of the power, the power plant experienced an explosion, further hindering the power restoration process. The progression of these outages often results from the failure of one

component, especially in the context of deliberate attacks, which then initiates a chain reaction of failures in other components.

Therefore, in the context of energy transition and the progressive development and adoption of CPPSs, an escalating number of threats is being encountered by the system, making the efficient, secure, and stable operation of the power grid a critical issue for power infrastructure. The identification and mitigation of vulnerabilities within CPPSs, which hold significant practical significance in preventing large-scale grid outages, is fundamental to addressing this concern.

1.3. Organization

The present paper is structured as follows: An overview of the research content of CPPS vulnerability assessment is provided in Section 2, including the definition of vulnerability assessment; a discussion of distinctions between vulnerability, risk, reliability, and resilience; and several classifications of vulnerability assessment. The research framework for CPPS vulnerability assessment, which includes an analysis of the feasibility of complex network theory in CPPS vulnerability assessment and a discussion summarizing the general steps involved in CPPS vulnerability assessment, is introduced in Section 3. An overview of the current status of CPPS vulnerability assessment based on complex network theory is presented in Section 4, covering both structural and operational aspects. The relationship between system vulnerability and cascade failures is analyzed in Section 5. A prospect on CPPS vulnerability assessment based on complex network theory is provided in Section 6 within the context of considering multistage coordinated cyber–physical attacks and incorporating situation awareness. Finally, the paper is concluded in Section 7. This review aims to summarize the existing research topic and framework of CPPS vulnerability assessment and provide prospects for future research and applications.

2. The Connotation of CPPS Vulnerability Assessment Research

2.1. The Definition of CPPS Vulnerability Assessment

In CPPSs, vulnerability research is a necessity and holds significance as an extension of the concept of system security [25–27]. On the one hand, with the continuous expansion of the power grid's scale, its spatial distribution has become increasingly extensive, rendering it challenging to effectively monitor and provide real-time protection. Consequently, the power grid becomes more susceptible to extreme events compared to other components within the power system. On the other hand, from the analysis of past cascading outage events, the importance of the coupling relationship between cyber nodes and physical nodes within the power grid, as well as the complexity of the fault cascade relationship between components, has been evident. Failures of cyber nodes (such as dispatch centers, communication routing, and data acquisition equipment) and physical components (including transmission branches, protection, and communication equipment) have emerged as crucial factors contributing to system cascading outage events [7,18,28].

To date, power system vulnerability has been extensively studied; however, a precise and rigorous definition has not yet been established. In 1994, the concept of vulnerability was first introduced into the dynamic security assessment of power systems in [29,30]. This involved using the system's physical parameters to construct a security assessment framework. Subsequently, the concept of vulnerability underwent further expansion, and [26] defined power system vulnerability as the evaluation or measurement of the impact of uncertain internal and external factors (e.g., hidden failures of protection [31,32], deliberate attacks [33,34], natural disasters [35,36]) on the system for potential large outages. Vulnerability assessment research methods are systematically described from the perspective of major outages in [37]. These studies and definitions demonstrate that the primary purpose of vulnerability assessment is to evaluate the negative consequences of potential threat factors on the system [38]. These negative consequences represent low-probability, high-risk impacts on the system, such as a major system outage. However, the potential threat factors lack a clear definition, leading to

confusion between vulnerability assessment and other security assessments (especially risk assessment). Regarding potential threat factors in vulnerability assessment, in 2002, the U.S. Department of Energy published a report on vulnerability assessment methods for electric power infrastructure [39]. The report's introduction emphasizes that vulnerability assessment is particularly concerned with terrorist attacks. Additionally, many studies in the literature focus on high-threat events, particularly deliberate attacks, as the key threat factors in vulnerability assessment. Hence, from the summary and analysis of the literature, it is evident that vulnerability is an inherent property of the system and that the essence of vulnerability research is to identify potential vulnerabilities of the system at the system level under specific conditions. This process aims to reveal the extent of damage to the system's operation resulting from these vulnerabilities. The specific conditions are as follows:

- Its triggers are high threat, such as deliberate attacks and extreme weather.
- The consequences of events with low probability and high risk include system destabilization, major power outages, and severe structural damage.
- Its assessment is negative, which is a relative measure of the degree of damage to the system.

Importantly, vulnerability is studied at the system level, with a specific focus on the threat level posed by vulnerabilities to the system. Consequently, factors such as the vulnerability characteristics of the vulnerability point itself, as well as whether and when the vulnerability point is attacked, are not related to the system and are not part of the system vulnerability assessment study.

2.2. The Difference between Vulnerability and Risk, Reliability, and Resilience

In CPPS security assessment, vulnerability, risk, reliability, and resilience represent inherent properties of a system that persist despite changes in external conditions. However, these four properties are assessed with distinct focuses [40]. In this paper, the dissimilarity between vulnerability and risk, reliability, and resilience is identified in five aspects: predisposing factors I, assessment results R, operational state S, time scale T, and statistical probability P.

Predisposing factors I: a source event that causes a loss of system functionality or structural damage. Source events include high-threat I_H and low-threat I_L events, i.e., $I = I_H \cup I_L$.

Assessment results R: evaluate the performance or characteristics of the system structure or function. The system function mainly refers to the power supply (outage) performance of the system R_B, i.e., $R_B \subset R$.

Operational state S: This includes the normal operating state of the system S_N (including before and after recovery) and the fault operating state S_F, i.e., $S_N \cup S_F$.

Time scale T: the triggers, the operational state of the system, or the duration (or the time of occurrence) of the system performance.

Statistical probability P: statistical probability of occurrence of predisposing factors and assessed results.

With the above definition, (I, R, S, T, P) is used to describe the four CPPS security assessment terms. As analyzed in 1.1.2, in the power system vulnerability assessment, the consequences of system vulnerability points on the system under high-threat events are mainly studied, as shown in Equation (1):

$$(S_F, P(R), R/I_H) \tag{1}$$

where $P(R)$ indicates that the assessment result R is a probabilistic statistical value, and R/I_H indicates the system assessment result under a high-risk event. The vulnerability assessment is independent of the time scale, and the assessment result is a probabilistic statistical value.

2.2.1. The Difference between Vulnerability and Risk

At the system level, risk assessment has not yet been strictly defined; however, the literature commonly characterizes it as a composite measure of the probable consequences resulting from the occurrence of uncertainties faced by the CPPS [41,42]. This can be expressed as Equation (2):

$$(S_F, P(R), R/I) \tag{2}$$

As observed from the definition, risk assessment encompasses a broader scope than vulnerability assessment, and the main differences are as follows:

- Regarding predisposing factors, all uncertainties are considered in risk assessment, whereas vulnerability assessment focuses solely on high-threat factors.
- Event consequences are the subject of risk assessment studies, encompassing events that can have a negative impact on the system. In contrast, vulnerability assessments concentrate on events characterized by severe negative impacts.

In summary, vulnerability assessment is considered narrower in scope compared to risk assessment and can be seen as a special case of risk assessment [43]. Furthermore, as the system's vulnerability increases, its level of risk also escalates.

2.2.2. The Difference between Vulnerability and Reliability

Reliability is defined as the measure of a power system's capability to consistently and uninterruptedly supply electricity and power to customers at an acceptable standard and in the required quantity [44]. Essentially, it focuses on the efficient provision of electrical energy to meet customer demand [45]. CPPS reliability encompasses two primary aspects: adequacy and security. Adequacy assesses the system's ability to maintain a continuous supply of electrical energy and meet customer demand under static conditions, whereas security evaluates its capacity to withstand sudden disturbances and provide uninterrupted electrical energy to customers under dynamic conditions [46]. By combining these two aspects, the reliability index can be expressed as Equation (3):

$$(S, T(I, R_B), P(I, R_B), R_B/I) \tag{3}$$

where $T(I, R_B)$ represents the duration (occurrence) of the triggers and the system to maintain power supply, and $P(I, R_B)$ represents both the triggers and the assessment results as a probability statistic (model). From the definition, vulnerability and reliability are fundamentally different, and the main differences are as follows:

- Regarding the predisposing factors, reliability necessitates attention to both the duration (occurrence) and the probability of occurrence of these factors. These factors can be diverse, considering not only uncertainties but also certainties, such as planned outages of components and reasonably expected unplanned outages [44]. In contrast, vulnerability does not concern itself with the duration and probability of the predisposing events, as these factors are inherently uncertain. Additionally, reliability, in general, places more emphasis on high-probability and low-impact events [47].
- The assessment results differ for reliability and vulnerability. Reliability solely concentrates on the system's continuous-time metric of continuously supplying power, whereas vulnerability encompasses all time-independent metrics related to negative structural and functional aspects.
- In relation to operating states, both normal and fault operating states are considered in reliability assessment, with the fault operating state commonly regarded as an $N-1$ criterion [48]. Conversely, vulnerability assessment focuses on evaluating the system specifically in the fault operating state.

2.2.3. The Difference between Vulnerability and Resilience

The definition of resilience, as a novel assessment concept in the power system, is still a subject of academic consideration [49]. Nonetheless, several organizations (e.g., UK Energy

Research Center [50], National Infrastructure Advisory Council [51]), along with expert scholars, regard resilience as a characteristic of the grid's capability to prevent, absorb, respond, and recover rapidly when confronted with high-threat events [52,53]. This can be described by Equation (4):

$$(S, T(I_H, R_B, S_F \rightarrow S_N), P(I_H, R_B), R_B / I_H) \quad (4)$$

where the high-threat factor and the duration (occurrence) of maintaining the power supply and the time taken to recover from the failed operating state to the normal operating state, are denoted by $T(I_H, R_B, S_F \rightarrow S_N)$. From the definition, it is evident that vulnerability and resilience assess system performance from different perspectives, and the main differences are as follows:

- Regarding predisposing factors, although both vulnerability and resilience concentrate on high-threat factors, resilience is similar to reliability in that it considers the duration or occurrence time of high-threat factors (e.g., extreme weather [54]) to some extent [17,55].
- In relation to the assessment results, resilience and vulnerability differ. Resilience, unlike vulnerability, not only focuses on the system's ability to continuously power itself but also takes into account the time it takes for the system to recover from a failure to its prefailure operational state [52]. This measurement involves continuous time. Additionally, vulnerability can, to some extent, indicate the system's resilience ability [56]. As shown in Figure 1, when the power grid encounters a disturbance event, vulnerability affects the severity of the system damage, and when the losses reach a certain level, it becomes challenging for the system to return to a normal state. In other words, if the system exhibits greater vulnerability, disturbances can propagate rapidly and extensively within the system (as discussed in Section 5), resulting in difficulties in recovery. This implies that the system possesses lower resilience.
- Regarding the operating state, resilience takes into consideration the system operating state before, during, and after the failure, whereas vulnerability solely measures the system's performance during the failed operating state.

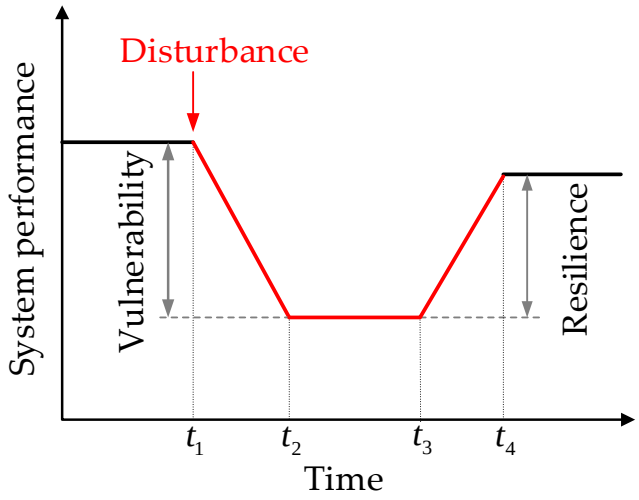

Figure 1. Performances of CPPSs that are resilient under disruptive events.

2.3. Classification of Vulnerability Assessment

2.3.1. Structural Vulnerability and Operational Vulnerability

From the perspective of the system's structural and operational characteristics, vulnerability assessment can be divided into structural vulnerability [57] and operational vulnerability [58]. Structural vulnerability assessment analyzes the impact of vulnerable points in the system's topology on the system's operational state and the grid characteristics of its physical structure. On the other hand, operational vulnerability assessment primarily

analyzes the impact on the system's operational state caused by changes in its physical or operational characteristics when the vulnerable points are disturbed or fail.

To illustrate the difference between the two, consider the analogy of a cup and water, as shown in Figure 2. In this analogy, the cup represents the system's topology, and the water in the cup represents the system's operating state. The system's operating state is heavily influenced by its structure, analogous to the height of the water surface in the figure (although factors such as generators and loads also play a role in determining the system's operating state). The cracks on the cup represent the vulnerable points of the system.

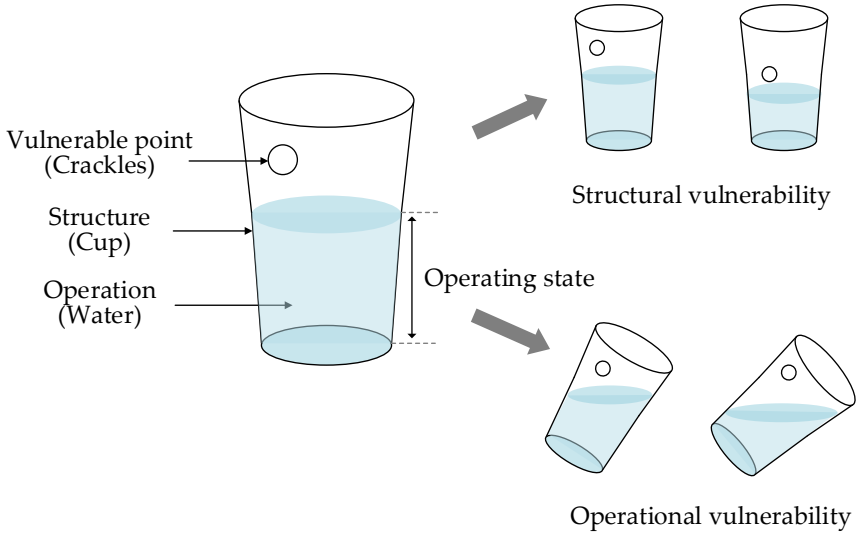

Figure 2. Differences between structural vulnerability and operational vulnerability.

In structural vulnerability assessment, the analysis primarily focuses on the impact of the vulnerable points in the structure on the system's operational state, i.e., the influence of structural characteristics (robustness) on the operational state. The locations of the different cracks in the figure correspond to the height of the water surface. On the other hand, in operational vulnerability assessment, the vulnerable points affect the system's structural properties, leading to changes in both the physical and the operational properties of the system. Analogously, the cup in the figure undergoes rotation. Therefore, operational vulnerability assessment is a comprehensive assessment that considers all system characteristics.

It is important to note that, on the one hand, in topological vulnerability assessment, the operational state serves as the foundation for structural vulnerability assessment, and the latter would lack significance without considering the operational state in the system. On the other hand, in operational vulnerability assessment, the physical, operational, and structural properties of the system are interdependent, resulting in an integration of the physical, operational, and structural properties. Therefore, the physical, operational, and structural characteristics are integrated into the assessment process.

2.3.2. Spontaneous and Forcible Disturbance Vulnerability

Regarding disturbance characteristics, as depicted in Figure 3, vulnerability assessment can be subdivided into two categories: spontaneous disturbance vulnerability assessment and forcible disturbance vulnerability assessment.

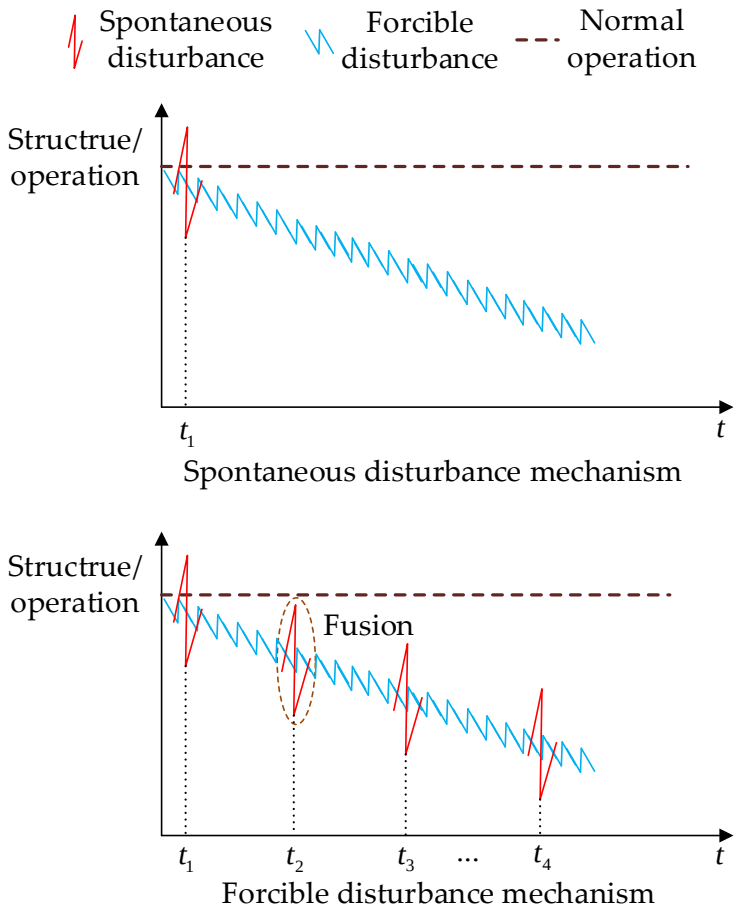

Figure 3. Differences between spontaneous disturbance and forcible disturbance.

In spontaneous disturbances, the system experiences source events (comprising external factors such as severe weather or natural disasters and internal factors such as protection malfunctions) that cause its operational deterioration [59], thus exceeding its tolerable range (branch overload, heavy load). Subsequently, this triggers successive failures of the system components [60], ultimately leading to system collapse and a major outage. Therefore, in spontaneous disturbance vulnerability assessment, a system-level perspective places more emphasis on understanding how failures propagate between components, indirectly leading to a chain collapse of the system. Essentially, greater attention is given to the intrinsic mechanism of fault propagation at the vulnerable points in the system's fault evolution [61].

In forcible disturbance vulnerability assessment, the primary focus lies in studying the extent of damage that is possibly caused to the system's functionality or structure after a deliberate attack on the vulnerable point (such as cyberattacks or physical damage) [62,63]. In CPPS, attacks on the cyber layer are stealthy, efficient, and destructive, allowing attackers to use fewer resources while causing significant damage. As the structure and function of the complete power grid are generally predetermined, its topology remains fixed. This enables attackers to intentionally identify and target vulnerable points in the physical system of power information. Deliberate attacks on vulnerable points typically result in more severe damage [64]. Although nonspontaneous perturbations may accompany spontaneous perturbations, vulnerability assessment primarily concerns the direct impact of the vulnerable points on the system's function or structure.

2.3.3. Impactability Vulnerability and Susceptibility Vulnerability

Regarding the failure mechanism, vulnerability assessment can be categorized into susceptibility to impactability vulnerability assessment and susceptibility vulnerability as-

sessment [65,66], as illustrated in Figure 4. Impactability vulnerability refers to a vulnerable point in the system being prone to propagating the failure to other components when it fails, whereas susceptibility vulnerability denotes a vulnerable point being susceptible to the failure itself. Elaborating on these two vulnerability characteristics helps unveil the essence of system blackouts. On the one hand, impactable points are inclined to spread faults within the system, which to some extent determines the breadth of the system collapse. On the other hand, susceptible points are susceptible to the propagation of faults, which further exacerbates the system collapse and influences the depth of the system collapse to a certain extent.

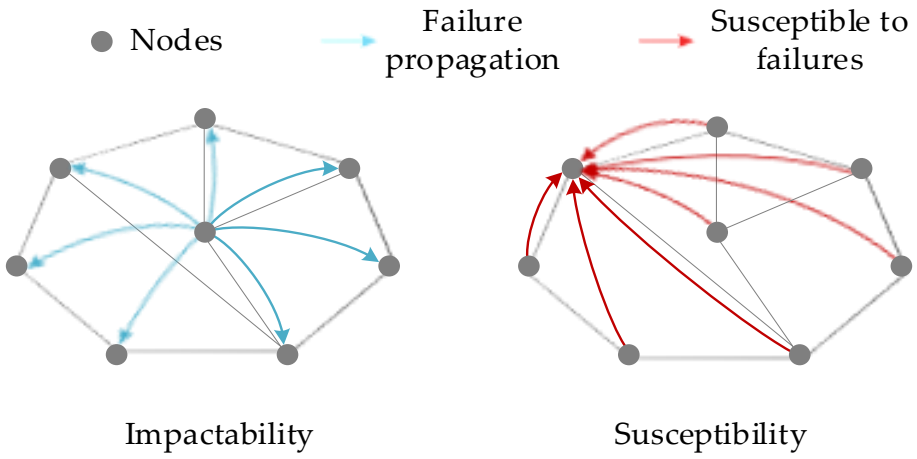

Figure 4. Differences between impactability vulnerability and susceptibility vulnerability.

3. The Foundation Framework for CPPS Vulnerability Assessment Based on Complex Network Theory

3.1. Feasibility of Complex Network Theory in CPPS Vulnerability Assessment Research

Although CPPSs are often studied as a whole, cyber networks and physical networks have their own distinct characteristics. Therefore, it is common practice to first study cyber networks and physical networks separately before investigating their coupling. The operational status of the cyber network directly impacts the state of the power system, making it akin to a complex system due to the significant increase in the size and complexity of information across various services [27,67]. Likewise, the power system strictly adheres to physical operation rules (e.g., Kirchhoff's law) [68] and exhibits general characteristics of a complex system [69,70]. Thus, when analyzing coupled networks at the subnetwork level, a perspective grounded in complex systems science can be employed. Furthermore, CPPS vulnerability assessment centers on the network's connectivity relationships and the interaction between its components, which affect the system's failure evolution mechanism. As such, its research perspective concentrates on the system level. Consequently, complex network theory, a branch of complexity systems science, proves feasible for CPPS vulnerability assessment, as it examines network science at the system level. The feasibility of applying complex network theory to CPPS vulnerability assessment research can be demonstrated by the following points:

- Complexity: The power grid has transformed into a high-dimensional, nonlinear, and complex artificial network [71], with a wide spatial distribution and a large range of disturbance propagation, as a result of power grid interconnection and continuous expansion in scale [72]. Simultaneously, the power grid's evolution into a complex cyber-physical system characterized by multidimensional heterogeneity and intricate interaction mechanisms further adds to its complexity [73]. On the one hand, the CPPS is subject to various complex and variable internal and external threat factors, with contingencies and correlations among these factors. On the other hand, the interrelationships between components and systems, as well as the inter-component relationships, are closely tied to the system's topology and operation. The convergence

and interplay of these aspects contribute to the highly complex failure mechanism of the system, challenging conventional analysis methods and imposing limitations on vulnerability assessment. To address this challenge, complex network theory emerges as a promising analytical approach from the field of complexity studies. By employing complex network theory, one can effectively explore and elucidate the uncertainty and intricate characteristics inherent in vulnerability assessment, thus offering a novel perspective to tackle the complexity of the system.

- Similarity: From the perspective of basic functions, both the cyber network and the physical network within the CPPS share similarities with other infrastructure, as they facilitate the transportation or exchange of material, whether tangible or intangible [74,75]. Considering the structural characteristics, the CPPS topology exhibits some correlation with the system performance and operational characteristics [70]. Regarding operational attributes, CPPSs demonstrate self-organized critical properties and kinetic characteristics in fault propagation [76]. As these properties are typical of complex systems and tightly linked to the system's vulnerability points, they offer substantial guidance for the implementation of complex network theory in CPPS vulnerability assessment.
- Holistic: The classical electrical theory has its foundation in a reductionist approach to analysis [70], leading traditional vulnerability assessment methods for steady-state and transient states to focus more on qualitative analysis of the local electrical–physical characteristics of the system or individual components, as well as the operational attributes the system [77,78]. However, assessing the vulnerability of a CPPS requires the impact of interactions between the cyber network and the physical network to be considered. The conventional approach of studying vulnerability in the CPPS solely from a single network perspective (either a cyber or a physical network) has proven quite limited [73,79]. In contrast, complex network theory represents an analytical approach rooted in systems theory, encompassing statistical analysis of the overall expression of the power system [80]. Consequently, it places greater emphasis on studying the statistical characteristics of faults among components and systems from a holistic standpoint, thereby revealing the system's vulnerability. Thus, complex network theory introduces a novel analytical perspective for vulnerability assessment.

3.2. Research Topics of Complex Network Theory in CPPS Vulnerability Assessment

The literature on CPPS vulnerability assessment incorporates complex network theory, which comprehensively considers the characteristics of both the cyber and the physical layers. The cyber layer entails the study of communication nodes (such as data collection terminals, communication routing, computing terminals, and dispatch centers) and communication links (real or virtual circuits [81]). On the physical layer, the focus is on bus nodes (generator nodes, transformer nodes, and load nodes) and branch circuits (branches and transformers). The primary objective is to identify vulnerable nodes or branches that directly or indirectly trigger system collapse (major outage) through statistical analysis of cascades, which encompass fault cascade relationships and topological cascade relationships between nodes or branches. The research framework, illustrated in Figure 5, comprises four essential steps: model abstraction, vulnerability index construction, assessment criteria establishment, and experimental analysis.

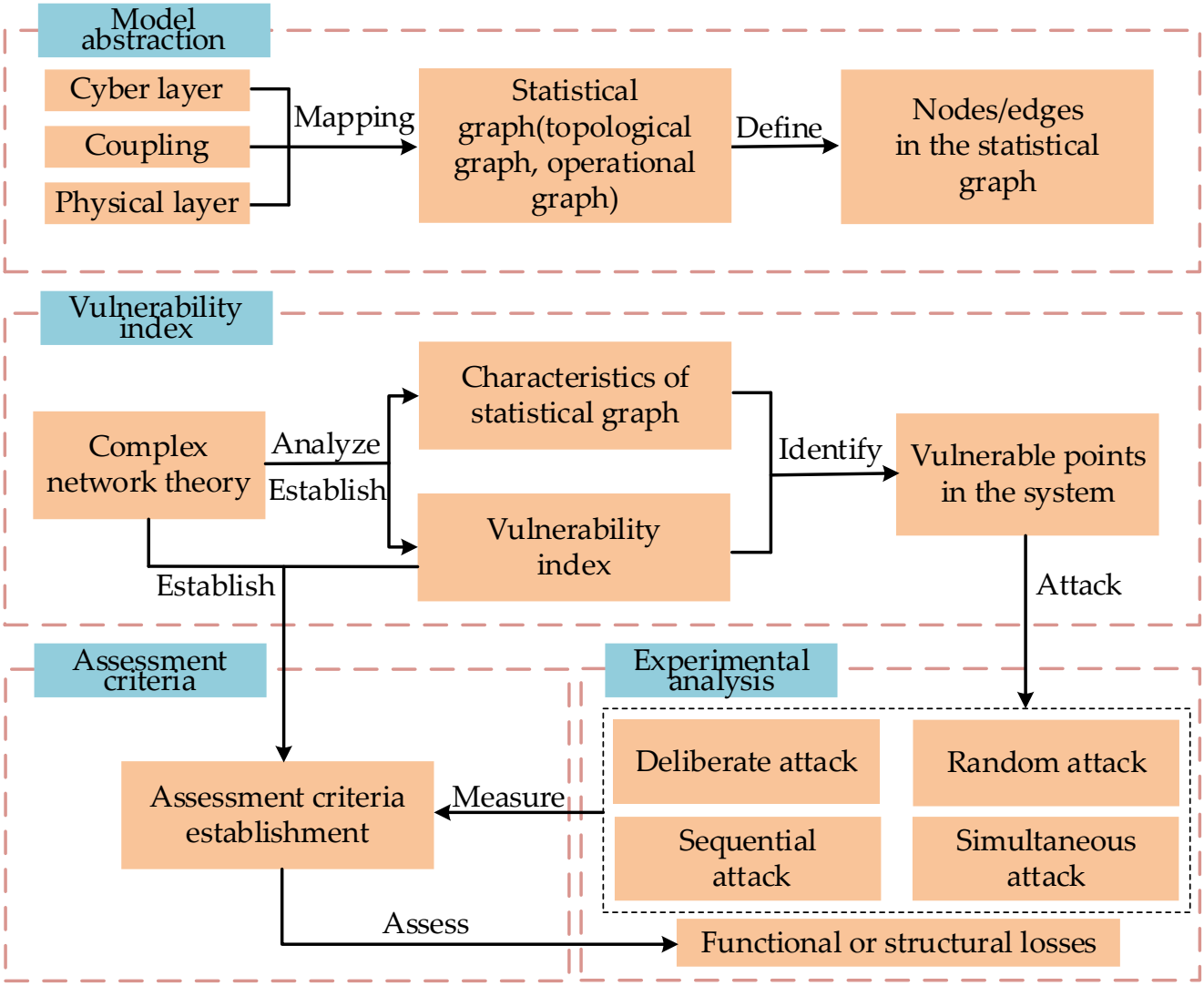

Figure 5. Framework of CPPS vulnerability assessment based on complex network theory.

In model abstraction, a statistical characteristic graph is generated to abstract the physical, operational, or structural characteristics of a system. Considering that a cyber-physical system comprises at least a cyber network and a physical network, the way these two networks are coupled significantly impacts the system's operation. Various approaches, such as interdependent networks [82–84] and hybrid systems [85,86], are employed for model abstraction of cyber–physical systems. Interdependent networks facilitate intuitive exploration of cyber–physical systems from topological and operational perspectives through the coupling of different networks via interdependent edges [87]. Consequently, interdependent networks are widely utilized in the study of CPPSs from a complex network perspective. The general process of model abstraction involves separately modeling cyber networks and physical networks using complex network theory. Subsequently, the coupling of these two networks is achieved through interdependent networks. For instance, from the perspective of structural characteristics, data collection equipment and computing equipment are considered nodes in the statistical graph of the cyber layer, whereas communication links serve as edges. On the physical layer, bus nodes represent nodes in the statistical graph, and branches act as edges. This results in separate topological graphs for the cyber system and the physical system. By employing interdependent edges, different connectivity patterns (one-to-one [88], one-to-many [89], many-to-many [84], etc.) are established between nodes in the two topologies, forming a comprehensive topological graph

of the CPPS. On this basis, the meanings and weights of edges and nodes in a statistical graph can be defined according to the research problem and methodology.

The vulnerability index construction involves analyzing the system's vulnerability by examining the properties of statistical graphs using complex network theory. Subsequently, vulnerability indices are constructed to identify the vulnerable nodes or branches within the system. It is essential to highlight that the model abstraction and vulnerability indices will be elaborated upon in detail in the following section.

Assessment criteria encompass both structural and functional aspects. Their primary objective is to quantify the extent of the structural or functional impairment (destructiveness) within the system after the elimination of a vulnerable node or branch. These criteria serve as crucial tools to validate the proposed vulnerability metrics. Structural assessment criteria commonly utilize established metrics from complex networks (e.g., connectivity [61,90]). Furthermore, although CPPS needs to be analyzed as a whole, due to the specificity of power systems, whose main purpose is to transmit the power generated by generators to consumers, only indices from the power grid layer, such as network connectivity [91] and network efficiency [92,93], are typically utilized in research to describe the vulnerability of the entire CPPS; such indices are widely employed to gauge the level of connectivity between generator nodes and load nodes across the system when vulnerable points are removed. Presently, there is no standardized approach for devising these assessment criteria, and different criteria are selected based on specific research objectives. In functional assessment criteria, the load loss of the system [93] is currently the commonly used criterion for functional assessment, since the main function of the system is to provide electrical energy to the users. For instance, the generalized system average interruption frequency index, generalized system average interruption duration index, generalized expectation of energy not supply, and generalized average service availability index were proposed in [94] to describe the power supply capability of cyber–physical power from the perspective of functional assessment criteria after being subjected to network disturbances.

In the experimental analysis, one of the primary ways to conduct simulation studies is by attacking the system, which involves removing the target nodes or branches from the system. Among the various attack methods, numerous studies in the literature have demonstrated that the system exhibits high robustness when subjected to random attacks [93,95]. Consequently, random attacks are commonly used as a benchmark to validate the effectiveness of the proposed method. In contrast to random attacks, deliberate attacks encompass static attacks [96,97] and dynamic attacks [92,97]. Static attacks are mainly based on the results of structural vulnerability metrics ranking, where branches (or nodes) are removed from the network, and the ranking results remain unchanged even if there are changes in the network's topology due to network failures. In comparison, dynamic attacks involve reranking based on the current network state after certain targets are removed from the network. Moreover, temporal relationship classification leads to the distinction between sequential attacks and simultaneous attacks [96,98]. Sequential attacks involve the sequential removal of a certain number of branches (or buses) from the system, one at a time, whereas simultaneous attacks simultaneously target a specific number of branches (or nodes) in the system. The selection of different attack methods is contingent on the research objectives. For instance, sequential attacks simulate the cascade occurrence of incidents to some extent, making them suitable for analyzing the impact of a vulnerable branch (or bus) on a cascading failure. From the perspective of the defender or attacker, simultaneous attacks offer a reasonable method to effectively analyze how the system can be prevented from being rapidly destroyed. Additionally, comparing the two attack methods reveals that sequential attacks possess a greater destructive capability to some extent than simultaneous attacks [96,98].

4. Current Status of Research on CPPS Vulnerability Assessment Based on Complex Network Theory

In the vulnerability assessment of CPPSs using complex network theory, model abstraction and vulnerability index construction constitute the core elements of the assessment system and have been extensively investigated by both domestic and international scholars. This chapter discusses the current research status of vulnerability assessment in CPPSs using complex network theory, focusing on the perspectives of topological vulnerability and operational vulnerability.

4.1. Structural Vulnerability Assessment Based on Complex Network Theory

In the context of topological vulnerability assessment, the fundamental approach involves abstracting the system's topology into a topological graph. Subsequently, complex network theory is utilized to construct a vulnerability index based on this topological graph, as illustrated in Figure 6. The pure vulnerability index (PVI) focuses solely on the topological characteristics of the system. In other words, the system's topology is directly represented by an undirected and weightless topological graph [99,100]. Building upon this representation, statistical measures from complex network theory [101,102], such as betweenness [103] and degree [104], are employed to identify the system's vulnerability points.

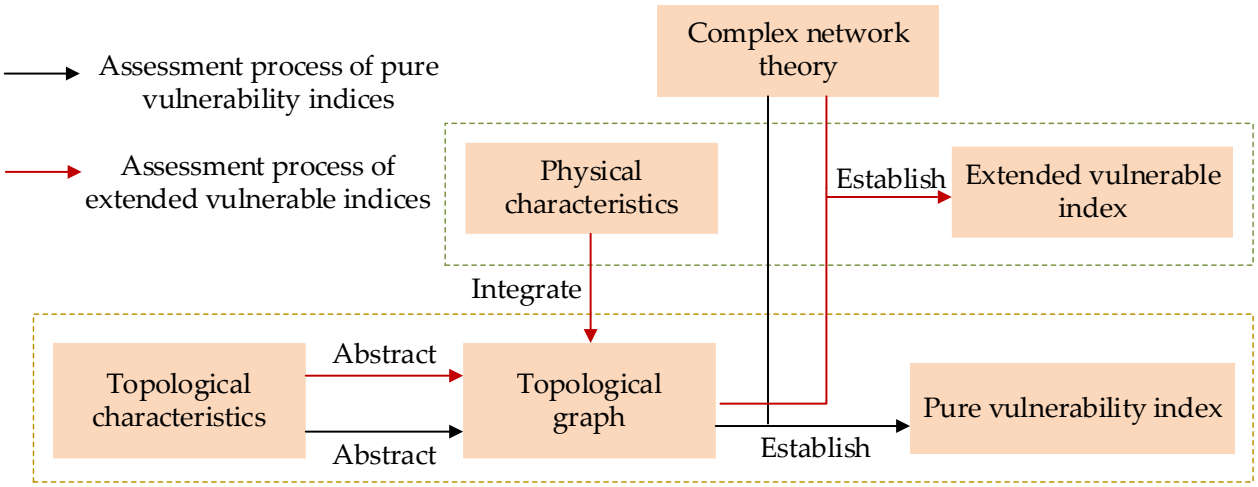

Figure 6. Framework of structural vulnerability assessment based on complex network theory.

However, by focusing solely on the topological characteristics of the system and neglecting its physical aspects, the pure vulnerability index results in one-sided assessment outcomes. To truly reflect the system's vulnerability characteristics, the topological graph must be constructed with consideration of the physical features of the system, employing weights or directed topology.

In the literature, to incorporate the physical characteristics into the topology graph, the direction or weight of edges/nodes is generally defined based on electrical quantities of the physical layer, as presented in Table 1. Among the weight definitions, branch reactance (impedance) and capacitance are commonly used to measure the electrical distance between nodes and serve as weights of the edges [102,105], and they are one of the most widely used electrical quantities. Reactance, being an inherent property of the branch (static property), remains unchanged with network operation state fluctuations. Furthermore, it is a critical parameter determining the system flow distribution, with smaller branch reactance implying higher power transmission through the branch under similar conditions. Consequently, reactance as a weight in the topology graph can to some extent reflect the power transmission capability of each branch. Moreover, to refine the influence of different generators and load nodes on power transmission within each branch, the power transmission distribution factor (PTDF), unit injection current, and other methods are

successively employed to define branch weights. Additionally, electrical quantities such as branch capacity and voltage level are designated as layer weights to reveal the sensitivity of branch contributions to tidal current transmission.

Furthermore, with the development of CPPSs, it has become evident that the physical characteristics of the cyber layer also directly impact the system's vulnerability [106]. However, defining the weight or direction of the cyber layer topology proves more challenging than that of the physical layer. Information entropy [107] in current studies is generally employed to portray the amount of information contained in cyber nodes or their collections. Higher information entropy in a cyber node signifies greater diversity and uniqueness of the transmitted information, which may play a vital role in information transmission throughout the entire network [108], making the node more susceptible to fault propagation. Consequently, information entropy can be used to define the weights of the cyber-layer topology graph. These weight definitions effectively reflect the essence of branch/node transmission capability and the importance within the network.

Table 1. Definition of weights of edges/nodes.

Nodes/Edges	Weights	Dynamic/Static	Meaning	Related Literature
Edges	Branch reactance (impedance)	Static	Characterize the power capacity of the transmission (the smaller the branch reactance, the greater the power transmitted under the same conditions)	[90,109–114]
Edges	Branch capacity	Static	Characterize the power capacity of the transmission (the larger the capacity, the greater the power capacity transmitted)	[115,116]
Edges	Branch voltage level	Static	Characterize the power capacity transmitted (the higher the voltage level, the higher the corresponding transmission capacity [117])	[117]
Edges	Branch circuit impedance multiplied by the inverse of the voltage rating factor	Static	Characterize the power capacity of the transmission	[68]
Edges	Branch power transmission distribution factor	Dynamic (changes in generator load node pairs)	Characterize the sensitivity of each branch to the tidal transmission contribution	[57,93,102,118–121]
Edges	The probability that a branch circuit will be in normal operation for a certain period of time	Dynamic (branch operation time related)	Cumulative running time of the characterization branch	[122]
Edges	Branch current sharing factor	Dynamic (injection current and branch voltage variation)	Characterize the effect of unit injected power on the branch current	[95,123]
Edges	Current (power) flowing in the branch circuit after the generator load node pair and injection of current (power)	Dynamic (changes in generator load node pairs)	Characterize the degree of contribution of branch flows to the whole network	[92,97,124–126]
Nodes	Rated capacity or output of the generator node, actual or peak value of the load node	Static/dynamic (changes with flow distribution)	Characterize the importance of node transmission and distribution power	[97,116,117,124]

Dynamic/static is characterized by whether this weight changes with the operational state of the system.

Based on this, the abstracted topological graph, considering physical characteristics, becomes the object of research to construct extended vulnerability indices (EVIs) utilizing statistical characteristic quantities from complex network theory (e.g., betweenness, average path, degree, and maximum flow), as shown in Table 2. Among these, betweenness in complex network theory serves to reflect the role and influence of edges/nodes in the entire network, making it one of the most widely used indices in CPPS vulnerability assessment.

Regarding the steady-state operation of the system, electrical quantities such as branch reactance and branch capacity are incorporated into the betweenness index, leading to the construction of expanded betweenness indices, such as electrical betweenness [97,126], capacity betweenness [115], and power flow betweenness [125]. These indices capture the nodes'/branches' abilities and influence in power transmission and distribution within the system, indirectly reflecting their impact on system outages when they fail and thereby revealing vulnerable points in the system. Additionally, expanded metrics such as expanded degree and average path are utilized to characterize the power transmission capability and the importance of nodes/branches within the system. From the perspective of the system's transient operation, the impact of transient energy on the system during significant short-period disturbances is considered in [127], and the kinetic energy injection betweenness is proposed as a means to assess the extent of disturbance to the branches.

The use of extended statistical characteristic indices to assess the vulnerability of the system has two advantages at the steady state level or from the transient perspective of the system. First, the statistical characteristic quantities of the complex network define the impact of the branches/nodes on the system topology from a system-wide perspective, thereby characterizing the topological statistical properties of the system. Second, the incorporation of electrical quantities characterizes the physical properties of the system, enabling the extended indices to integrate the system topology and physical characteristics. As a result, they align to a certain extent with the actual characteristics of the power system. Furthermore, comprehensive utilization of different expanded metrics is enabled, as they reveal the topological and physical characteristics of the CPPS from diverse perspectives, allowing for a comprehensive assessment of the vulnerability of the CPPS [128].

Table 2. Extended vulnerability indices.

Basic Characteristic Quantity	Research Object	Operating State	Electrical Quantity	Meaning	Related Literature
Betweenness	Branch/node	Normal	Branch reactance, branch capacity	Characterize the importance of branch transmission and distribution power from a system perspective	[57,90,93,114,115, 120,128]
Betweenness	Branch	Normal	Branch circuit current (power), generator rated (issued) power, load	Reflects the power transfer of the branch in the generation load node from a system perspective	[95,97,124–126]
Betweenness	Branch	N-1 standard	Branch power, generator capacity, peak load, branch impedance, branch capacity	Characterize the importance of branch transmission and distribution power and the coupling between the branches from a system perspective	[92]

Table 2. *Cont.*

Basic Characteristic Quantity	Research Object	Operating State	Electrical Quantity	Meaning	Related Literature
Betweenness	Branch/node	Normal	The probability of normal operation time in a certain period of time for a branch	Characterize the continuous operation time of system components from a reliability perspective	[122]
Betweenness	Branch	Normal	Branch circuit voltage level, branch circuit impedance	Characterize the importance of branch transmission and distribution power from a system perspective	[68]
Betweenness	Branch	Normal	Node injection current, branch conductance	Characterize the importance of branch transmission and distribution power from a system perspective	[123]
Betweenness	Branch	N-1 standard	Kinetic energy of generator rotor	The degree of transient impulse to the branch circuit after the system is disturbed	[127]
Average path	Node	Normal	Branch reactance	Characterize the connectivity of nodes in the system	[110]
Degree	Node	Normal	Node injection power, branch voltage level	Integrated characterization of the topological and power characteristics of the system	[117]
Degree	Node	Normal	Branch reactance	Characterize the power transmission capability of the node	[128]
Degree	Node	Normal	The probability of normal operation time in a certain period of time for a branch	Characterize the node's duration of operation from a reliability perspective	[122]
Maximum flow	Branch/node	Normal	Branch reactance, branch capacity	Characterize the carrying capacity of the branch/node for system flow	[112,116,118]

The table is classified by electrical quantities.

Although to some extent the extended vulnerability index considers the physical characteristics of the power system, it is primarily constructed based on the topological statistical characteristics of the system, thereby remaining within the domain of topological structure fragility assessment.

Second, current research predominantly focuses on constructing vulnerability indices in the normal operational or $N-1$ fault state of the system, with limited consideration of the $N-k$ fault state of the system. Consequently, the resulting indices do not effectively capture intercomponent relationships, such as fault propagation relationships, and fail to adequately reflect the impact on the network when vulnerable components fail and when the mechanisms lead to cascading failure propagation.

Last, the majority of topological vulnerability indices still fall under the category of "static" indices in complex network theory, primarily relying on basic static characteristic

statistical indices (e.g., degree, betweenness). Therefore, further investigation is needed to effectively incorporate the dynamic theory of complex networks into the assessment of topological vulnerability in systems.

4.2. Operational Vulnerability Assessment Based on Complex Network Theory

In contrast to general complex systems, CPPSs operate according to physical rules, such as adhering to bandwidth constraints for power data transmission and following Kirchhoff's law in grid operation. Consequently, a topology-based vulnerability assessment alone fails to offer a comprehensive understanding of the system's (operational) vulnerability characteristics. To address this limitation, operational graphs are devised by integrating the operational, physical, and topological characteristics of the system, with a focus on cascading faults. For instance, two types of characteristic temporal–spatial correlation graphs [66], cascading fault graphs [98,129,130], risk graphs [96,131], influence graphs [132], and interaction graphs [133,134] are constructed to elucidate the operational vulnerability of the system. The assessment framework for these operational graphs is presented in Figure 7. It is essential to note that the nodes in the operational graph represent components in the source system at that particular point in time.

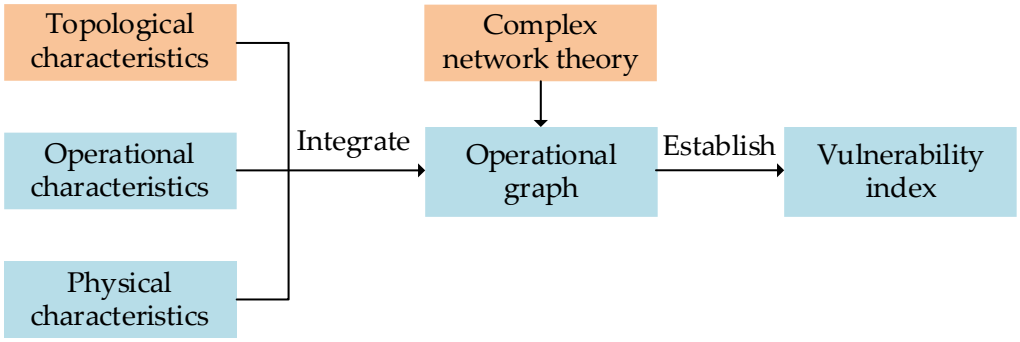

Figure 7. Framework of operational vulnerability assessment based on complex network theory.

The construction of the operational graph involves two primary approaches. First, different combinations of components are simultaneously or sequentially removed, and the combinations that cause significant damage to the system function or structure are filtered to form the operational graph [96,131]. Second, cascading fault propagation paths obtained from counting the cascading fault propagation paths in the system under different fault operation states are combined and then mapped into the operational graph [98,129,130]. In the first operational graph, a node with a high number of neighboring nodes indicates that the components in the source system corresponding to that node have a high operational vulnerability within the network. On the other hand, the second operational graph utilizes cascading fault propagation paths, which reflect the sequential cascading failure relationships between components. This results in a statistical graph that transforms spatial information from the source physical network into information that reveals the sequential associations of component failures. The direction of the edges in the second operational graph effectively illustrates the fault cascade relationship between components and the fault propagation mechanism of the system under different fault operation states. Meanwhile, the weights of the edges can reveal the propagation likelihood between components, the degree of structural damage, or the loss of load [135].

On this basis, the operational vulnerability of the system is assessed using complex network theory to construct vulnerability indices on the operational graph. Based on the static characteristic statistical indices of complex networks, degree, in-degree, and out-degree indices are utilized to identify components with distinct vulnerability characteristics [98,129,130]. Components with higher out-degree indicate a higher likelihood of propagating faults during fault propagation, making them impactable vulnerability nodes. Conversely, components with higher in-degree are more susceptible to the influence of

propagating faults and represent susceptible vulnerable nodes. Furthermore, in the second type of operational graph, nodes map the importance of components in the source system, whereas the distance between nodes illustrates the cascade propagation relationship between components in the source system (referred to as vulnerability distance in [65], which uses vulnerability distance as a replacement for electrical distance to measure the relationship between nodes). Therefore, in [66], attempts are made to construct dynamic vulnerability indices considering the importance of components and the cascade propagation relationship between them from the perspective of the dynamic model of complex network theory using the load–capacity model [136,137] This dynamic vulnerability index is employed to identify vulnerable branches within the system.

The utilization of operational graphs in studying the vulnerability of systems effectively addresses the shortcomings of topological structure graphs in accurately reflecting the system's operational characteristics among nodes or branches. In particular, the topological characteristics of the second type of operational graph reveal the cascade failure propagation mechanisms between components in the source system, thus offering new insights for conducting dynamic studies on the vulnerability of complex network theory-based systems.

However, operational vulnerability assessment based on complex network theory using operational graphs still faces several challenges. Since operational graphs are essentially statistical graphs from a type perspective, further exploration is needed to effectively select component combinations (for the first type of operational graph) or cascade failure propagation paths (for the second type of operational graph) for constructing the operational graph. On the one hand, if the selected component combinations or cascade propagation paths are too few, the constructed operational graph may not fully reveal the system's vulnerability characteristics, leading to overly simplistic assessment results. On the other hand, if the selected component combinations or cascade propagation paths are too numerous, it may not only lead to the "curse of dimensionality" but also fall into the realm of risk assessment, resulting in insufficiently meaningful conclusions from the perspective of vulnerability assessment.

Furthermore, the construction of operational graphs is commonly based on the operational state at a specific moment and does not consider the time-evolving operational characteristics. In actual operation, the system's operational state changes over time, resulting in the operational graph being influenced by the system's evolving state. Therefore, it is necessary to construct time-evolving operational graphs and utilize complex network theory to analyze graph evolution patterns, thus revealing the time-varying operational vulnerability of the system.

5. Interrelationship between System Vulnerability and Cascading Failures

From the perspective of complex network theory, numerous studies have indicated that the topology of CPPSs exhibits small-world network characteristics, as demonstrated in various power grids, such as the power grid of the western United States [138], the Brazilian grid [139], the Iranian grid [140], and the power grid of northern China [141]. The small-world properties of the topology imply that the network possesses high clustering coefficients and relatively short average path lengths, indicating close connections between nodes or branches. Consequently, when nodes or branches in the network experience failures, the high clustering coefficient facilitates the easy propagation of failures to neighboring and even non-neighboring nodes, revealing the characteristics of cross-regional propagation of cascading failures. Meanwhile, the shorter average path lengths accelerate the speed of failure propagation.

On the other hand, by analyzing the extent of functional or structural damage to the system after removing certain nodes or branches from the network, it is found that specific critical nodes or branches contribute significantly to the severe disruption of system functionality or structure (particularly in terms of functional damage). Therefore, from the perspective of deliberate attacks, the system exhibits a scale-free nature [95].

It should be noted that although the general topology of the system is not a scale-free network, it displays certain scale-free characteristics under deliberate attacks. This scale-free nature of the network indicates the presence of vulnerable points in the system. Once these vulnerable points experience failures, they easily trigger and exacerbate the propagation of failures.

In conclusion, as illustrated in Figure 8, the small-world characteristics of the CPPS topology and the scale-free nature observed under deliberate attacks partially reveal the essence of system vulnerability and cascading failures.

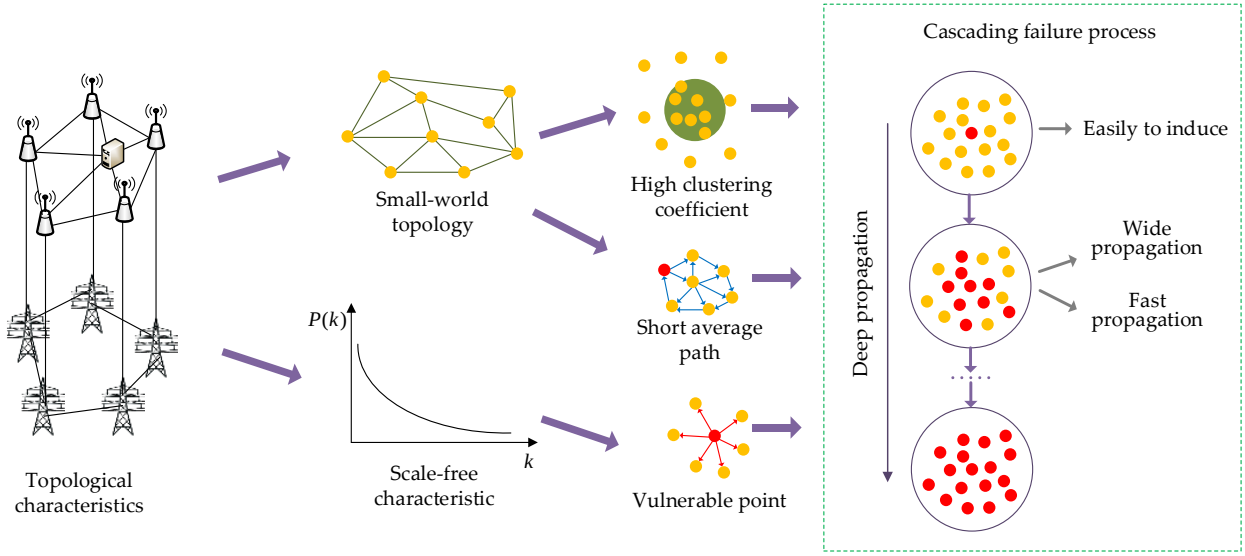

Figure 8. Analysis of propagation mechanism of cascading faults from a topological perspective.

Figure 8 only reveals the interrelation between structural vulnerability and cascading failure propagation mechanisms from a topological perspective. As mentioned earlier, the power grid is an artificial network that follows physical operating rules, and therefore, the cascading failure mechanisms and operational characteristics of the system are closely linked. It is necessary to analyze the cascading failure mechanisms of the system from the perspective of its operational characteristics. A risk propagation model for the cyber–physical system of the distribution network was constructed using a dynamic Bayesian network in [142]. The impact after cyberattacks under different operational states was evaluated, and the probability of fault risk propagation in the network when nodes fail from an operational perspective was revealed. The system's scale-free characteristics were indirectly revealed in [98,129,130] by analyzing the topological characteristics of the constructed cascading failure graph, indicating the existence of a small number of highly vulnerable components in the network that, when attacked, lead to severe nonoperational states (or even system collapse).

Furthermore, to elucidate the roles of different types of vulnerable components (i.e., impactable components and susceptible components) in the cascade failure propagation process, the study conducted by [66] utilized symmetric entropy to construct the impactability temporal–spatial correlation graph and the susceptibility temporal–spatial correlation graph. Building upon this, as illustrated in Figure 9, the analysis of the topological characteristics of these two types of graphs revealed that the impactability temporal–spatial correlation graphs exhibit scale-free network properties, whereas the susceptibility temporal–spatial correlation graphs display small-world network characteristics. Moreover, it was observed from the scale-free properties of the impactability temporal–spatial correlation graphs that branches with high susceptibility in terms of propagating failures are more likely to trigger failure propagation, resulting in heightened network vulnerability and an intensified depth of failure propagation. Conversely, based on the small-world properties of

the susceptibility temporal–spatial correlation graphs, the cross-influence between branches during failure propagation amplifies the breadth of failure propagation.

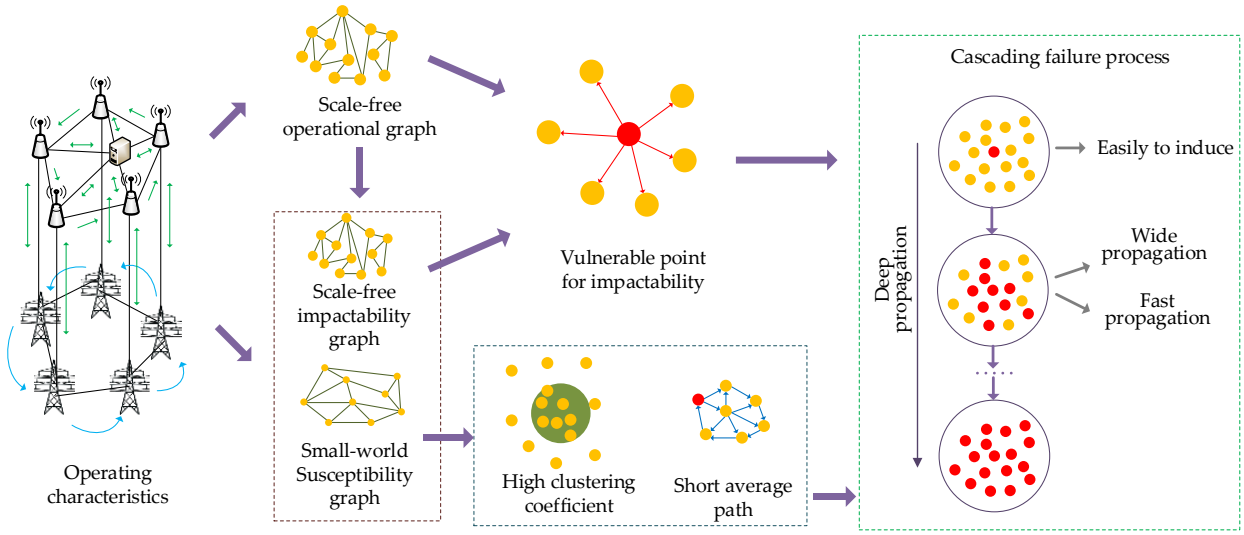

Figure 9. Analysis of propagation mechanism of cascading failures from an operational perspective.

From the perspective of complex network theory, one of the most significant reasons for cascade failure propagation in a system is the presence of vulnerable points. In particular, when the system operates at a critical state, these vulnerable points can become crucial factors leading to system collapse. As a result, there is a close association between the system's self-organized criticality and vulnerable points.

Additionally, from the perspective of cyber–physical coupling, due to the influence of interdependencies, there is a probability of interconnected vulnerable nodes/edges between the two interconnected networks. This leads to a situation where failures on one layer have a probability of propagating through interdependent edges to the other layer and initiating further propagation. If the vulnerable points of both interconnected networks are directly connected, it can cause the failure to rapidly spread throughout the entire system, resulting in cascading failures and ultimately leading to system collapse [84]. Therefore, the vulnerability of CPPSs may be amplified through coupling characteristics, exacerbating the propagation of cascade failures.

6. Applications and Prospects of Vulnerability Assessment Based on Complex Network Theory

The development of smart grids has brought about a growing diversity of potential threats and disruptions. When the physical layer of the CPPS is exposed to low probability, high-risk extreme events, such as terrorist attacks or extreme weather, the vulnerable points in the system are susceptible to damage. The cyber layer is vulnerable to cyberattacks, such as denial of service (DoS) attacks, false data injection attacks (FDIAs) [143], or replay attacks (RAs) [144,145]. Although these attack methods and principles vary, all of these types of attacks rely on cyber communication. Attackers attempt to execute their attacks by disrupting or deceiving cyber communication with the aim of causing cyber nodes to fail, ultimately triggering fault propagation. It is worth noting that there is a significant distinction between attacks and faults, and there is no inherent causal relationship. The system does not necessarily experience a fault after an attack, and faults are not always caused by attacks. The analysis in this section is based on the attacker's objective, which is to trigger a system-wide cascade failure through attacks. It assumes that the system undergoes operational-state changes after an attack, and therefore the application and prospects of CPPS vulnerability assessment in the context of attacks are analyzed. This analysis considers the potential changes in the system's operational state as a result of

attacks without implying a direct cause-and-effect relationship between network attacks and faults.

As the CPPS's structure and functionality become more complex, conventional single-layered attacks pose diminishing threats to the system. Attackers are now resorting to coordinated cyber–physical attacks based on FDIAs, such as load redistribution (LR) [146] and false topology attacks (FTAs) [147]. These methods can mislead the dispatching system through false data, causing operators to make incorrect decisions and altering the normal operation state of the grid. Concurrently, physical attacks are launched on the physical layer, leading to cascading failures in the system [148], as shown in Figure 10.

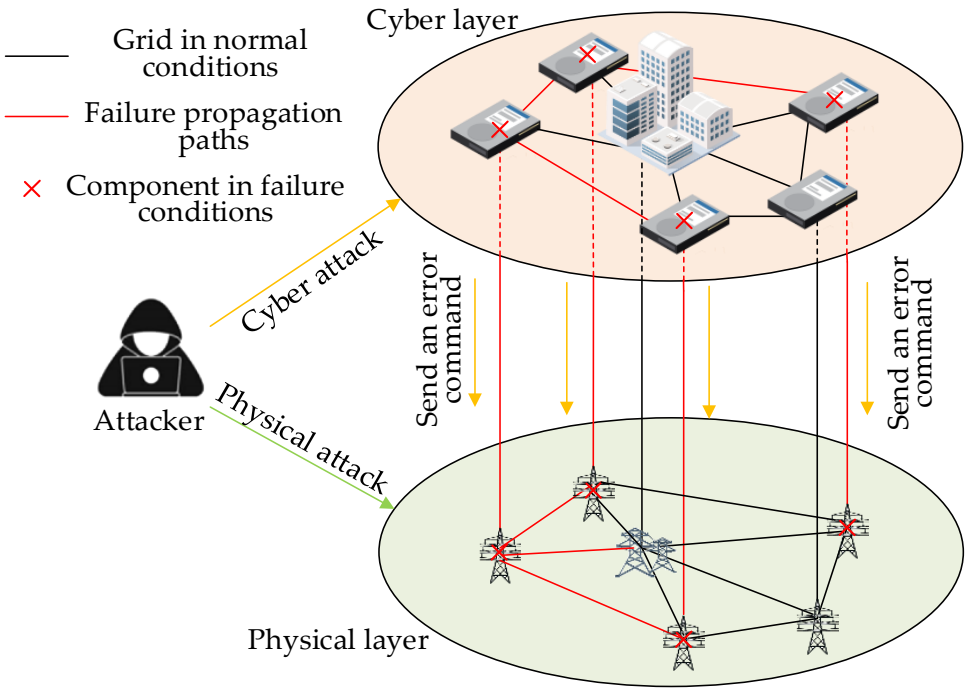

Figure 10. Schematic diagram of a coordinated cyber–physical attack.

Coordinated cyber–physical attacks are typically not single occurrences and are often carried out in a continuous or sustained manner. A multistage coordinated cyber–physical attack strategy was proposed in [149], which, when directed at the CPPS, leads to widespread cascading failures. Faced with these threats and attacks, vulnerability assessment based on complex network theory can offer valuable guidance for the security analysis of CPPS operations.

As shown in Figure 11, the first step of vulnerability assessment is to model the system, and complex network theory can be utilized for coupling modeling of the CPPS. However, this type of model is isolated and static, which is not entirely suitable for dynamic CPPSs. Nevertheless, situation awareness technology enables real-time data acquisition and an in-depth understanding of the system's state [150], providing a new approach for coupling modeling with complex network theory. Through real-time situation awareness, an accurate understanding of the current system state and prediction of future states can be achieved, leading to the establishment of a dynamic complex network model for CPPSs. Based on situation awareness and dynamic complex network modeling, dynamic vulnerability assessment of the system can be conducted, facilitating the identification of vulnerable components during dynamic processes and the prediction of failure propagation risks. The results from dynamic vulnerability assessment can be used for research on security protection and operational optimization, thereby enhancing system reliability and operational efficiency. Finally, with the development of the energy internet (EI), vulnerability assessment can also be applied to an integrated energy cyber–physical system (IECPS) to guide the safe operation of these comprehensive energy cyber–physical systems.

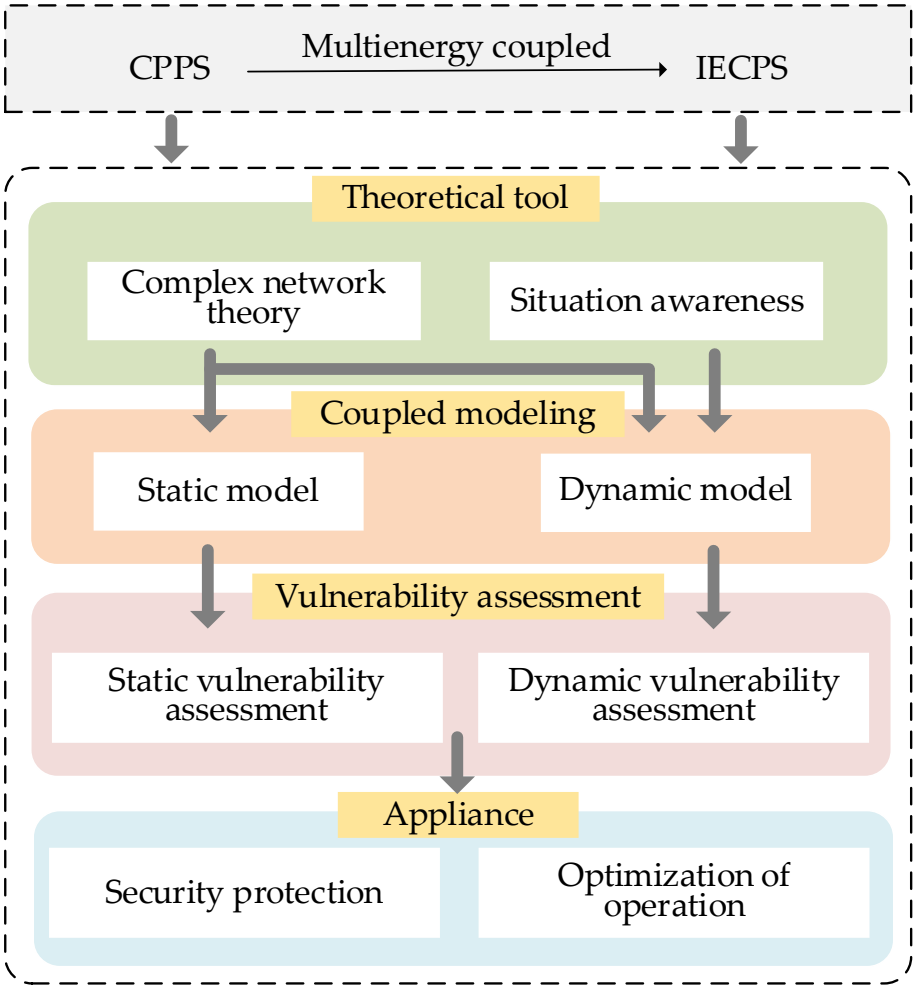

Figure 11. Applications and perspectives of CPPS vulnerability assessment.

6.1. CPPS Coupling Modeling and Analysis

Vulnerability assessment is often carried out for a specific system, network, or organization. When conducting vulnerability assessment of a system, the first step is system modeling, as a well-defined model can provide a comprehensive understanding of the system's structure, components, and relationships. As shown in Figure 12, in CPPS vulnerability assessment, complex network theory is commonly used for coupling modeling of the system. The general approach involves defining separate models for the physical network and cyber network, abstracting them as sets of nodes and edges, and then connecting the nodes of both networks to form an interdependent network. Mathematically, the interdependent relationships can be represented using a cyber–physical association matrix established through interdependent edges, achieving the coupling of the two networks' topologies. The coupling connection methods can vary based on different research objectives, such as one-to-one, one-to-many, many-to-one, or partial one-to-one connections. Based on the coupled topological network, the structural vulnerability of the system can be analyzed. Apart from the structural characteristics, the concept of weights was introduced to the topological graphs. In studies based on complex network theory, there are generally two approaches: One is to use electrical quantities themselves as weight indices; the other is to use complex network theory parameters as weight indices. Some studies also combine electrical quantities and complex network parameters to form extended metrics similar to electrical centrality [151]. These methods redefine the coupled network from an operational perspective.

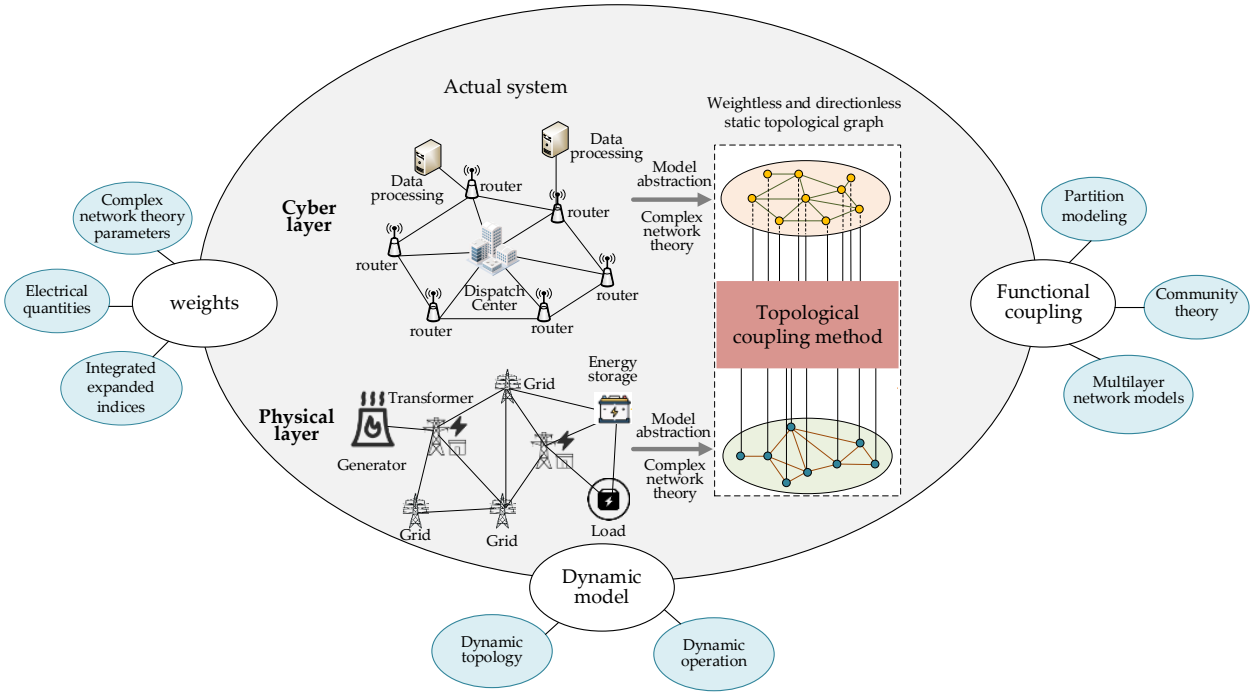

Figure 12. CPPS coupling modeling for vulnerability assessment.

In addition to topological coupling, in recent years, many studies have started to focus on functional coupling—for example, a subset of nodes in the cyber network directly controlling a specific region of the power network while having little association with other nodes. To conduct vulnerability assessments of such functionally coupled systems from the perspective of complex network theory, methods such as partition modeling [152], community theory [153], and multilayer network modeling [154] have been proposed. The common idea behind these methods is to treat sets of nodes in CPPS that exhibit strong overall similarity and interaction for research purposes. Integrating complex network theory, these methods further divide subnetworks into even smaller subnets, where each subnet possesses its own complex network attributes, allowing for the definition of its connectivity and network parameters. At the same time, these subnets contribute to defining the attributes of the upper-level subnetworks, thus simplifying the modeling complexity and reducing model calculation difficulties. These approaches are suitable for research in scenarios such as regional dispatch, hierarchical dispatch, and island grids, and they facilitate regional management and protection of vulnerable elements. Since complex network theory primarily adopts a static perspective, static network models may not capture the dynamic behavior of CPPSs. Therefore, recent research has proposed dynamic complex network models [155], where network connections and topological structures can change. This dynamic approach better describes the sequential nature and evolution process of the system, providing insights for the assessment of the system's dynamic vulnerability.

Multiple studies have indicated that the aforementioned coupling modeling methods based on complex network theory can address most of the research on vulnerability assessment in CPPSs. However, there are still many aspects that warrant improvement. With the development of the energy internet and the construction of new power systems, the application scenarios of vulnerability assessment are continuously evolving. The way to improve various indices in complex network theory to adapt to modeling different characteristic networks, such as vulnerability assessment in distribution networks with distributed energy resources, is a critical consideration. Under the framework of the source–grid–load–storage architecture, when large-scale new energy, energy storage facilities, and distributed energy resources are integrated into the power system for vulnerability assessment, the type of

new ideas that can be derived from complex network theory is an important question. In integrated energy systems, where cyber and multienergy coupling are involved, it is crucial to explore how to utilize complex network theory to establish a cyber–physical model of the integrated energy system and conduct vulnerability assessments of the IECPSs. All these issues require further research.

6.2. Dynamic Vulnerability Assessment Based on Situation Awareness

With the development of new power systems, a large number of heterogeneous data are always generated in the system. Traditional perception techniques mainly relying on manual analysis struggle to handle such vast and complex data. This has led to the application of situation awareness technology in the power system. Situation awareness refers to the capability of collecting, monitoring, and analyzing various data and information related to the operational status of the power system to gain a comprehensive understanding of the current state and accurately predict future development trends. Its basic framework is shown in Figure 13. Situation awareness is divided into three stages: situation detection, situation comprehension, and situation projection, as proposed in reference [150], which also presents a five-layer comprehensive framework of smart distribution network situation awareness.

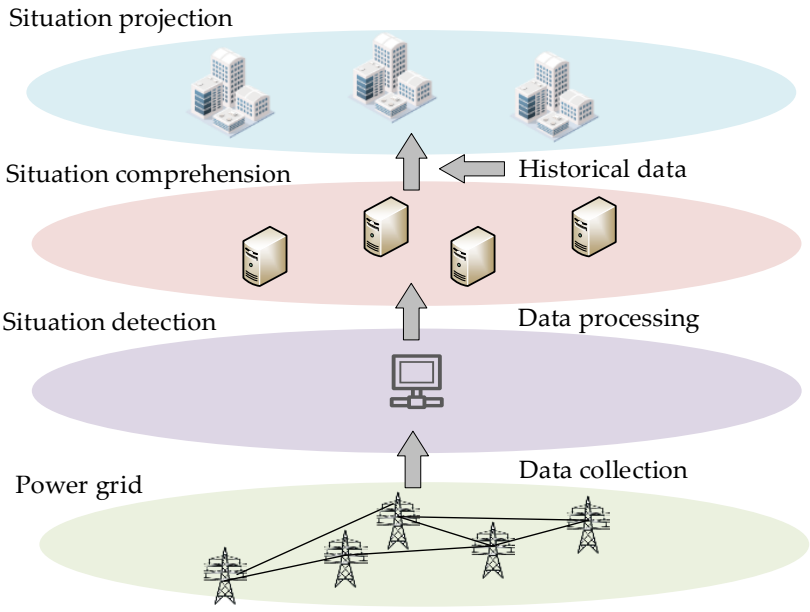

Figure 13. Framework of situation awareness.

Situation detection primarily focuses on acquiring real-time data from various aspects of the power system and conducting preliminary integration and analysis to obtain a comprehensive understanding of the current state of the power system. This involves key technologies such as data acquisition and sensing, data processing and analysis, and data integration. In recent years, numerous data-processing algorithms have been applied to situation detection, such as Kalman filtering [156] and neural networks [157], to optimize and integrate measurement data and identify operational states. However, effectively extracting real-time operational states from a large number of multidimensional heterogeneous data while ensuring high accuracy and timeliness remains a research challenge.

Situation comprehension involves comprehensive analysis and interpretation of the real-time data and information obtained from the power system to gain an in-depth understanding of the overall state and interrelationships of the system. It builds upon the foundation of situation detection and further analyzes and interprets the data to gain deeper insights into the system's state, attributes, and operational characteristics. Currently, some artificial intelligence algorithms have been applied to situation comprehension, en-

abling the understanding of system states by comparing measurement data models with a vast number of historical operational data, laying the groundwork for situation projection. However, challenges remain in accurately conducting data mining and feature extraction from large datasets during the situation comprehension process, as well as addressing the accuracy and computational complexity of power data modeling. Additionally, efficiently achieving human–computer interaction between the data and operational personnel is an area that warrants further research.

Situation projection involves forecasting and inferring the future state and trends of the power system based on existing data and information using established models and methods. This includes status forecasting [158], load forecasting [159], and renewable energy output forecasting [160], among others. It aids operational personnel and decision-makers in devising rational strategies and plans to cope with future changes and challenges. Moreover, situation projection guides the optimization scheduling, resource allocation, and fault handling in the power system, promoting its reliability, stability, and efficiency.

In summary, situation awareness possesses real-time, comprehensive monitoring and responsive capabilities, as well as an in-depth understanding of the system's operational state, thereby providing novel insights into the application of complex network theory in CPPSs.

Through situation awareness, various data and information related to the operation of the power system, such as power load, generation capacity, transmission line status, and equipment operation, can be collected. These data can be regarded as dynamic changes in nodes and edges in the complex network model. By analyzing these data, the interactions between nodes and the paths and patterns of information transmission in the CPPS can be revealed, forming a dynamic complex network model of the CPPS. Based on this dynamic complex network model, more in-depth analysis can be conducted using methods from complex network theory. For instance, when network topology and operational status change, the importance and influence of nodes can be re-evaluated dynamically using indices such as node degree centrality and betweenness centrality, thereby identifying critical nodes in the system. Simultaneously, the small-world property, scale-free characteristics, and community structure of the network can be further investigated, uncovering the dynamic patterns and features of CPPSs. Furthermore, situation awareness can provide real-time monitoring and forecasting of CPPS. By continuously collecting and analyzing system-state data, the network model can be updated in real time. By combining big data analytics, artificial intelligence, and other technologies, future trends of system states can be predicted. This offers real-time decision support for the operation and dispatch of the power system, contributing to optimizing system performance and robustness. It also provides novel approaches for risk prediction and security protection.

Situation awareness combines traditional static complex network analysis with real-time monitoring and forecasting of dynamic systems, providing deeper insights and effective tools for the study and operation management of CPPSs. Traditional vulnerability assessment is primarily based on static system models and static network topology, which cannot accurately reflect the vulnerability of the system under dynamic changing environments. For instance, when attackers target the vulnerable points of a CPPS, causing node failures, there is a probability that the connected edges or nodes may also fail, resulting in changes to the system's topology. Additionally, active defense mechanisms triggered in the system may lead to local load shedding, power flow redistribution, and other behaviors, causing changes in the operational parameters of system nodes and altering the system's operational characteristics.

From the perspective of complex network theory, when a CPPS experiences cascading failures or multistage attacks, the topological and operational characteristics undergo dynamic changes, leading to changes in system properties. First, there are changes in the system parameters; previously important nodes may lose their significance, whereas noncritical nodes may become new important nodes. This is because changes in the system structure may alter the degrees, betweenness, or centrality of nodes, affecting their

status and influence within the system. Second, there are changes in the system properties; systems originally exhibiting scale-free characteristics may transition to small-world or other forms due to the failure of critical nodes, causing localized node failures. This is because changes in the system structure lead to a redistribution and readjustment of node centrality and clustering coefficients. Third, there are changes in the community structure; when system topological and operational characteristics change, the complex network theory's community structure of systems may be adjusted. Previous community structures may be disrupted and new community structures may form, impacting the local centrality of nodes and intercommunity connection patterns. Therefore, vulnerability assessment results under normal system conditions are no longer applicable after the system is attacked. Similarly, if the system experiences multistage coordinated cyber–physical attacks, the system's vulnerability may change after each attack. Hence, dynamic vulnerability assessment in the post-failure dynamic process of CPPSs is an area worth researching.

This section mentions that dynamic complex network modeling can be achieved through situation awareness, thereby enabling the dynamic study of system parameters and attributes. Similarly, based on situation awareness and complex network theory, research on the dynamic vulnerability assessment of CPPSs can be conducted. As shown in Figure 14, during the dynamic process after the system is disrupted, anomalies in the data can be immediately detected through situation detection, and then situation comprehension can be used to identify and understand the current failure state of the system, including failure source localization, failure type, and system losses. By combining automated dynamic complex network modeling with highly autonomous management systems, the operating parameters and complex network theory parameters of the current stage of the system can be updated in real time to detect vulnerable nodes, branches, and potential vulnerability propagation paths within the system. Based on this, the results of vulnerability assessment can also be updated in real time, which helps identify risk areas and vulnerable points that may exist in the system during dynamic changes, providing guidance for the safe operation and protection of the system.

Dynamic vulnerability assessment based on situation awareness has the potential to improve the accuracy and real-time capability of vulnerability assessment, offering a promising approach to address vulnerabilities in CPPSs. However, there are still many issues that need to be investigated, such as the data-processing accuracy of situation awareness, the accuracy and applicability of dynamic complex network models, real-time performance and quick response in practical applications, and the comprehensiveness of multi-indicator decision-making in dynamic vulnerability assessment.

In the future, situation awareness-based dynamic vulnerability assessment can be applied to scenarios where the CPPS faces multistage collaborative cyber–physical attacks and dynamic attack–defense games, requiring dynamic decision-making. It can also be applied to complex systems such as mixed AC/DC power grids, which involve multiple couplings, multienergy systems, and multi-indicators. Moreover, in extreme natural disasters, the power grid exhibits strong uncertainty and multiple risk factors, and considering the characteristics of spatial and temporal scales is essential. In such scenarios, vulnerability assessment can be studied based on situation awareness.

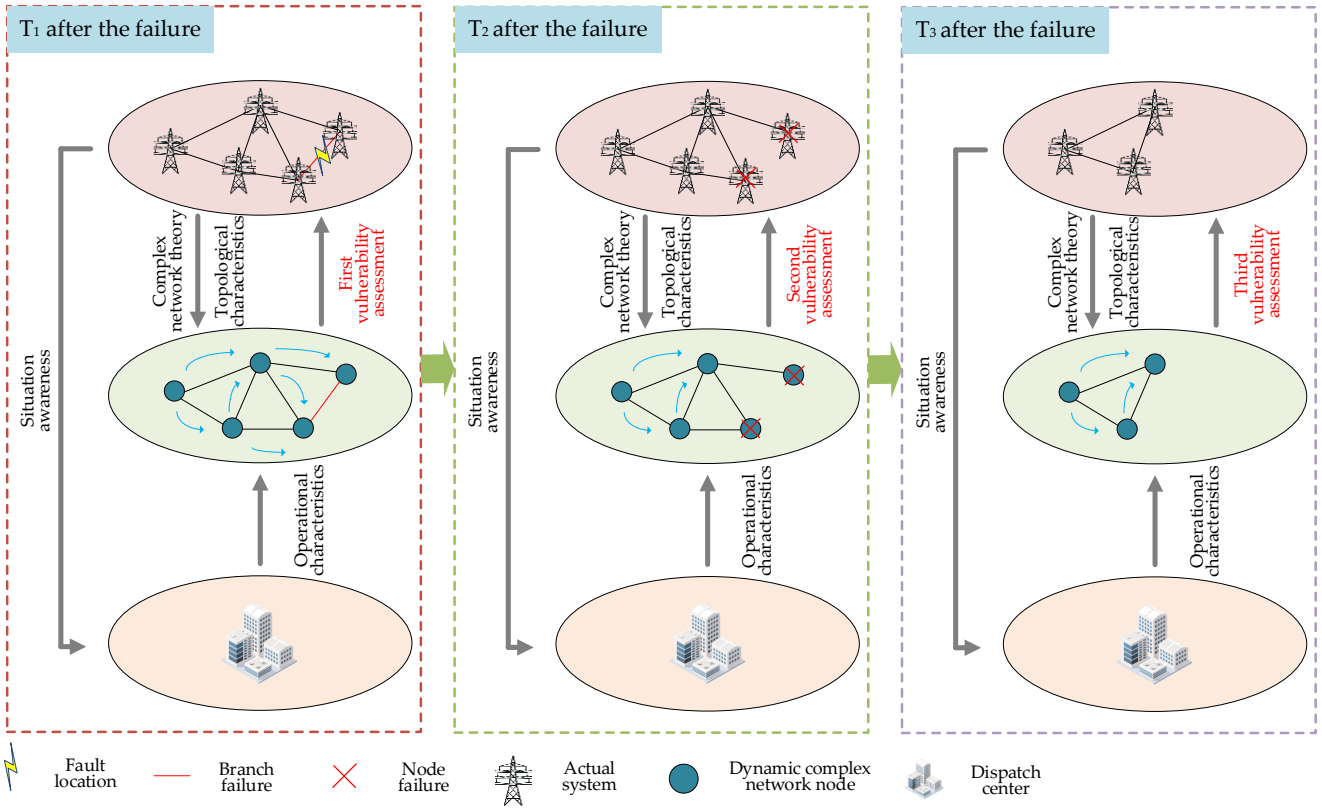

Figure 14. Dynamic vulnerability assessment process based on situation awareness.

6.3. Security Protection of CPPS Based on Vulnerability Assessment

Based on static vulnerability assessment, potential vulnerable components within the CPPS can be identified and security risks and threats can be uncovered, thereby strengthening the protection of critical elements. This is of great significance for CPPS security protection. The results of vulnerability assessment can offer guidance for CPPS security protection. Since security protection is integral throughout the entire operational process of CPPS, this section uses the variations in CPPS operational states as the basis and categorizes CPPS security protection methods based on vulnerability assessment into three phases: normal operational (pre-attack), early stages of attack (post-attack but before significant failure), and fault operation (post-attack with severe failures). It is worth noting that in actual CPPS systems, there is no fundamental cause-and-effect relationship between attacks and faults. An attack on the system does not necessarily result in faults, and faults are not exclusively caused by attacks. The categorization of CPPS operational states into three phases in this paper is solely for the purpose of facilitating the discussion of security protection techniques across different phases while assuming that the system is in a normal state before an attack occurs and that an attack may lead to fault propagation.

As shown in Figure 15, before the attack, the system is in a normal state, and research on risk assessment, proactive defense, online monitoring, and attack warning based on vulnerability assessment can be conducted. First, by quantifying the vulnerability assessment results, the probability of node failure after being attacked and the path of failure propagation can be simulated, thereby assessing the risk of cascading failures in the existing system. Second, proactive defense of the system before an attack serves as the first line of defense against attacks. Designing influencing factors based on vulnerability assessment results, conducting attack modeling (typically, the most severe system damage is used as the objective function), and studying network attack path prediction can help analyze the impact and consequences of network attacks on the system. This, in turn, allows for the rational allocation of defense resources, enhancing the system's ability to withstand attacks from both layers before an attack occurs. Last, online monitoring and attack warning serve

as the second line of defense against attacks. Since vulnerability assessment effectively identifies system vulnerabilities, it has become an effective method for power system monitoring and early warning. By dynamically monitoring key components, operations personnel can take targeted measures at vulnerable nodes (or branches), strengthen data monitoring, and improve the capability to identify and respond to abnormal data. This helps mitigate or avoid cascading failures.

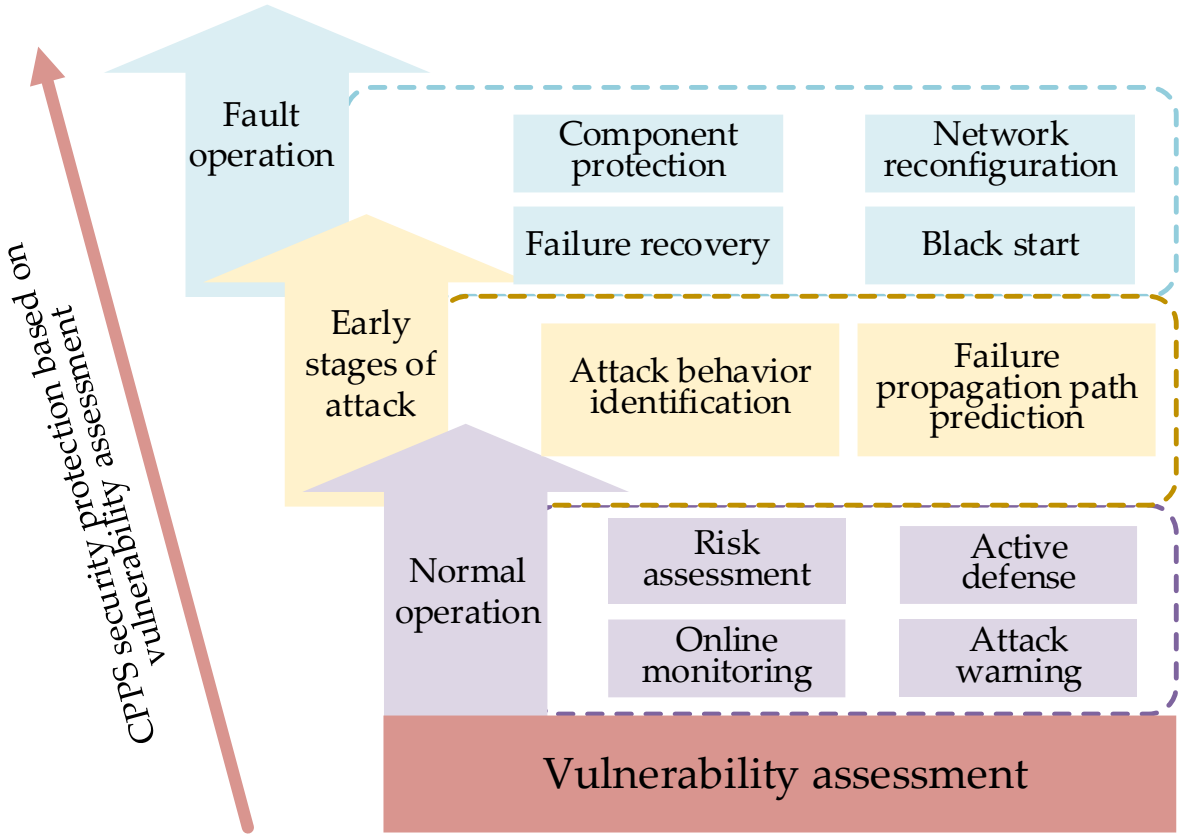

Figure 15. Security protection of CPPS based on vulnerability assessment.

When an attack occurs but severe failures have not yet occurred, it is referred to as the early stages of attack. Vulnerability assessment can be used for attack identification and prediction of failure propagation paths. During vulnerability assessment, system-state awareness and simulated attack modeling are often involved. Based on these data, analysis can be conducted using methods such as state estimation, trajectory prediction, and artificial intelligence to identify attack behaviors and guide defense strategies after failures. Additionally, vulnerability assessment reveals the weak links in the system and high-risk paths of failure propagation. This information can be used to predict failure propagation paths, analyze the consequences of system cascading failures after an attack, and allocate redundant defense resources on both layers to reduce the breadth of failure propagation.

When cascading failures are inevitable, to minimize economic losses caused by structural or functional disruptions of the system, critical components that are highly impactable and susceptible must be protected to reduce propagation time and losses. Vulnerability assessment can identify impactable and susceptible components and infection in the system. Based on this information, adjustments can be made to the topological and operational state after a failure occurs to mitigate failure propagation. Furthermore, the results of the vulnerability assessment can be used for network reconfiguration after cascading failures and provide guidance for failure recovery strategies and black start procedures.

Additionally, the results of dynamic vulnerability assessment can be applied to dynamic attack–defense games. After the system experiences a network attack, it adjusts its defense strategies to minimize losses. Subsequently, the attackers may devise new strategies for further attacks, leading to the system adjusting its defense strategies again. This process constitutes a multistage dynamic attack–defense game, often described using the defend–attack–defend (DAD) model [147,161]. However, adjusting defense strategies involves changes in topology and operational parameters, and the parameter changes in the DAD model must be adjusted offline, making such methods inefficient in practical applications. Based on situation awareness, dynamic vulnerability assessment can identify critical nodes and vulnerable areas in the system in real time and monitor their operational status, enabling the timely understanding of the current vulnerability and the prediction of possible evolutionary trends. During the process of dynamic attack–defense games, the changes in system topology and operations, as well as the results of vulnerability assessment, can be updated in real time. Therefore, dynamic vulnerability assessment can be applied to the formulation of defense strategies and the allocation of defense resources in dynamic attack–defense games.

6.4. Optimization Operation of CPPS Based on Vulnerability Assessment

CPPS operation optimization can be carried out from two aspects: normal operation and fault operation. As shown in Figure 16, under normal operation, vulnerability assessment can be applied to formulate risk-control strategies against attacks. Since the results of vulnerability assessment include overall system status, weak links, and redundant resources, it is possible to mobilize redundant resources to protect critical nodes—for example, through the addition of autonomous nodes or the implementation of edge strategies. Additionally, to achieve the optimization goal of simultaneously protecting critical components and improving system operational efficiency, structural changes in the system are often necessary, and vulnerability assessment can provide insights into network reconfiguration strategies. For instance, based on the results of vulnerability assessment, network topology can be adjusted, coupling methods can be modified to reduce network clustering coefficients, and information transmission efficiency can be enhanced. The network can also be restructured based on node importance rankings.

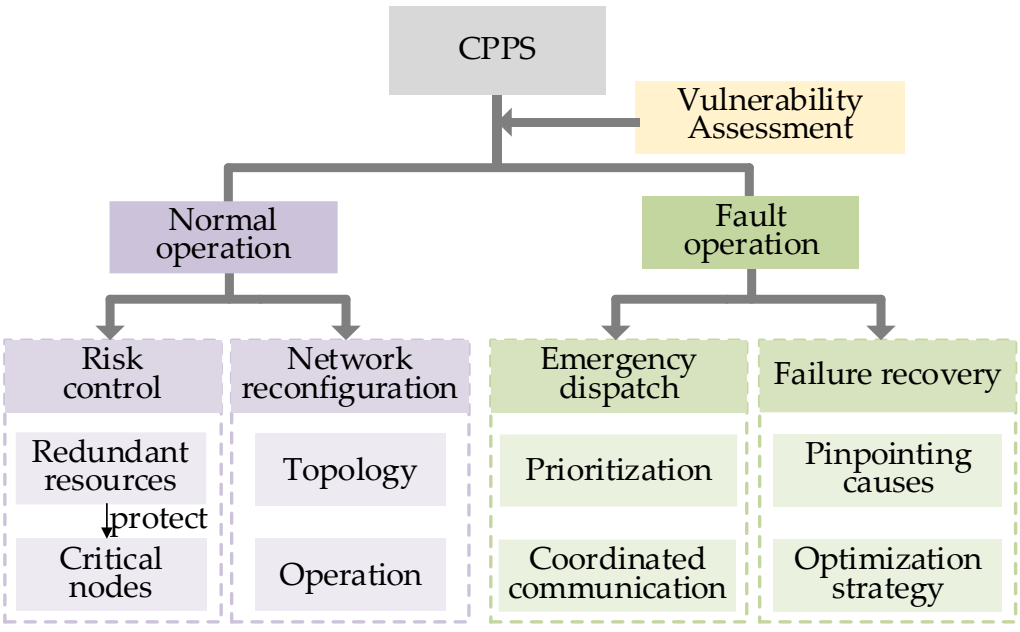

Figure 16. Optimization of CPPS operation based on vulnerability assessment.

In the event of a fault, the system's emergency dispatch faces issues such as information channel congestion and power imbalance. Advanced communication algorithms can play a critical role in emergency dispatch [162]. Furthermore, vulnerability assessment plays a significant role in emergency dispatch. Based on vulnerability assessment, task priorities in emergency dispatch can be determined, potential risks can be assessed, and coordinated communication in emergency dispatch can be guided to minimize the impact of failures. Vulnerability assessment can also provide guidance for fault recovery, pinpointing the cause of the failure and optimizing recovery strategies, such as prioritizing the restoration of critical nodes or easily impactable nodes. These optimized operational strategies will drive the intelligence, autonomy, reliability enhancement, and efficient operation of CPPSs.

Furthermore, based on the results of the dynamic vulnerability assessment, research can be conducted on distributed energy resource allocation strategies, energy storage allocation strategies, and other multistage and multilayer optimization scheduling strategies for CPPSs. This provides insights into the integration of flexible resources and enables access to them in scenarios such as distribution networks with distributed energy resources, power grids with high uncertainties due to the integration of renewable energy sources, electric vehicle-charging scheduling, and microgrid dispatch. These applications show promising prospects.

6.5. Vulnerability Assessment of the Integrated Energy Cyber–Physical System

With the development of the energy internet, future energy systems will involve the integration of energy cyber–physical systems (IECPSs) centered around the power grid, supported by cyber technology, and coupling multiple energy networks. Due to the characteristics of multinetwork coupling, the vulnerability and security risks of IECPSs will increase sharply, posing new challenges to the stability and security of system structure and operation. Some scholars have already conducted research on the vulnerability assessment of IECPSs. A coupling model of the gas–electric cyber–physical system was established, considering the topological and operational characteristics of multiple networks, and its vulnerability was assessed in [163]. A key node identification method for the integrated energy system was proposed in [164] based on complex network theory, considering the topological and operational perspectives.

As shown in Figure 17, vulnerability assessment can be applied to the design, deployment, security protection, and optimization of IECPSs. Based on the vulnerability assessment results, it can promote the large-scale integration of highly uncertain renewable energy sources and improve the stability of new power systems. Additionally, it can provide guidance for the coupling of multiple energy systems and enhance the collaborative operation capability of the energy internet. It helps us identify weak points in the system, discover potential threats, and protect them to ensure the safe operation of the system. Moreover, it can optimize the system's operational scheduling strategies to improve efficiency, robustness, and resilience when facing disturbances.

Currently, there is a scarcity of research on the vulnerability of IECPSs. In the future, vulnerability assessment research can be conducted from the perspective of complex network theory to enhance the reliability and stability of integrated energy networks and achieve optimized scheduling of these networks. This involves multilayer and multiscale modeling of multienergy networks. Such a vast network requires analyzing complexity and uncertainty and designing effective comprehensive vulnerability assessment methods. Additionally, applying the results of vulnerability assessment to the analysis of IECPSs requires further research.

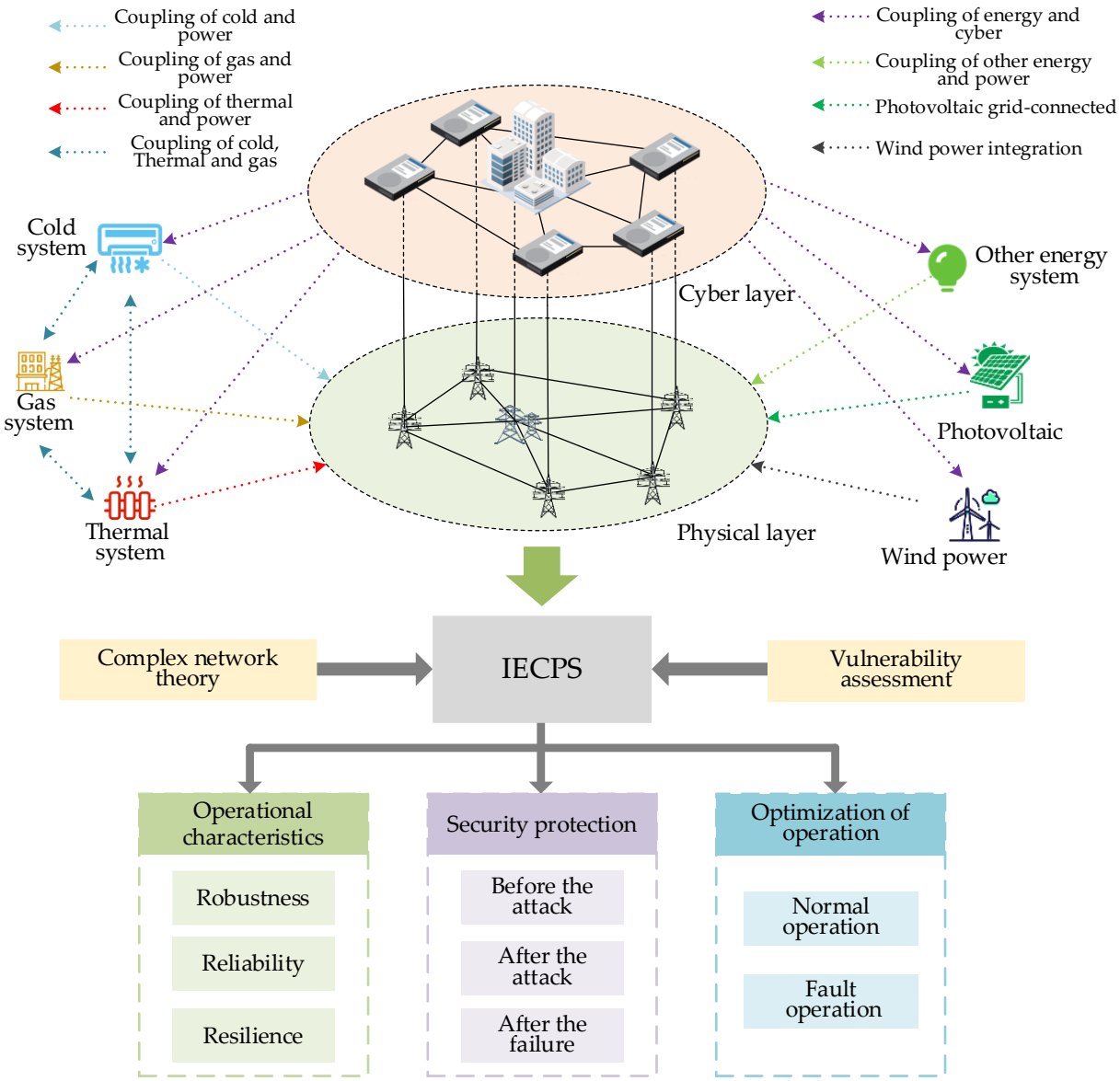

Figure 17. Vulnerability assessment based on complex network theory in IECPS.

7. Conclusions

The CPPS represents a complex system deeply intertwined with both information systems and electrical power systems, and vulnerability is an inherent challenge in any intricate system. Complex network theory possesses the capacity to comprehend complex systems and engage in multilayered analyses, providing an efficient theoretical framework for assessing system vulnerability. Building upon complex network theory, this paper begins by introducing the concepts and definitions of vulnerability assessment, differentiating vulnerability, risk, reliability, and resilience using five parameters and offering an extensive analysis of vulnerability assessment classifications from various perspectives. Subsequently, we attempt to synthesize the existing research framework for vulnerability assessment based on complex network theory into four steps, followed by an in-depth analysis of each step. We delve into the realm of vulnerability assessment research from two perspectives: structural and operational. Within structural vulnerability analysis, we outline both pure vulnerability indices and extended vulnerability indices. In operational vulnerability analysis, we combine operational graphs and summarize an operational vulnerability assessment framework. Furthermore, we delve into the intricate relationship between system vulnerability and cascade failures. Additionally, we introduce the concepts

of multistage coordinated cyber–physical attacks and situation awareness. Within the context of multistage coordinated cyber–physical attacks, we assess the viability of dynamic vulnerability assessment, incorporating situation awareness. On this foundation, we offer a perspective on the potential applications of vulnerability assessment in enhancing the security protection and optimization operation of CPPS. Subsequently, we extend the scope of CPPS vulnerability assessment to IECPS.

For future perspectives, a pivotal research objective for vulnerability assessment lies in its practical application within real systems, moving beyond mere assumptions and simplified models. Nonetheless, current CPPS vulnerability assessment encounters certain limitations, encompassing complexities within real systems, precision in collecting and transmitting power data, the availability of real-time and historical data, uncertainties within vulnerability assessment models, algorithmic efficiency, multistage dynamic vulnerability assessment, and more. These challenges represent the forefront of vulnerability assessment research. High-quality guidance for the maintenance of real systems can only be achieved through rapid, precise vulnerability assessment results. Therefore, it is imperative that not only theoretical research such as vulnerability assessment continue to evolve and innovate but also that critical technologies like situation awareness and artificial intelligence expand. Moreover, as interdisciplinary collaboration deepens, the future of vulnerability assessment will become an amalgamation of multiple fields, with diverse ideas and technologies propelling the development and application of vulnerability assessment.

Author Contributions: Conceptualization, T.Z. and X.W.; methodology, Z.W. and Y.Z.; investigation, Z.W. and Y.Z.; resources, Z.W. and J.W.; writing—original draft preparation, T.Z., Z.W., X.W. and B.Z.; writing—review and editing, T.Z., Z.W., X.W. and J.W.; visualization, X.W. and Z.W.; supervision, T.Z., X.W. and B.Z.; project administration, T.Z. and X.W.; funding acquisition, T.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Science Foundation of China (No. 51907097) and the National Key R&D Program of China (No. 2021YFB4000500).

Data Availability Statement: Not applicable.

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

References

1. Cai, Y.; Huang, T.; Ettore, B.; Cao, Y.; Li, Y. Self-Sustainable Community of Electricity Prosumers in the Emerging Distribution System. *IEEE Trans. Smart Grid* **2017**, *8*, 2207–2216. [CrossRef]
2. Wei, X.; Gao, S.; Zang, T.; Huang, T.; Wang, T.; Li, D. Social Energy Internet: Concept, Architecture and Outlook. *Proc. CSEE* **2018**, *38*, 4969–4986+5295.
3. Gao, S.; Gao, F.; Liu, Y.; Zang, T.; Huang, T.; Chen, K. Prospect of Research on Self-Aware Energy Internet. *Autom. Electr. Power Syst.* **2021**, *45*, 1–17.
4. Chen, Q.; Liu, D.; Lin, J.; He, J.; Wang, Y. Business Models and Market Mechanisms of Energy Internet(1). *Power Syst. Technol.* **2015**, *39*, 3050–3056.
5. Liu, D.; Zeng, M.; Huang, R.; Ji, L.; Chen, Q.; Duan, J.; Li, Y. Business Models and Market Mechanisms of E-Net(2). *Power Syst. Technol.* **2015**, *39*, 3057–3063.
6. He, R.; Long, L.; Zhang, B.; Wang, Y.; Xiao, Z. Cyber System Physicalizing Modeling and Analysis Method in Cyber-Physical Power Systems. *Proc. CSEE* **2022**, 1–14. Available online: http://kns.cnki.net/kcms/detail/11.2107.TM.20220909.1500.002.html (accessed on 21 August 2023).
7. Zhang, Y.; Liu, W.; Liu, G.; Huang, S. Modeling and Vulnerability Analysis of Electric Cyber Physical System Considering Topological Correlation and Double Coupling. *Proc. CSEE* **2021**, *41*, 5486–5500.
8. Yuan, H.; Niu, F.; Gao, X. Establishment and Application of an Urban Economic Vulnerability Evaluation System. *Acta Geogr. Sin.* **2015**, *70*, 271–282.
9. Wang, Y.; Lan, H. Fresh Agricultural Products Supply Chain in the E-Commerce Environment Vulnerability Model. In Proceedings of the 2015 International Conference on Logistics, Informatics and Service Sciences (LISS), Barcelona, Spain, 27–29 July 2015; pp. 1–4.
10. Aretano, R.; Semeraro, T.; Petrosillo, I.; Marco, A.D.; Pasimeni, M.R.; Zurlini, G. Mapping Ecological Vulnerability to Fire for Effective Conservation Management of Natural Protected Areas. *Ecol. Model.* **2015**, *295*, 163–175. [CrossRef]
11. He, L.; Shen, J.; Zhang, Y. Ecological Vulnerability Assessment for Ecological Conservation and Environmental Management. *J. Environ. Manag.* **2018**, *206*, 1115–1125. [CrossRef] [PubMed]

12. Du, W.; Mathur, A.P. Testing for Software Vulnerability Using Environment Perturbation. *Qual. Reliab. Eng. Int.* **2002**, *18*, 261–272. [CrossRef]
13. Rahimi, S.; Zargham, M.R. Vulnerability Scrying Method for Software Vulnerability Discovery Prediction Without a Vulnerability Database. *IEEE Trans. Reliab.* **2013**, *62*, 395–407. [CrossRef]
14. Rodríguez-Núñez, E.; García-Palomares, J.C. Measuring the Vulnerability of Public Transport Networks. *J. Transp. Geogr.* **2014**, *35*, 50–63. [CrossRef]
15. Cats, O.; Jenelius, E. Dynamic Vulnerability Analysis of Public Transport Networks: Mitigation Effects of Real-Time Information. *Netw. Spat. Econ.* **2014**, *14*, 435–463. [CrossRef]
16. Panteli, M.; Trakas, D.N.; Mancarella, P.; Hatziargyriou, N.D. Boosting the Power Grid Resilience to Extreme Weather Events Using Defensive Islanding. *IEEE Trans. Smart Grid* **2016**, *7*, 2913–2922. [CrossRef]
17. Mathaios, P.; Cassandra, P.; Sean, W.; Richard, D.; Pierluigi, M. Power System Resilience to Extreme Weather: Fragility Modeling, Probabilistic Impact Assessment, and Adaptation Measures. *IEEE Trans. Power Syst.* **2017**, *32*, 3747–3757.
18. Bompard, E.; Huang, T.; Wu, Y.; Cremenescu, M. Classification and Trend Analysis of Threats Origins to the Security of Power Systems. *Int. J. Electr. Power Energy Syst.* **2013**, *50*, 50–64. [CrossRef]
19. Anderson, C.W.; Santos, J.R.; Haimes, Y.Y. A Risk-Based Input-Output Methodology for Measuring the Effects of the August 2003 Northeast Blackout. *Econ. Syst. Res.* **2007**, *19*, 183–204. [CrossRef]
20. Ralph, L. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51.
21. Mao, A.; Zhang, G.; Lü, Y.; Gao, J. Analysis on Large-Scale Blackout Occurred in South America and North Mexico Interconnected Power Grid on Sept. 8, 2011 and Lessons for Electric Power Dispatching in China. *Power Syst. Technol.* **2012**, *36*, 74–78.
22. Tang, Y.; Bu, G.; Yi, J. Analysis and Lessons of the Blackout in Indian Power Grid on July 30 and 31. *Proc. CSEE* **2012**, *32*, 167–174.
23. Guo, Q.; Xin, S.; Wang, J.; Sun, H. Comprehensive Security Assessment for a Cyber Physical Energy System a Lesson from Ukraine's Blackout. *Autom. Electr. Power Syst.* **2016**, *40*, 145–147.
24. Zeng, H.; Sun, F.; Li, T.; Zhang, Q.; Tang, J.; Zhang, T. Analysis of "9.28" Blackout in South Australia and Its Enlightenment to China. *Autom. Electr. Power Syst.* **2017**, *41*, 1–6.
25. Bai, J.; Liu, T.; Cao, G.; Chen, C. A Survey Vulnerability Assessment Method for Power System. *Power Syst. Technol.* **2008**, *32*, 26–30.
26. Liu, C.C.; Jung, J.; Heydt, G.T.; Vittal, V.; Phadke, A.G. The Strategic Power Infrastructure Defense (SPID) System. A Conceptual Design. *IEEE Control Syst. Mag.* **2000**, *20*, 40–52.
27. Li, Q.; Cao, Z.; Tanveer, M.; Pandey, H.M.; Wang, C. An Effective Reliability Evaluation Method for Power Communication Network Based on Community Structure. *IEEE Trans. Ind. Appl.* **2019**, *56*, 4489–4500. [CrossRef]
28. Huang, T.; Voronca, S.L.; Purcarea, A.A.; Estebsari, A.; Bompard, E. Analysis of Chain of Events in Major Historic Power Outages. *Adv. Electr. Comput. Eng.* **2014**, *14*, 63–70. [CrossRef]
29. Fouad, A.A.; Zhou, Q.; Vittal, V. System Vulnerability as a Concept to Assess Power System Dynamic Security. *IEEE Trans. Power Syst. A Publ. Power Eng. Soc.* **1994**, *9*, 1009–1015. [CrossRef]
30. Zhou, Q.; Davidson, J.; Fouad, A.A. Application of Artificial Neural Networks in Power System Security and Vulnerability Assessment. *IEEE Trans. Power Syst. A Publ. Power Eng. Soc.* **1994**, *9*, 525–532. [CrossRef]
31. Tamronglak, S.; Horowitz, S.H.; Phadke, A.G.; Thorp, J.S. Anatomy of Power System Blackouts: Preventive Relaying Strategies. *IEEE Trans. Power Deliv.* **1996**, *11*, 708–715. [CrossRef]
32. Phadke, A.G.; Thorp, J.S. Expose Hidden Failures to Prevent Cascading Outages [in Power Systems]. *IEEE Comput. Appl. Power* **1996**, *9*, 20–23. [CrossRef]
33. Liang, J.; Sankar, L.; Kosut, O. Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation. *IEEE Trans. Power Syst. A Publ. Power Eng. Soc.* **2016**, *31*, 3864–3872. [CrossRef]
34. Bompard, E.; Napoli, R.; Xue, F. Vulnerability of Interconnected Power Systems to Malicious Attacks under Limited Information. *Int. Trans. Electr. Energy Syst.* **2013**, *18*, 820–834. [CrossRef]
35. Mohagheghi, S.; Javanbakht, P. Power Grid and Natural Disasters: A Framework for Vulnerability Assessment. In Proceedings of the 2015 Seventh Annual IEEE Green Technologies Conference, New Orleans, LA, USA, 15–17 April 2015; pp. 199–205.
36. Kwasinski, A. Analysis of Vulnerabilities of Telecommunication Systems to Natural Disasters. In Proceedings of the 2010 IEEE International Systems Conference, San Diego, CA, USA, 5–8 April 2010; pp. 359–364.
37. Rodriguez, C.M.F. *Vulnerability and Robustness Indices against Blackouts in Power Grids*; Alma Mater Studiorum—Università di Bologna: Bologna, Italy, 2013.
38. Johansson, J.; Hassel, H.; Zio, E. Reliability and Vulnerability Analyses of Critical Infrastructures: Comparing Two Approaches in the Context of Power Systems. *Reliab. Eng. Syst. Saf.* **2013**, *120*, 27–38. [CrossRef]
39. Office of Energy Assurance. *Vulnerability Assessment Methodology—Electric Power Infrastructure*; Department of Energy: Washington, DC, USA, 2002.
40. Terje, A. On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience. *Risk Anal.* **2011**, *31*, 515–522.
41. McCalley, J.D.; Vittal, V.; Abi-Samra, N. An Overview of Risk Based Security Assessment. In Proceedings of the 1999 IEEE Power Engineering Society Summer Meeting. Conference Proceedings (Cat. No. 99CH36364), Edmonton, AB, Canada, 18–22 July 1999; Volume 1, pp. 173–178.

42. Feng, Y.; Wu, W.; Zhang, B.; Li, W. Power System Operation Risk Assessment Using Credibility Theory. *IEEE Trans. Power Syst.* **2008**, *23*, 1309–1318. [CrossRef]
43. Blockley, D.I.; Agarwal, J.; Pinto, J.T.; Woodman, N.J. Structural Vulnerability, Reliability and Risk. *Prog. Struct. Eng. Mater.* **2002**, *4*, 203–212. [CrossRef]
44. Guo, Y. *Power System Reliability Analysis*; Tsinghua University Press: Beijing, China, 2003.
45. Allan, R. Power System Reliability Assessment—A Conceptual and Historical Review. *Reliab. Eng. Syst. Saf.* **1994**, *46*, 3–13. [CrossRef]
46. Chen, L.; Guo, Y. Transient Energy Function Algorithm for Reliability Security Evaluation. *J. Tsinghua Univ. (Sci. Technol.)* **2001**, *41*, 5–8.
47. Panteli, M.; Mancarella, P. The Grid: Stronger, Bigger, Smarter?: Presenting a Conceptual Framework of Power System Resilience. *IEEE Power Energy Mag.* **2015**, *13*, 58–66. [CrossRef]
48. Gu, C.; Tang, Q.; Shen, Y. N-1 Reliability of 220kV Power Grid under Maintenance. *East China Electr. Power* **2014**, *42*, 2369–2372.
49. Bie, Z.; Lin, Y.; Qiu, A. Concept and Research Prospects of Power System Resilience. *Autom. Electr. Power Syst.* **2015**, *39*, 1–9.
50. Chaudry, M.; Ekins, P.; Ramachandran, K.; Shakoor, A.; Skea, J.; Strbac, G.; Wang, X.; Whitaker, J. *Building a Resilient UK Energy System*; UK Energy Research Center(UKERC): London, UK, 2011.
51. National Infrastructure Advisory Council. *A Framework for Establishing Critical Infrastructure Resilience Goals*; National Infrastructure Advisory Council: Washington, DC, USA, 2010.
52. Bie, Z.; Lin, Y.; Li, G.; Li, F. Battling the Extreme: A Study on the Power System Resilience. *Proc. IEEE* **2017**, *105*, 1253–1266. [CrossRef]
53. Huang, G.; Wang, J.; Chen, C.; Qi, J.; Chuangxin, G. Integration of Preventive and Emergency Responses for Power Grid Resilience Enhancement. *IEEE Trans. Power Syst.* **2017**, *32*, 4451–4463. [CrossRef]
54. Zhou, X.; Ge, S.; Li, T.; Liu, H. Assessing and Boosting Resilience of Distribution System under Extreme Weather. *Proc. CSEE* **2018**, *38*, 505–513+681.
55. Wang, C.; Hou, Y.; Qiu, F.; Lei, S.; Liu, K. Resilience Enhancement With Sequentially Proactive Operation Strategies. *IEEE Trans. Power Syst.* **2017**, *32*, 2847–2857. [CrossRef]
56. Zio, E. Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures. *Reliab. Eng. Syst. Saf.* **2016**, *152*, 137–150. [CrossRef]
57. Bompard, E.; Wu, D.; Xue, F. Structural Vulnerability of Power Systems: A Topological Approach. *Electr. Power Syst. Res.* **2011**, *81*, 1334–1340. [CrossRef]
58. Wang, A.; Luo, Y.; Tu, G.; Liu, P. Vulnerability Assessment Scheme for Power System Transmission Networks Based on the Fault Chain Theory. *IEEE Trans. Power Syst. A Publ. Power Eng. Soc.* **2011**, *26*, 442–450. [CrossRef]
59. Liu, Y.; Hu, B.; Liu, J.; Ding, L.; Xu, W.; Song, Z.; Li, Y. Power System Cascading Failure Analysis Theories and Application I—Related Theories and Application. *Power Syst. Prot. Control* **2013**, *41*, 148–155.
60. Liu, Y.; Xu, W.; Ding, L.; Liu, J.; Hu, B.; Song, Z.; Xu, L. Power System Cascading Failure Analysis Theories and Application II—Key Features of Real Cascading Failures and Revelation Aspects. *Power Syst. Prot. Control* **2013**, *41*, 146–155.
61. Ding, M.; Han, P. Small-World Topological Model Based Vulnerability Assessment Algorithm for Large-Scale World Power Grid. *Autom. Electr. Power Syst.* **2006**, *8*, 7–10+40.
62. Juan, T.; Diego, C.; Manuel, J. An Electrical Power System Reconfiguration Model Based on Optimal Transmission Switching under Scenarios of Intentional Attacks. *Energies* **2023**, *16*, 2879.
63. Fang, Y.; Sansavini, G. Optimizing Power System Investments and Resilience against Attacks. *Reliab. Eng. Syst. Saf.* **2017**, *159*, 161–173. [CrossRef]
64. Sang, M.; Bao, M.; Ding, Y.; Xue, Y.; Yang, Y. Identification of Vulnerable Lines in Power Grid Considering Impact of Natural Gas Network. *Autom. Electr. Power Syst.* **2019**, *43*, 34–43.
65. Wei, X.; Gao, S.; Huang, T.; Wang, T.; Fan, W. Identification of Two Vulnerability Features: A New Framework for Electrical Networks Based on the Load Redistribution Mechanism of Complex Networks. *Complexity* **2019**, *2019*, 3531209. [CrossRef]
66. Wei, X.; Gao, S.; Huang, T.; Wang, T.; Zang, T. Electrical Network Operational Vulnerability Evaluation Based on Small-World and Scale-Free Properties. *IEEE Access* **2019**, *7*, 181072–181082. [CrossRef]
67. Sergiou, C.; Lestas, M.; Antoniou, P.; Liaskos, C.; Pitsillides, A. Complex Systems: A Communication Networks Perspective Towards 6G. *IEEE Access* **2020**, *8*, 89007–89030. [CrossRef]
68. Wei, Z.; Liu, J.; Li, J.; Han, W.; Pan, R. Vulnerability Analysis of Electric Power Network under a Directed-Weighted Topological Model Based on the P-Q Networks Decomposition. *Power Syst. Prot. Control* **2010**, *38*, 19–22.
69. Song, X. Complexity, Complex System, and the Science of Complexity. *Bull. Natl. Nat. Sci. Found. China* **2003**, *17*, 262–268.
70. Wei, Z.; Gou, J. An Overview on Application of Complex Network Theory in Power System Analysis. *Power Syst. Technol.* **2015**, *39*, 279–287.
71. Li, J.; Wang, H. Analysis on Power Grids and Blackouts with Complex Network Theory. *Comput. Technol. Dev.* **2008**, *18*, 247–249+253.
72. Chen, W.; Jiang, Q.; Cao, Y.; Han, Z. Risk Based Vulnerability Assessment in Complex Power Systems. *Power Syst. Technol.* **2005**, *29*, 12–17.

73. Wang, X.; Zhu, G.; He, R.; Tian, M.; Dong, Z.; Dai, D.; Long, J.; Zhao, L.; Zhang, Q. Survey of Cascading Failures in Cyber Physical Power System Based on Complex Network Theory. *Power Syst. Technol.* **2017**, *41*, 2947–2956.
74. Parisa, R.; Abbas, J. Toward the Evolution of Wireless Powered Communication Networks for the Future Internet of Things. *IEEE Netw.* **2017**, *31*, 62–69.
75. Gupta, A.; Bokde, N.; Kulat, K.D. Hybrid Leakage Management for Water Network Using PSF Algorithm and Soft Computing Techniques. *Water Resour. Manag.* **2018**, *32*, 1133–1151. [CrossRef]
76. Dobson, J.; Carreras, B.A.; Lynch, V.E. Complex Systems Analysis of Series of Blackouts: Cascading Failure, Criticality, and Self-Organization. *Chaos Interdiscip. J. Nonlinear Sci.* **2007**, *17*, 026103. [CrossRef] [PubMed]
77. Liu, Y.; Liu, J.; Yang, J.; Wang, M. Stage Vulnerability of Power Grid and Its Alert Vulnerability Based on Faults Evolution. *Power Syst. Technol.* **2011**, *35*, 46–52.
78. Huang, Z.; Li, H.; Du, T.; Lin, M. Vulnerable branch assessment based on branch energy function. *Power Syst. Prot. Control* **2012**, *40*, 7–11+115.
79. Guo, H.; Yu, S.S.; Iu, H.H.; Fernando, T.; Zheng, C. A Complex Network Theory Analytical Approach to Power System Cascading Failure-From a Cyber-Physical Perspective. *Chaos* **2019**, *29*, 053111. [CrossRef]
80. Bai, W.; Wang, B.; Zhou, T. Brief Review of Blackouts on Electric Power Grids in Viewpoint of Complex Networks. *Complex Syst. Complex. Sci.* **2005**, *2*, 29–37.
81. Hu, D.; Wo, J. Virtual Circuit System of Smart Substations Based on IEC61850. *Autom. Electr. Power Syst.* **2010**, *34*, 78–82.
82. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic Cascade of Failures in Interdependent Networks. *Nature* **2010**, *464*, 1025–1028. [CrossRef] [PubMed]
83. Jiang, J.; Xia, Y.; Xu, S.; Shen, H.-L.; Wu, J. An Asymmetric Interdependent Networks Model for Cyber-Physical Systems. *Chaos* **2020**, *30*, 053135. [CrossRef]
84. Ji, X.; Wang, B.; Liu, D.; Zhao, T. Review on Interdependent Networks Theory and Its Applications in the Structural Vulnerability Analysis of Electrical Cyber-Physical System. *Proc. CSEE* **2016**, *36*, 4521–4533.
85. Wang, Y.; Liu, D.; Lu, Y. Research on Hybrid System Modeling Method of Cyber Physical System for Power Grid. *Proc. CSEE* **2016**, *36*, 1464–1470.
86. Bu, L.; Wang, Q.; Chen, X.; Wang, L.; Zhang, T.; Zhao, J.; Li, X. Toward Online Hybrid Systems Model Checking of Cyber-Physical Systems' Time-Bounded Short-Run Behavior. *ACM SIGBED Rev.* **2011**, *8*, 7–10. [CrossRef]
87. Amir, B.; Roni, P.; Shlomo, H. Percolation in Networks Composed of Connectivity and Dependency Links. *Phys. Rev. E* **2011**, *83*, 051127.
88. Wang, T.; Sun, C.; Gu, X.; Qin, X. Modeling and Vulnerability Analysis of Electric Power Communication Coupled Network. *Proc. CSEE* **2018**, *38*, 3556–3567. [CrossRef]
89. Zeng, Z.; Liu, D. Study on Cyber-Physical System Modeling on Coordinated Control of Photovoltaic Generation and Battery Energy Storage System. *Power Syst. Technol.* **2013**, *37*, 1506–1513.
90. Cao, Y.; Chen, X.; Sun, K. Identification of Vulnerable Lines in Power Grid Based on Complex Network Theory. *Electr. Power Autom. Equip.* **2006**, *26*, 1–5.
91. Yan, J.; He, H.; Sun, Y. Integrated Security Analysis on Cascading Failure in Complex Networks. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 451–463. [CrossRef]
92. Bai, H.; Miao, S. Hybrid Flow Betweenness Approach for Identification of Vulnerable Line in Power System. *IET Gener. Transm. Distrib.* **2015**, *9*, 1324–1331. [CrossRef]
93. Bompard, E.; Pons, E.; Wu, D. Extended Topological Metrics for the Analysis of Power Grid Vulnerability. *IEEE Syst. J.* **2012**, *6*, 481–487. [CrossRef]
94. Zhou, B.; Cai, Y.; Zang, T.; Wu, J.; Sun, B.; Chen, S. Reliability Assessment of Cyber–Physical Distribution Systems Considering Cyber Disturbances. *Appl. Sci.* **2023**, *13*, 3452. [CrossRef]
95. Wang, K.; Zhang, B.; Zhang, Z.; Yin, X.; Wang, B. An Electrical Betweenness Approach for Vulnerability Assessment of Power Grids Considering the Capacity of Generators and Load. *Phys. A Stat. Mech. Its Appl.* **2011**, *390*, 4692–4701. [CrossRef]
96. Zhu, Y.; Yan, J.; Tang, Y.; Sun, Y.L.; He, H. Resilience Analysis of Power Grids Under the Sequential Attack. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 2340–2354. [CrossRef]
97. Xu, L.; Wang, X.; Wang, X. Electric Betweenness and Its Application in Vulnerable Line Identification in Power System. *Proc. CSEE* **2010**, *30*, 33–39.
98. Wei, X.; Gao, S.; Li, D.; Huang, T.; Pi, R.; Wang, T. Cascading Fault Graph for the Analysis of Transmission Network Vulnerability under Different Attacks. *Proc. CSEE* **2018**, *38*, 465–474.
99. Crucitti, P.; Latora, V.; Marchiori, M. A Topological Analysis of the Italian Electric Power Grid. *Phys. A Stat. Mech. Its Appl.* **2004**, *338*, 92–97. [CrossRef]
100. Albert, R.; Albert, I.; Nakarado, G.L. Structural Vulnerability of the North American Power Grid. *Phys. Rev. E Stat. Nonlinear Soft Matter Phys.* **2004**, *69*, 025103. [CrossRef]
101. Bilis, E.I.; Kröger, W.; Nan, C. Performance of Electric Power Systems Under Physical Malicious Attacks. *IEEE Syst. J.* **2013**, *7*, 854–865. [CrossRef]
102. Sanchez, E.C.; Hines, P.D.H.; Barrows, C.; Blumsack, S. Comparing the Topological and Electrical Structure of the North American Electric Power Infrastructure. *IEEE Syst. J.* **2012**, *6*, 616–626. [CrossRef]

103. Barthélemy, M. Betweenness Centrality in Large Complex Networks. *Eur. Phys. J. B* **2004**, *38*, 163–168. [CrossRef]
104. Meghanathan, N. Spectral Radius as a Measure of Variation in Node Degree for Complex Network Graphs. In Proceedings of the 2015 7th International Conference on u-and e-Service, Science and Technology, Haikou, China, 25–28 November 2015.
105. Lagonotte, P.; Sabonnadiere, J.C.; Leost, J.Y.; Paul, J.P. Structural Analysis of the Electrical System: Application to Secondary Voltage Control in France. *IEEE Trans. Power Syst. A Publ. Power Eng. Soc.* **1989**, *4*, 479–486. [CrossRef]
106. Zhu, B.; Guo, Y.; Li, C.; Jiang, Z.; Zhang, X.; Yuan, X. A Suvey of the Security Assessment and Securtity Defense of a Cyber Physical Power System Under Cyber Failure Threat. *Power Syst. Prot. Control* **2021**, *49*, 178–187.
107. Shannon, C.E. A Mathematical Theory of Communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
108. Zhang, G.; Zhong, H. Review and Prospect of Information Entropy and Its Applications in Power Systems. *Proc. CSEE* **2023**, *43*, 6155–6181. [CrossRef]
109. Ding, M.; Han, P. Vulnerability Assessment to Small-World Power Grid Based on Weighted Topological Model. *Proc. CSEE* **2008**, *28*, 20–25.
110. Xie, Q.; Deng, C.; Zhao, H.; Weng, Y. Evaluation Method for Node Importance of Power Grid Based on the Weighted Network Model. *Autom. Electr. Power Syst.* **2009**, *33*, 21–24.
111. Cai, Y.; Cao, Y.; Li, Y.; Huang, X.; Tan, Y. Identification of Vulnerable Lines in Urban Power Grid Based on Voltage Grad and Running State. *Proc. CSEE* **2014**, *34*, 2124–2131.
112. Dwivedi, A.; Yu, X. A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis. *IEEE Trans. Ind. Inform.* **2013**, *9*, 81–88. [CrossRef]
113. Nasiruzzaman, A.B.M.; Pota, H.R.; Akter, M.N. Vulnerability of the Large-Scale Future Smart Electric Power Grid. *Phys. A Stat. Mech. Its Appl.* **2014**, *413*, 11–24. [CrossRef]
114. Han, C.; Lin, Z.; Yang, L.; Lin, J.; Liu, Y.; Zhu, J. Multi-Dimensional Critical Line Identification for Regional Power Systems under Typhoon. *Autom. Electr. Power Syst.* **2018**, *42*, 118–125.
115. He, J.; Pang, S.; Yu, B.; Zhang, W.; Linq, H.; Liu, Y. Vulnerable Line Identification of Power Grid Based on Capacity Betweenness Index. *Power Syst. Prot. Control* **2013**, *41*, 30–35.
116. Fang, J.; Su, C.; Chen, Z.; Sun, H.; Per, L. Power System Structural Vulnerability Assessment Based on an Improved Maximum Flow Approach. *IEEE Trans. Smart Grid* **2018**, *9*, 777–785. [CrossRef]
117. Zhang, G.; Zhang, J.; Yang, J.; Wang, C.; Zhang, Y.; Duan, M. Vulnerability Assessment of Bulk Power Grid Based on Weighted Directional Graph and Complex Network Theory. *Electr. Power Autom. Equip.* **2009**, *29*, 21–26.
118. Ju, W.; Li, Y. Identification of Critical Lines and Nodes in Power Grid Based Maximum Flow Transmission Contribution Degree. *Autom. Electr. Power Syst.* **2012**, *36*, 6–12.
119. Xu, L.; Liu, J.; Liu, Y.; Liu, Y.; Gou, J.; Masoud, B. Node Importance Classified Comprehensive Assessment. *Proc. CSEE* **2014**, *34*, 1609–1617.
120. Liu, L.; Liu, J.; Wei, Z.; Gong, H. Transmission Line Vulnerability Assessment Based on Synergetic Effect Analysis. *Electr. Power Autom. Equip.* **2016**, *36*, 30–37.
121. Bompard, E.; Napoli, R.; Xue, F. Extended Topological Approach for the Assessment of Structural Vulnerability in Transmission Networks. *IET Gener. Transm. Distrib.* **2010**, *4*, 716–724. [CrossRef]
122. Wei, Z.; Liu, J.; Zhu, G.; Zhu, K.; Liu, Y.; Wang, M. Vulnerability Evaluation Model to Power Grid Based on Reliability-Parameter-Weighted Topological Model. *Trans. China Electrotech. Soc.* **2010**, *25*, 131–137.
123. Ma, J.; Wang, X.; Wang, Z. Operation Betweenness Based Assessment on Overload Vulnerability. *Power Syst. Technol.* **2012**, *36*, 47–50.
124. Xu, Q.; Wang, W.; Liu, J.; Liu, Z.; Xin, J.; Xu, Q. Application of Weighted Electric Betweenness Considering Sensitivity Factor in Identification of Vulnerable Grid Lines. *Electr. Power Autom. Equip.* **2013**, *33*, 53–58.
125. Liu, W.; Liang, C.; Xu, P.; Dan, Y.; Wang, J.; Wang, W. Indetification of Critical Line in Power Systems Based on Flow Betweenness. *Proc. CSEE* **2013**, *33*, 90–98.
126. Huang, Y.; Li, H.; Huang, T.; Li, Q.; Zheng, G. Branch Transient Vulnerability Assessment Based on the Complex Network and Transient Energy Function. *Power Syst. Prot. Control* **2014**, *42*, 69–74.
127. Liu, Y.; Liu, J.; Wang, M.; Yang, J. Fast Assessment Method for Transient Vulnerability of Transmission Lines Based on Kinetic Energy Injection Betweenness. *Proc. CSEE* **2011**, *31*, 40–47.
128. Xu, J.; Chen, C.; Luo, C.; Chen, X.; Xiong, W.; Lin, X. Identification of Power Grid Key Parts Based on Improved Complex Network Model. *Autom. Electr. Power Syst.* **2016**, *40*, 53–61.
129. Wei, X.; Zhao, J.; Huang, T.; Ettore, B. A Novel Cascading Faults Graph Based Transmission Network Vulnerability Assessment Method. *IEEE Trans. Power Syst.* **2018**, *33*, 2995–3000. [CrossRef]
130. Wei, X.; Gao, S.; Huang, T.; Bompard, E.; Pi, R.; Wang, T. Complex Network-Based Cascading Faults Graph for the Analysis of Transmission Network Vulnerability. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1265–1276. [CrossRef]
131. Zhu, Y.; Yan, J.; Sun, Y.; He, H. Revealing Cascading Failure Vulnerability in Power Grids Using Risk-Graph. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 3274–3284. [CrossRef]
132. Hines, P.D.H.; Dobson, L.; Rezaei, P. Cascading Power Outages Propagate Locally in an Influence Graph That Is Not the Actual Grid Topology. *IEEE Trans. Power Syst.* **2016**, *32*, 958–967. [CrossRef]

133. Qi, J.; Sun, K.; Mei, S. An Interaction Model for Simulation and Mitigation of Cascading Failures. *IEEE Trans. Power Syst.* **2015**, *30*, 804–819. [CrossRef]
134. Ju, W.; Sun, K.; Qi, J. Multi-Layer Interaction Graph for Analysis and Mitigation of Cascading Outages. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2017**, *7*, 239–249. [CrossRef]
135. Wang, T.; Wei, X.; Huang, T.; Wang, J.; Peng, H.; Pérez-Jiménez, M.J.; Valencia-Cabrera, L. Modeling Fault Propagation Paths in Power Systems: A New Framework Based on Event SNP Systems With Neurotransmitter Concentration. *IEEE Access* **2019**, *7*, 12798–12808. [CrossRef]
136. Zhao, L.; Kwangho, P.; Lai, Y. Attack Vulnerability of Scale-Free Networks Due to Cascading Breakdown. *Phys. Rev. E Stat. Nonlinear Soft Matter Phys.* **2004**, *70*, 035101. [CrossRef]
137. Dong-Hee, K.; Jun, K.B.; Hawoong, J. Universality Class of the Fiber Bundle Model on Complex Networks. *Phys. Rev. Lett.* **2005**, *94*, 025501.
138. Watts, D.J.; Strogatz, S.H. Collective Dynamics of "small-World" Networks. *Nature* **1998**, *393*, 440–442. [CrossRef]
139. Surdutovich, G.; Cortez, C.; Vitilina, R. Dynamics of 'Small-World' Networks and Vulnerability of the Electric Power Gird. In Proceedings of the VIII Symposium of Specialists in Electric Operational and Expansion Planning, Brsilia, Brazil, 17 May 2002.
140. Monfared, M.A.S.; Jalili, M.; Alipour, Z. Topology and Vulnerability of the Iranian Power Grid. *Phys. A Stat. Mech. Its Appl.* **2014**, *406*, 24–33. [CrossRef]
141. Meng, Z.; Lu, Z.; Song, J. Comparison Analysis of the Small-Word Topological Model of Chinese and American Power Grids. *Autom. Electr. Power Syst.* **2004**, *28*, 21–24.
142. Zhou, B.; Sun, B.; Zang, T.; Cai, Y.; Wu, J.; Luo, H. Security Risk Assessment Approach for Distribution Network Cyber Physical Systems Considering Cyber Attack Vulnerabilities. *Entropy* **2022**, *25*, 47. [CrossRef]
143. Wang, Q.; Li, M.; Tang, Y.; Ni, M. A Review on Research of Cyber-Attack and Defense in Cyber Physical Power System Part One Modelling and Evaluation. *Autom. Electr. Power Syst.* **2019**, *43*, 9–21.
144. Hosseinzadeh, M.; Sinopoli, B.; Garone, E. Feasibility and Detection of Replay Attack in Networked Constrained Cyber-Physical Systems. In Proceedings of the 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, VA, USA, 24–27 September 2019; pp. 712–717.
145. Tran, T.-T.; Shin, O.-S.; Lee, J.-H. Detection of Replay Attacks in Smart Grid Systems. In Proceedings of the 2013 International Conference on Computing, Management and Telecommunications (ComManTel), Ho Chi Minh, Vietnam, 21–24 January 2013; pp. 298–302.
146. Zhou, B.; Min, X.; Zang, T.; Zhang, Y.; Chen, Y.; Zhao, W. Loss Assessment and Vulnerability Analysis of an Intergrated Electricity Natural Gas System Under Load Redistribution Attack. *Adv. Eng. Sci.* **2023**, *55*, 3–13.
147. 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.
148. Ruan, Z.; Lü, L.; Liu, Y.; Liu, J.; Wang, D.; Huang, L. Coordinated Attack Model of Cyber-Physical Power System Considering False Load Data Injection. *Electr. Power Autom. Equip.* **2019**, *39*, 181–187.
149. Cao, M.; Wang, L.; Hu, B.; Xie, K.; Fu, J.; Wen, L.; Zhou, P.; Fan, X.; Li, B.; Zeng, Y. Coordinated Cyber-Physical Multi-Stage Attack Strategy Considering Cascading Failure of Intergrated Electricity-Natural Gas System. *Electr. Power Autom. Equip.* **2019**, *39*, 128–136.
150. Ge, L.; Li, Y.; Li, Y.; Yan, J.; Sun, Y. Smart Distribution Network Situation Awareness for High-Quality Operation and Maintenance: A Brief Review. *Energies* **2022**, *15*, 828. [CrossRef]
151. Hu, F.; Chen, L.; Chen, J. Cascading Failure Modeling and Robustness Evaluation Evaluation Based on Power Flow. *Power Syst. Prot. Control* **2021**, *49*, 35–43.
152. Zou, Y.; Li, H. Study on Power Grid Partition and Attack Strategies Based on Complex Networks. *Front. Phys.* **2022**, *9*, 790218. [CrossRef]
153. Pan, H.; Lian, H.; Na, C.; Li, X. Modeling and Vulnerability Analysis of Cyber-Physical Power Systems Based on Community Theory. *IEEE Syst. J.* **2020**, *14*, 3938–3948. [CrossRef]
154. Jia, C.; Li, M.; Liu, R. Percolation and Cascading Dynamics on Multilayer Complex Networks. *J. Univ. Electron. Sci. Technol. China* **2022**, *51*, 148–160.
155. Sun, K.; Wang, D.; Ge, X.; Wang, W.; Sun, W. Topological Evolution Model of Power System Based on Positioning Probability and Attenuation Mechanism. *Proc. CSU-EPSA* **2021**, *33*, 22–28.
156. Beng, L.Y.; Abdulrazzaq, K.A.; Selvakumar, M.; Samer, A.S. An Adaptive Assessment and Prediction Mechanism in Network Security Situation Awareness. *J. Comput. Sci.* **2017**, *13*, 114–129.
157. Chen, H.; Hu, Z.; Chen, S.; Yang, Y.; Fan, S. Research on Security Situation Awareness Method of Power Network Monitoring System Based on Data Mining. *J. Phys. Conf. Ser.* **2022**, *2351*, 012043. [CrossRef]
158. Tian, S.; Li, K.; Wei, S.; Fu, Y.; Li, Z.; Liu, S. Security Situation Awareness Approach for Distribution Network Based on Synchronous Phasor Measurement Unit. *Proc. CSEE* **2021**, *41*, 617–632.
159. Xiao, B.; Xiao, Z.; Jiang, Z.; Zhao, X.; Kan, Z.; Qi, X.; Bai, Y. Spatial Load Situation Awareness Based on Denoising Autoencoder, Singular Spectrum Analysis and Long Short-Term Memory Neural Networks. *Proc. CSEE* **2021**, *41*, 4858–4867.
160. Shi, Z.; Wang, Z.; Wu, W.; Wang, X.; Hu, Z. Evaluation Renewable Energy Intergration Capability and Network Expansion Planning Based on Situation Awareness Theory. *Power Syst. Technol.* **2017**, *41*, 2180–2186.

161. Yang, J.; Guo, Y.; Guo, C.; Chen, Z.; Wang, S.; Jiang, B. A Robust Active Distribution Network Defensive Strategy against Cyber-attack Considering Multi-uncertainties. *IET Gener. Transm. Distrib.* **2022**, *16*, 1476–1488. [CrossRef]
162. 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]
163. Song, J.; Wang, Y.; Hu, R.; Xu, G.; Ma, S. Identification of Critical Nodes for the Integrated Energy Systems Based on Complex Networks and Unified Energy Flows. *J. Phys. Conf. Ser.* **2022**, *2301*, 012013. [CrossRef]
164. Dong, S.; Zhou, B.; Zang, T.; Xiao, X. Vulnerability Assessment of Electrical and Thermal Cyber Physical System Considering Dual Coupling Characteristics. *IET Gener. Transm. Distrib.* **2022**, *16*, 4215–4229. [CrossRef]