Risk Assessment and Defense Resource Allocation of Cyber-physical Distribution Systems Under Denial-of-service Attacks

Han Qin, Jiaming Weng, *Member*, *IEEE*, Dong Liu, *Senior Member*, *IEEE*, Donglian Qi, *Member*, *IEEE*, and Yufei Wang, *Member*, *CSEE*

***Abstract*—With the help of advanced information technology, real-time monitoring and control levels of cyber-physical distribution systems (CPDS) have been significantly improved. However due to the deep integration of cyber and physical systems, attackers could still threaten the stable operation of CPDS by launching cyber-attacks, such as denial-of-service (DoS) attacks. Thus, it is necessary to study the CPDS risk assessment and defense resource allocation methods under DoS attacks. This paper analyzes the impact of DoS attacks on the physical system based on the CPDS fault self-healing control. Then, considering attacker and defender strategies and attack damage, a CPDS risk assessment framework is established. Furthermore, risk assessment and defense resource allocation methods, based on the Stackelberg dynamic game model, are proposed under conditions in which the cyber and physical systems are launched simultaneously. Finally, a simulation based on an actual CPDS is performed, and the calculation results verify the effectiveness of the algorithm.**

***Index Terms*—Cyber physical distribution system, defense resource allocation, denial-of-service attack, risk assessment, Stackelberg dynamic game model.**

I. Introduction

With the increasing development and application of distributed energy, the organizational structure and operation mode of power systems are gradually changing [1]. With the help of advanced computation, communication, and control technologies, the distribution network has significantly improved in power flow calculation, voltage and load control, and fault processing. However, with the increasing dependence on cyber systems, an abnormal state in the cyber system can cause control failures and deterioration of the system state [2]. With the impending integration of the physical system and the cyber system, the traditional distribution network is being transformed into a cyber-physical distribution system (CPDS) [3]–[5].

For a CPDS, the system not only faces accidents caused by natural disasters (ice, fires, typhoons, etc.), component failures (aging, malfunctioning, etc.), and physical attacks, but also threats from cyber-attacks. Cyber-attacks can damage or weaken the functions of the cyber system in order to affect the stable operation of the distribution network. Cyber-attacks have the characteristics of low cost, high concealment, and large scope. Once an attack is successful, the consequences could be quite serious [6]. Therefore, it is of practical significance to study CPDS risk assessment methods under the influence of cyber systems.

Research on the impact of cyber systems on the risk to the power system primarily focuses on interactive impact analysis and evaluation methods. The effects of cyber-attacks on physical systems can be categorized as direct interdependency and indirect interdependency, respectively describing the direct failure and hidden failure of the power system caused by cyber-attacks [7], [8]. The direct interdependency of cyber-attacks on a physical system means that a cyber-attack would directly result in the failure of part or all of the physical components. There are three main research scenarios concerning direct interdependency: the first is an attack on Supervisory Control and Data Acquisition. For example, the control authority is invaded or the application algorithm is tampered with, which may cause malfunctions in the dispatch system or bulk system outages. The second research scenario is tampering with the control parameters of terminals, measurement, and control equipment, such as tampering with distributed generation (DG) active and reactive power settings or the feeder terminal unit (FTU) over-current protection settings [9]. The third scenario is cyber systems data tampering; that is, tampering with communication data through cyber-attacks [10]. Indirect interdependency refers to the fact that cyber-attacks can lead to the degradation of physical performance. This interdependency can be divided into two situations. One is that the monitoring failure of the cyber system has a potential impact on the physical system during its normal operation [11]. For example, when the monitoring system fails, the distribution automation center (DAC) cannot perceive the status of lines, and thus cannot deal with

Manuscript received August 30, 2020; revised February 11, 2021; accepted March 10, 2021. Date of online publication December 30, 2021; date of current version August 8, 2023. The work was supported in part by the National Key Research and Development Program of China (2017YFB0903000), and in part by the National Natural Science Foundation of China (No. 51677116).

H. Qin, J. M. Weng (corresponding author, email: wrzx_5@sjtu.edu.cn; ORCID: https://orcid.org/0000-0002-0129-072X), and D. Liu are with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China.

D. L. Qi is with the School of Electrical Engineering, Zhejiang University, Hangzhou 310027, China.

Y. F. Wang is with China Electric Power Research Institute, Beijing 102209, China.

DOI: 10.17775/CSEEJPES.2020.04550

accidents, such as power flow violation. The other situation is that the cyber-attacks affect the fault processing and worsen the operational status when the physical system is in a fault state. For example, when physical faults occur, the failure of the circuit breaker control equipment would cause the occurrence of cascade faults. Indirect interdependency cannot be directly reflected in the physical system and is affected by other complex factors. Consequently, it is rather difficult to quantify the indirect interdependency in the risk assessment. At present, there are many studies on direct interdependency, and the research on indirect interdependency primarily focuses on transmission networks. However, there are few studies on the indirect interdependency of fault processing and recovery function abnormalities resulting from cyber-attacks in CPDS.

In terms of CPDS risk assessment methods, most of the current research is based on graph theory, probability statistical theory, and other theories, and analyzes the probability and the system losses of accidents in specific scenarios. Literature [12] calculated the cyber power physical system (CPPS) risk by considering the attack probability, failure probability, and attack consequences. Literature [13] expresses the CPPS risk through the product of emergency measures failure rate and load loss and proposed a probability model to calculate the failure of cyber components. Literature [14] is based on attack graph theory, considering communication network topology, cyber element status, and an attacker intrusion algorithm to construct a potential attack path probability model of cyber-attacks and quantify the damage of nodes to calculate the risk of CPPS. However, none of the above research studies considered attacker or defender behavior. In response to the above shortcomings, [15] and [16] established attack-defense game models based on game theory to simulate the decision-making process and evaluate system losses according to the game results. However, the above-mentioned research based on game theory still has certain limitations; these studies only analyze the attack-defense game process from the macro level and do not consider the impact of specific control algorithms on the attack-defense game process.

Cyber-attacks have caused several actual power system accidents, including the well-known "Stuxnet" virus in Iran and the "Blackout" in the Ukraine. These attacks can be divided into integrity attacks [10], [17] and denial-of-service (DoS) attacks [11], [18]. Integrity attacks are also called false data injection attacks, which try to mislead the system state estimation and further cause system abnormal states by injecting false data into the measurement system. A DoS attack refers to an attack method that exhausts the computing and communication resources of the attacked object, causing the attacked object to fail to respond to commands. To some degree, compared to integrity attacks in which cyber-attacks inject false data into the measurement system (which is quite difficult from the side of the attack), DoS attacks are more likely to occur in CPDS. More importantly, DoS attacks are usually not easily detected. Inspired by the above discussions, this paper attempts to assess the risk of CPDS by considering the DoS attack that occurred in the cyber systems.

In order to overcome the deficiencies of the current research and realize the quantitative assessment of CPDS risk under DoS attacks, this paper proposes an assessment method based on a dynamic attack and defense game. The principal aims of this paper can be summarized as follows: 1) In CPDS with embedded Centralized Feeder Automation (CFA), taking the data collection and instruction execution in the fault processing process as clues, the impact of the Dos attack on the physical system status is analyzed; 2) Considering the attacker or defender's strategy model and the attack damage, a CPDS risk assessment framework is proposed under the condition that cyber and physical systems are simultaneously attacked; 3) Establish a dynamic attack-defense game model to evaluate CPDS risks, and on this basis, optimize the allocation of defense resources; and 4Validate the proposed risk assessment and defense resource allocation based on an actual CPDS.

The remainder of this paper is organized into the following sections. Section II analyzes the impact of DoS attacks on the CPDS fault processing process. Section III establishes a CPDS risk assessment framework based on the relationship between attack or defense strategies and component failure probability. Section IV evaluates system risks through dynamic attack-defense games and proposes a defense resource allocation method. In Section V, an actual CPDS is used as a test system to validate the proposed method. Conclusions are presented in Section VI.

II. The Impact of DoS Attacks on CPDS

A. The Typical Topology of CPDS

A typical CPDS consists of the physical system and the cyber system. To be more specific, the physical system includes traditional primary equipment, photovoltaic systems, wind power, and other renewable energy and energy storage systems. The cyber system includes communication equipment, communication protocol, software, and topological structure, and other components. The typical structure of a CPDS is shown in Fig. 1.

The DAC can achieve many functions, such as human-computer interaction and decision-making. The communication network is the hub of information interaction between the Intelligent Electronic Device (IED) and the DAC, which can adopt various types of communication methods, such as Ethernet, power line carrier, and wireless. IED includes feeder protection equipment, FTU, inverters, and other power distribution terminal equipment. Since most IEDs have an Uninterruptible Power System (UPS), conventional physical faults have little impact on the cyber system.

The interaction between cyber and physical systems is primarily reflected in the impact of IED abnormal operations on the CPDS fault processing. Local feeder automation is mostly used in a traditional distribution network. CFA is widely used in CPDS containing a large number of DGs, and its dependence on real-time monitoring and control is relatively high, which is the research focus of this paper. In CPDS under CFA, the interaction between cyber and physical systems is primarily reflected in the impact of abnormal status of cyber equipment on the fault processing process. In the cyber system of CPDS, the target of the DoS attack can be any component in the data transmission process, such as the DAC,

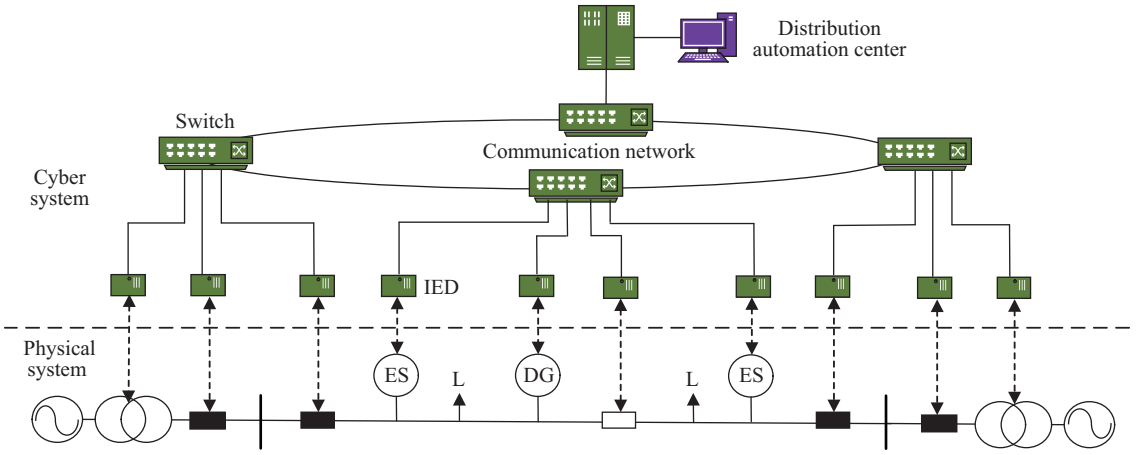

Fig. 1. Typical structure of CPDS.

switch, IED, etc. The attack effect is to make cyber equipment unavailable. With the construction of the distribution network, a large number of IEDs are applied to CPDS. Compared with the DAC and communication equipment with a higher level of cybersecurity, IEDs are more vulnerable to DoS attacks due to their complex application environment, diverse functional types, and unsound credibility mechanisms [19]. The monitoring and control function failures in the fault processing process resulting from the IED is an indirect interdependency, which increases the scope and outage of fault. This paper will focus on the above-mentioned indirect interdependency.

B. The Impact of DoS Attacks on CPDS Fault Processing

CPDS fault processing requires the coordination of cyber systems and physical systems. Therefore, the CPDS risk is affected by the operation status of the physical system and the cyber equipment. IED failures resulting from DoS attacks primarily affect fault processing and DG operating status. Due to the operating characteristics of the distribution network, the fault processing would not be triggered when the physical system is in normal operation. When the distribution network is in normal operation, the power change of distributed energy has no significant impact on distribution network users. Therefore, this paper analyzes the process of CPDS failure under DoS attack from three aspects: fault location, isolation, and recovery.

1) Fault Location

After a line fault occurs, the DAC judges the fault area based on the abnormal status data uploaded by IEDs. As shown in Fig. 2, if the IECB is unavailable resulting from a DoS attack, the uplink monitoring signal transmission of circuit break B, which is the upstream circuit break of the faulty line, would fail. If the monitoring signal of circuit break A is successfully transmitted, the DAC determines that the fault area is AC, where AB is the non-fault outage area.

2) Fault Isolation

If the IECC is attacked and becomes unavailable, the control command issued by DAC to circuit break C cannot execute, resulting in fault isolation failure. Since the DAC cannot receive the feedback signal that circuit break C successfully executed the command, it would issue a disconnect command to circuit break D to isolate the faulty area. The fault area isolated by the DAC is BD, and CD is the non-fault outage area.

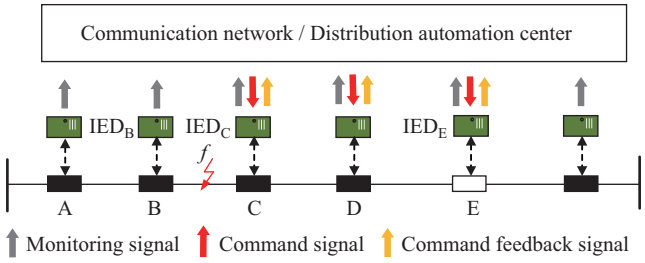

Fig. 2. Fault state analysis of CPDS.

3) Fault Recovery

The distribution network fault recovery includes load transfer and planned islands. If the IECE is attacked and becomes unavailable, the control command issued by DAC to circuit break E cannot execute, resulting in a non-fault area CE power outage. For planned islands, only when circuit breakers, DGs, and IEDs are available in the island area can it be considered a valid island; otherwise, it will cause a power outage in the island area.

III. CPDS Risk Assessment Framework

According to the terrorist attack risk model proposed by RAND Corporation in 2004, accident risk is expressed as the product of "threat", "vulnerability" and "consequence" [20]. This paper draws on the above model and proposes a risk assessment framework for CPDS under deliberate assaults:

$$R = P^{\mathrm{A}} P^{\mathrm{D}} H \tag{1}$$

where P^{A} is the probability of an attacker launching an attack; P^{D} is the target failure probability if it is attacked; H is the loss caused by the failure; and R is the expected value of the final loss, that is, the risk.

The evaluation framework in formula (1) takes into account the impact of the attacker and defender's strategies on CPDS risk and uses the actual loss in the physical system as the

criterion to quantify the attack damage. These all bring the risk assessment result closer to reality. This section analyzes P^{A}, P^{D}, and H respectively under a specific attacker or defender strategy to quantify the CPDS risk in specific attack scenarios.

This paper regards DoS attacks against cyber systems and line destruction against physical systems as deliberate assaults by attackers. Therefore, each assault can be equivalent to an attacker launching attacks on the cyber system and the physical system at the same time. Cyber-attacks are characterized by a large range. For example, an attacker can easily launch attacks on multiple devices in the cyber system through DoS attacks. Without loss of generality, this paper assumes that the attacker would select multiple IEDs in the cyber system to launch a cyber-attack while physically attacking a line.

In practice, attackers and defenders usually have limited resources (including manpower, technology, equipment, and capital required for an attack or defense action). The difference in the amount of attack or defense resources invested by the two parties on each component would affect the failure probability of each component, and then affect the risk of CPDS. In [21], a set of functions with diminishing marginal effects are used to describe the relationship between the above-mentioned resource input and the probability of successful attack and component vulnerability. In this paper, the attack targets are cyber components (IEDs) and physical components (lines). In the actual distribution network, due to the differences in factors, such as the characteristics and costs of the components, there are obvious differences in the number of attack resources and attack efficiency invested by different components. The above component characteristics would not only affect the attacker's attack resource allocation but also affect the defender's resource allocation tendency. Therefore, on the basis of [21], this paper introduces the concept of a resource conversion coefficient to describe the resource conversion efficiency of different components.

For an attacker, the more attack resources invested in a certain component, the greater the probability that the component would be successfully attacked. The relationship between the two can be modeled as follows:

$$p_i^{\mathrm{A}} = \frac{h_i^{\mathrm{A}} s_i^{\mathrm{A}}}{f_i^{\mathrm{A}} + h_i^{\mathrm{A}} s_i^{\mathrm{A}}} \tag{2}$$

where P_i^{A} is the probability of component i being attacked, $0 \le P_i^{\mathrm{A}} < 1$; s_i^{A} is the number of attack resources invested by the attacker on the component i; h_i^{A} is the attack resource conversion coefficient of component i, and the larger the value, the higher the conversion efficiency of attack resources; and f_i^{A} is the attack cost coefficient of the component i.

Similar to the attacker strategy, the more resources the defender invests in the component, the lower the failure probability of the component after being attacked. The relationship between the two can be modeled as follows:

$$p_i^{\mathrm{D}} = \frac{1}{f_i^{\mathrm{D}} + s_i^{\mathrm{D}} h_i^{\mathrm{D}}} \tag{3}$$

where P_i^{D} is the probability that the component i fails after being attacked, $0 \le P_i^{\mathrm{D}} < 1$; s_i^{D} is the number of attack resources invested by the defender on the component i; h_i^{D} is the defense resource conversion coefficient of the component i, and the larger the value, the higher the defense resource conversion efficiency; and f_i^{D} is the defense cost coefficient of component i.

In CPDS, the impact of an attack is multifaceted, including load loss, power outage range, power outage duration, economic loss, etc. Therefore, an evaluation method is needed to quantify the attack damage. In this paper, the expected energy not supplied after CPDS is attacked is the hazard evaluation index:

$$H_z = U_z T_z \tag{4}$$

where H_z is the expected energy not supplied caused by the attacked component combination z; U_z is the load reduction caused by z; and T_z is the load outage time caused by z.

Because the components in the system are independent of each other, the attack of a certain component would not affect the operating state of other components, so it can be considered that the attacks against each component are independent of each other. The probability of an attacker targeting multiple components can be expressed as the cumulative multiplication of the probability of each component being attacked, and the probability P_z^{A} of an attacker launching an attack on multiple components can be expressed as:

$$P_z^{\mathrm{A}} = \prod_{i \in f_z} p_i^{\mathrm{A}} \tag{5}$$

where f_z is the set of target attack components contained in z. According to formula (5), the more target components the attacker attacks, the lower the success rate of the attack; conversely, the attacker needs to attack multiple components in order to increase the loss. A rational attacker needs to weigh the attack success rate and system loss when deciding an attack strategy to cause the greatest risk to CPDS.

Similarly, after the defender is attacked against z, the probability P_z^{D} that the multiple components would fail is:

$$P_z^{\mathrm{D}} = \prod_{i \in f_z} p_i^{\mathrm{D}} \tag{6}$$

According to (2)–(6), the CPDS risk under a specific attack or defense resource strategy can be expressed as:

$$\begin{aligned} R &= P_z^{\mathrm{A}} P_z^{\mathrm{D}} H_z \\ &= \prod_{i \in f_z} p_i^{\mathrm{A}} \prod_{i \in f_z} p_i^{\mathrm{D}} U_z T_z \end{aligned} \tag{7}$$

IV. CPDS Dynamic Attack and Defense Game Algorithm Based on Stackelberg

A. CPDS Risk Assessment Method Based on the Stackelberg Attack and Defense Dynamic Game Model

The CPDS life cycle can be divided into three phases: planning, construction, and operation. For defenders, it takes a long period from the investment of defense resources to the improvement of defense capabilities, and the investment behavior usually occurs in the planning and construction phases. In contrast, the attacker's attack is faster and more flexible, and it can adjust its attack strategy more conveniently. The

period from the attacker's resource investment to the attack implementation is also relatively short, and the investment behavior usually occurs in the operational phase. Inspired by the above discussions, the actual attack and defense have obvious timing characteristics. However, in previous studies, this timing characteristic is often ignored, and it is believed that the attacker and defender have the same resource conversion period and stage, and this attack-defense game model is set as a complete information static game model (Cournot duopoly model) [16], [17]. Compared with the dynamic attack-defense game model considering the timing characteristics, the static game overestimates the ability of defense resource deployment and underestimates the amount of information the attacker has, resulting in the underestimation of the risk level of the system. In addition, with the privatization of the energy industry and the standardization of power system construction models, attackers can more easily collect enough information and conduct targeted deliberate assaults. In summary, it can be considered that the attacker and defender in CPDS is a two-stage dynamic game model in a state of complete information.

This paper uses a Stackelberg game model [22] to establish an attack-defense game model to determine the risk status of CPDS under a limited attack and defense resource. For CPDS, system risk is a function of attack and defense resources. The optimization problem can be solved by the following specific steps.

Step 1: In the face of a deliberate assault by an attacker, the defender formulates a resource allocation strategy. Defenders allocate defense resources to physical lines and IEDs, thereby affecting the failure probability of lines or IEDs after being attacked, as shown in (3).

Step 2: According to the resource allocation strategy of the defender, the attacker selects one line for physical attacks and several IEDs for cyber-attacks. The attacker allocates resources to the target attack components to increase the attack probability, as shown in (4).

Equation (8) is the mathematical model of the defender. The defender formulates the optimal defense resource allocation strategy to minimize the risk caused by the attack.

$$c^{\mathrm{D}*} = \arg\min_{C^{\mathrm{D}}} R\left(S^{\mathrm{D}}, S^{\mathrm{A}}, C^{\mathrm{D}}, C^{\mathrm{A}}, e^{\mathrm{A}}, e^{\mathrm{D}}, a\right) \tag{8}$$

$$q^{\mathrm{A}}\left(S^{\mathrm{A}}, C^{\mathrm{A}}, a\right) \geq 0 \tag{9}$$

$$q^{\mathrm{D}}\left(S^{\mathrm{D}}, C^{\mathrm{D}}\right) \geq 0 \tag{10}$$

where $c^{\mathrm{D}*}$ is the optimal strategy for the defender; S^{A} and S^{D} are the total resources of the attacker and the defender respectively; C^{A} and C^{D} are the resource allocation strategy set of the attacker and the defender respectively; e^{A} and e^{D} are the constraints of the attacker and the defender respectively; and a is the lower limit of the attacker's expected risk.

Equation (11) is the mathematical model of the attacker. On the basis of the defensive resource allocation strategy that has been formulated, the attacker would formulate the most effective attack strategy to cause the greatest risk to the attack.

$$c^{\mathrm{A}*} = \arg\max_{C^{\mathrm{A}}} R\left(S^{\mathrm{A}}, C^{\mathrm{A}}, c^{\mathrm{D}*}, e^{\mathrm{A}}\right) \tag{11}$$

where $c^{\mathrm{A}*}$ is the attacker's optimal strategy.

Calculating formulas (8)–(11) can get the system risk R^* in equilibrium.

$$R^* = R\left(S^{\mathrm{D}}, S^{\mathrm{A}}, c^{\mathrm{D}*}, c^{\mathrm{A}*}\right) \tag{12}$$

Formulas (8)–(12) show that in the case of complete information static, the number of attack strategies that an attacker can take is limited. For the defender, there is an optimal defense strategy, so that no matter what strategy the attacker adopts, the system risk would not exceed a certain limit. For the attacker, under the premise of understanding the defense strategy, there is an optimal attack strategy that makes the attack result in the greatest risk. Therefore, under the premise that both parties in the dynamic game are rational people, the system has a certain attack-defense equilibrium state, and the risk in this state can be regarded as systemic risk.

B. CPDS Optimal Defense Resource Allocation Method under Limited Resources

In the actual distribution network, the defense resources that can be used for attack protection are usually limited. It is necessary to analyze the key IEDs and lines to allocate defense resources more effectively. Therefore, it is of practical significance to study the optimal allocation method under limited defense resources.

In the first step of the dynamic attack-defense game, the defender allocates defense resources to the threatened components in CPDS without knowing the specific attack strategy. Consider that the ultimate goal of the defender is to minimize risk. Therefore, this paper analyzes the risks caused by the attack strategy on the premise that the contingency analysis (CA) results are known, to determine the optimal defense resource allocation strategy. That is, based on the CA analysis under the $N-K$ condition, the attack strategy that the defender needs to consider in the defense resource allocation process is determined. The defense resource allocation strategy can be solved by the following specific steps.

Step 1: In the initial state, set the defense resources of all components in the CPDS to 0, and divide the total defense resources S^{D} into M sub-defense resources.

Step 2: Calculate the system risk r_x caused by each attacker's strategy c_x^{A} under the current state of defense resources, where $c_x^{\mathrm{A}} \in C_{\mathrm{A}}$ and r_x can be calculated by formulas (2)–(7).

Step 3: From the attack strategy sets, filter the attack strategy set C_f^{A} whose r_x is greater than the lower limit of the attacker's expected risk a. According to the ratio of r_x to the total risk of all attack strategies in C_f^{A}, a sub-defense resource is allocated to different attack strategies, as shown in the following formula:

$$S_x^{\mathrm{D}} = \frac{r_x}{\sum_{k=1}^{n_{\mathrm{A}}} r_k} \frac{S^{\mathrm{D}}}{M} \tag{13}$$

where S_x^{D} is the number of defense resources allocated to attack strategy c_x^{A}; and n_{A} is the total number of attack strategies in C_f^{A}.

Step 4: According to the risk weight coefficient of the components included in the attack strategy, the defense resources are allocated to different components. The risk weight

coefficient is the ratio of the component failure probability to the sum of component failure probability in the strategy.

$$s_i^{\mathrm{D}} = s_i^{\mathrm{D}} + \sum_{x=1}^{b} \left(S_x^{\mathrm{D}} A_{x,i} \right) \tag{14}$$

$$A_{x,i} = \frac{p_i^{\mathrm{A}} p_i^{\mathrm{D}}}{\sum_{c=1}^{d} p_c^{\mathrm{A}} p_c^{\mathrm{D}}} \tag{15}$$

where s_i^{D} is the defense resources allocated to component i; b is the set of attack strategy that contains component i in C_f^{A}; $A_{x,i}$ is the risk weight coefficient of component i in attack strategy c_x^{A}; and d is the number of components in attack strategy c_x^{A}.

Step 5: If the defense resources have not been allocated, return to step 2; if the defense resources have been allocated, output the allocation result.

According to the above defense resource allocation process, the allocated resource s_i^{D} of component i can be further expressed as:

$$s_i^{\mathrm{D}} = \sum_{u=1}^{M} \left[\sum_{x=1}^{b} \left(\frac{r_x}{\sum_{k=1}^{n_{\mathrm{A}}} r_k} \frac{p_i^{\mathrm{A}} p_i^{\mathrm{D}}}{\sum_{c=1}^{d} p_c^{\mathrm{A}} p_c^{\mathrm{D}}} \frac{S^{\mathrm{D}}}{M} \right) \right]_{\mathrm{u}} \tag{16}$$

The defense resource allocation method described not only considers the attack strategy that causes the greater risk but also considers the difficulty of the components in the attack strategy to be attacked so that the defense resource allocation is reasonable. In summary, the process of risk assessment and defense resource allocation in CPDS is shown in Fig. 3.

V. Case Study

A. Simulation Example Setup

In this paper, MATLAB and OPNET co-simulation is used to analyze the CPDS risk under the established attacker/defender resources. MATLAB is used to simulate physical attacks and control algorithms, and OPNET is used to simulate network attacks. The simulation example is derived from an actual CPDS, and the cyber and physical topology are shown in Figs. 4 and 5, respectively. The example includes three PV units and three energy storage units, whose parameters are shown in Table I. The example includes three feeders with a total of 62 load points, and the total power load is 5.48 MW, as shown in Appendix A, Table I. The example contains two types of IEDs, namely the FTU and the PV/energy storage controller FPV/FBAT. The control and monitoring functions of a circuit break are all enabled by FTU. FBAT and FPV can adjust the power of energy storage systems and the PV. All IEDs can communicate with the DAC via a communication network.

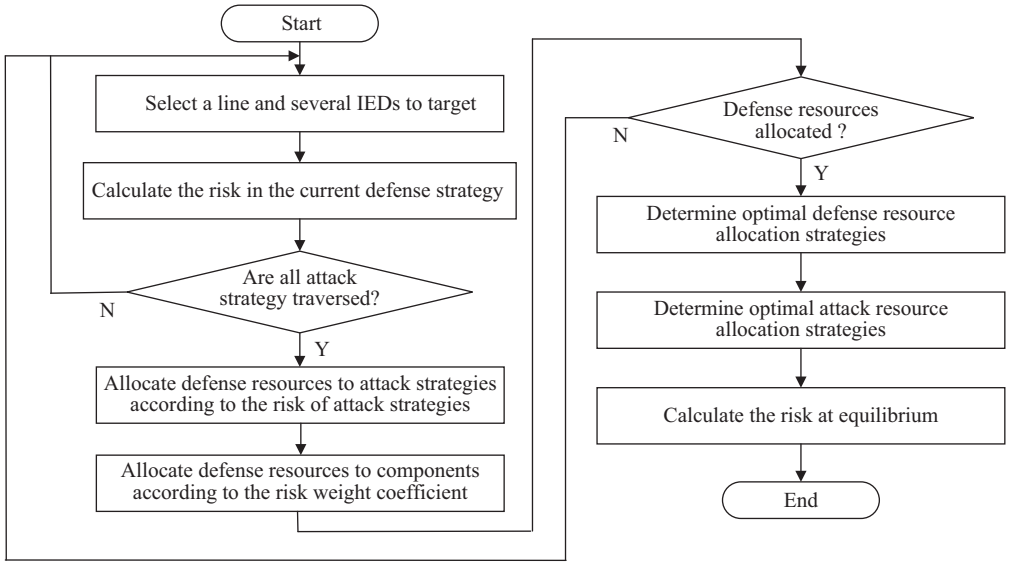

Fig. 3. Flow chart for risk assessment and defense resources allocation.

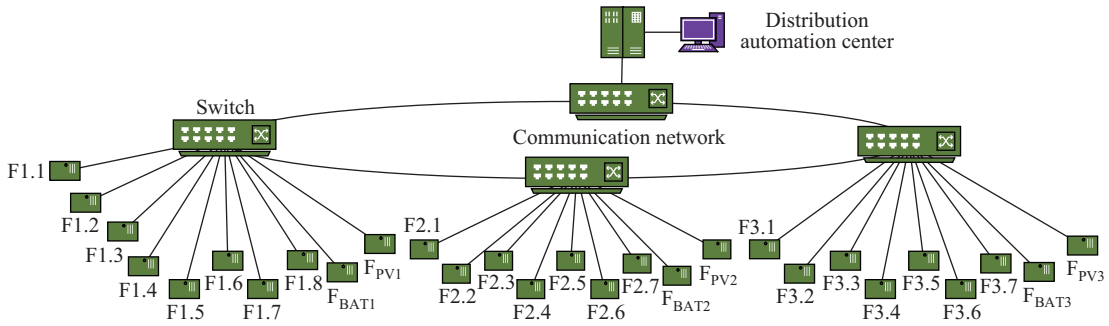

Fig. 4. Cyber topological structure of CPDS.

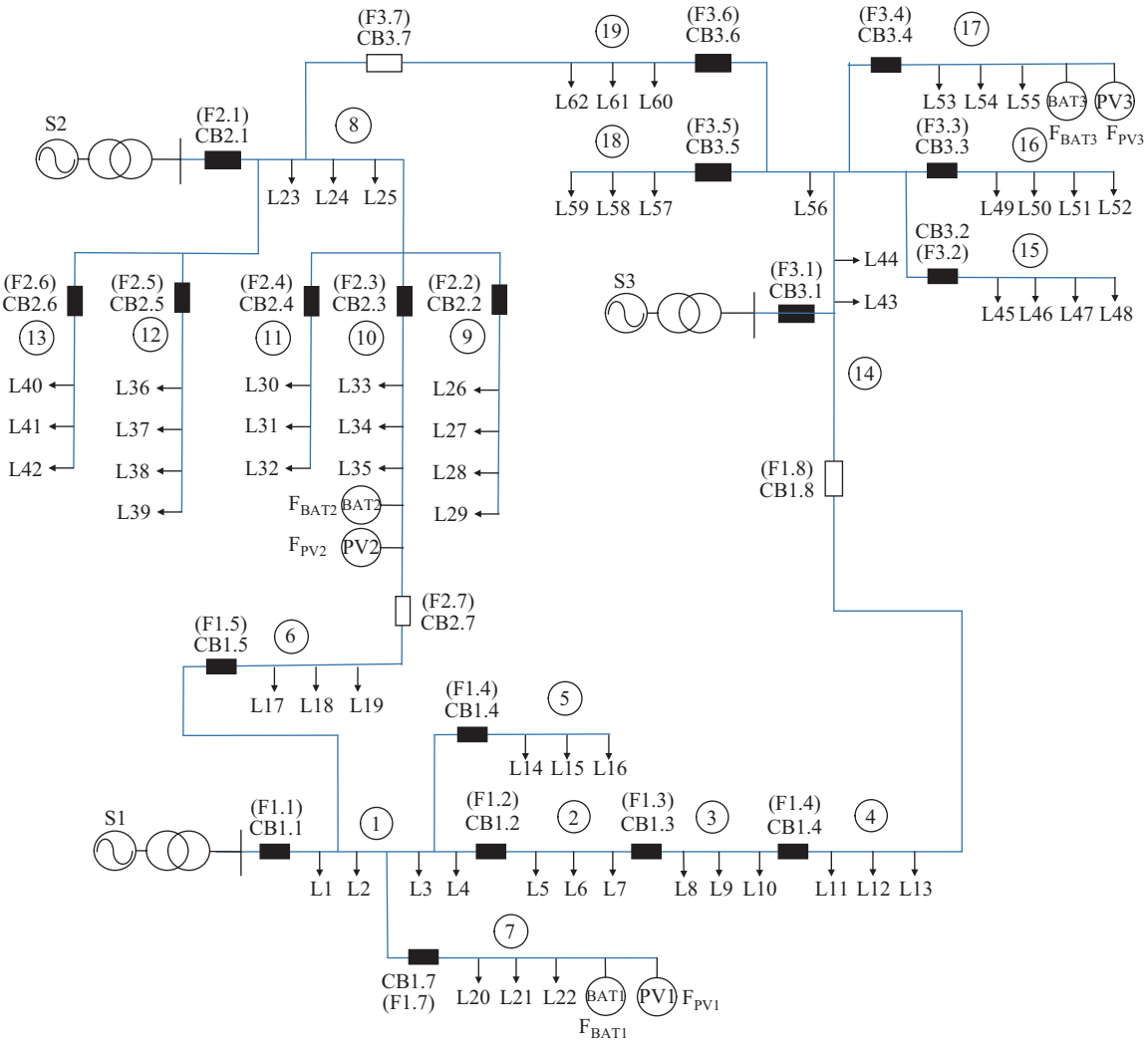

Fig. 5. Physical topological structure of CPDS.

TABLE I
CONFIGURATION DATA OF PHOTOVOLTAIC POWER AND ENERGY STORAGE

Energy storage	Maximum power (MW)	Capacity (MWh)	Photovoltaic	Rated capacity (MW)
BAT1	0.3	1.5	PV1	0.4
BAT2	0.4	2	PV2	0.5
BAT3	0.4	2	PV3	0.5
Total	1.1	5.5	Total	1.4

The non-faulty area caused by the attack in the system can be recovered by manual operationand the power outage time of the non-faulty area is 1 hour; the faulty area caused by the attack needs to be repaired, and the power outage time of the faulty area is 5 hours.

B. CPDS Optimal Defense Resource Allocation and Risk Assessment Under Limited Resources

The total resource of the attacker is $S^{\mathrm{A}} = 5$; the total resource of the defender is $S^{\mathrm{D}} = 30$; the precision of the defense resource allocation is $M = 50$; and the attack cost coefficient f^{A} and the defender cost coefficient f^{D} are both 1. The attacker resource conversion coefficient h^{A} and the defender resource conversion coefficient h^{D} are both 1. The lower limit of the attacker's expected risk is $a = 0.05$ MWh. According to the defense resource allocation method proposed, the defense resources are allocated to all threatened components. The final allocation result is shown in Table II.

As can be seen from Table II: 1) Feeder outlet lines (Line1, Line8, Line14) and FTU of outlet circuit breakers (F1.1, F2.1, F3.1) are allocated more defense resources. The reason is that the attacker simultaneously attacks the feeder outlet line (such as Line1) and the FTU of the outlet circuit breaker (such as F1.1), which can cause the entire feeder to be out of power, so the defender would allocate more resources to the above components; 2) F1.8, F2.7, and F3.7 allocate more defense resources. The reason is that the above-mentioned FTU can control the tie switch. Once the above-mentioned FTU fails, the load transfer process between feeders would be affected; and 3) compared with the FTU, F_{BAT}/F_{PV} are allocated fewer defense resources. The reason is that the start or stop of DGs would not cause power outages when the distribution network is operating in a normal state. If and only if the line to which the DG belongs is in the planned island state, F_{BAT}/F_{PV} being attacked would cause a power outage in the island area, which

TABLE II
RESULT OF DEFENSE RESOURCE ALLOCATION

IED number	Defense resources	Line number	Defense resources
F1.1	2.309	Line1	2.162
F1.2	0.752	Line2	0.514
F1.3	0.593	Line3	0.291
F1.4	0.373	Line4	0.330
F1.5	0.326	Line5	0.396
F1.6	0.462	Line6	0.448
F1.7	0.457	Line7	0.233
F1.8	1.510	Line8	2.071
F2.1	2.166	Line9	0.252
F2.2	0.448	Line10	0.310
F2.3	0.320	Line11	0.272
F2.4	0.426	Line12	0.252
F2.5	0.444	Line13	0.272
F2.6	0.396	Line14	2.094
F2.7	1.414	Line15	0.291
F3.1	2.084	Line16	0.310
F3.2	0.448	Line17	0.291
F3.3	0.414	Line18	0.330
F3.4	0.440	Line19	0.407
F3.5	0.467	–	–
F3.6	0.301	–	–
F3.7	1.382	–	–
F_{BAT1}	0.081	–	–
F_{PV1}	0.081	–	–
F_{BAT2}	0.100	–	–
F_{PV2}	0.100	–	–
F_{BAT3}	0.088	–	–
F_{PV3}	0.088	–	–

would affect users.

According to the above defense resource allocation method, the attacker launches an attack on the components (line and IEDs) and appropriately allocates resources to several attack targets. The resource allocation strategies that the attacker may adopt and the risks caused are shown in Table III. As there are many attacker strategies that the attacker can choose, only partial results are shown here.

TABLE III
RESULTS OF ATTACK RESOURCE ALLOCATION AND RISK ASSESSMENT

Attack Targets	Attack resource allocation	H (MWh)	Risk (MWh)
Line 1, F1.1	2.443, 2.557	2.562	0.072
Line 5, F1.4, F1.1	1.148, 1.130, 2.722	2.920	0.095
Line 7, F1.7, F1.8	1.186, 1.401, 2.414	2.548	0.126
Line 2, F1.8	1.88, 3.119	1.982	0.135
Line 12, F2.5, F2.7	1.225, 1.413, 2.362	2.940	0.153
Line 7, F1.7	2.292, 2.708	1.426	0.227
Line 5, F1.4	2.520, 2.480	1.591	0.248
Line16, F3.3, Fbat3	1.718, 1.85, 1.42	3.505	0.420
Line 16, F3.3	2.405, 2.595	3.105	0.490
Line 10, F2.3	2.491, 2.509	2.860	0.491

As can be seen from Table III: 1) Generally, the more attack components the attacker chooses to attack, the greater the damage caused by the attack. However, the increase in the number of attack components means that the resources allocated to a single attack component would decrease accordingly. Therefore, the risk caused by an attack strategy that includes multiple attack components may not be high; and 2) The attacker can use the control algorithm in CPDS to launch attacks on only a few relevant components, which can result in greater risk. In summary, the attacker traverses all possible attack strategies. Under the premise of known defense resource allocation, the attacker can attack Line 10 and F2.3 simultaneously, which can cause the greatest risk to the CPDS system. That is, when the defender adopts the defense resource allocation strategy in Table II, no matter what attack strategy the attacker adopts, the risk to the system is less than 0.491 MWh.

C. The Impact of Attack Resource Conversion Coefficient on Defense Resource Allocation

In the above simulation, it is assumed that lines and IEDs have the same attack/defense resource conversion coefficient. In actual systems, cyber system components and physical system components usually have different attack/defense resource conversion coefficients due to differences in functional characteristics. This subsection analyzes the impact of the above parameters on the allocation of defense resources.

1) The Impact of Attack Resource Conversion Coefficient Distribution

With the advancement of information technology in recent years, attackers can use more efficient cyber-attack methods to attack cyber systems; that is, the attack resource conversion coefficient of IEDs has increased. This paper analyzes the impact of IED's attack resource conversion coefficient on the allocation of defense resources through simulation.

Set the IED's attack resource conversion coefficient to increase from 0.4 to 1.6 with steps of 0.4. Other parameters are the same as in the previous section. The defense resource allocation and system risk obtained by simulation are shown in Table IV. As can be seen from Table IV, as the attacker's attack resource conversion coefficient of IEDs increases, the defender tends to allocate more resources to IEDs. The main reason is that as the attack resource conversion coefficient of IEDs increases, the possibility of attackers launching attacks against information systems increases. To reduce the harm of attacks, rational defenders will allocate more defense resources to IEDs. Especially in recent years, with the rapid progress of information technology, the security of power information systems has become the focus of many scholars.

2) The Impact of Defense Resource Conversion Coefficient Distribution

The defense resource conversion coefficient of lines is usually affected by factors such as equipment cost, installation location, terrain, and climate. Thus, it is necessary to analyze the impact of the defense resource conversion coefficient of lines on the allocation of defense resources.

Set the line's defense resource conversion coefficient to increase from 0.4 to 1.6 with steps of 0.4. Other parameters are the same as in the previous section. The defense resource allocation and system risk obtained by the simulation are shown in Table V. As can be seen from Table V, as the defender's defense resource conversion coefficient of lines increases, the defender tends to allocate fewer resources to lines. The main reason is that as the defense resource conversion coefficient increases, the defender can effectively reduce the possibility of successful attacks by investing fewer resources on lines. Therefore, a rational defender will allocate fewer resources to lines.

TABLE IV
RESULTS OF DEFENSE RESOURCE ALLOCATION IN DIFFERENT ATTACK RESOURCE ALLOCATION COEFFICIENT OF IEDS

IED Number	Attack resource allocation coefficient of IED			
	0.40	0.80	1.20	1.60
F1.1	1.65	2.09	2.57	3.02
F1.2	0.53	0.67	0.82	0.95
F1.3	0.42	0.53	0.64	0.75
F1.4	0.26	0.33	0.40	0.46
F1.5	0.24	0.30	0.37	0.44
F1.6	0.34	0.42	0.53	0.63
F1.7	0.32	0.41	0.49	0.56
F1.8	1.08	1.37	1.70	2.00
F2.1	1.54	1.96	2.41	2.82
F2.2	0.31	0.40	0.48	0.55
F2.3	0.22	0.28	0.34	0.39
F2.4	0.31	0.39	0.48	0.57
F2.5	0.32	0.40	0.49	0.57
F2.6	0.28	0.36	0.44	0.51
F2.7	1.01	1.28	1.57	1.84
F3.1	1.48	1.88	2.30	2.69
F3.2	0.32	0.41	0.51	0.60
F3.3	0.29	0.37	0.45	0.52
F3.4	0.31	0.39	0.48	0.55
F3.5	0.33	0.42	0.52	0.61
F3.6	0.21	0.27	0.32	0.36
F3.7	0.98	1.25	1.52	1.77
F_{BAT1}	0.04	0.07	0.09	0.10
F_{PV1}	0.04	0.07	0.09	0.10
F_{BAT2}	0.06	0.09	0.11	0.13
F_{PV2}	0.05	0.08	0.11	0.12
F_{BAT3}	0.07	0.08	0.10	0.12
F_{PV3}	0.07	0.08	0.10	0.12
Line1	3.17	2.50	1.78	1.13
Line2	0.75	0.59	0.42	0.26
Line3	0.42	0.33	0.23	0.14
Line4	0.48	0.38	0.26	0.15
Line5	0.58	0.46	0.32	0.20
Line6	0.67	0.53	0.39	0.28
Line7	0.35	0.27	0.20	0.14
Line8	3.04	2.40	1.71	1.10
Line9	0.36	0.29	0.19	0.10
Line10	0.45	0.36	0.25	0.16
Line11	0.40	0.31	0.22	0.13
Line12	0.38	0.30	0.23	0.18
Line13	0.39	0.31	0.21	0.12
Line14	3.08	2.43	1.74	1.13
Line15	0.43	0.34	0.26	0.18
Line16	0.46	0.37	0.28	0.20
Line17	0.43	0.34	0.26	0.18
Line18	0.48	0.38	0.27	0.17
Line19	0.60	0.47	0.33	0.21

TABLE V
RESULTS OF DEFENSE RESOURCE ALLOCATION IN DIFFERENT DEFENSE RESOURCE ALLOCATION COEFFICIENT OF LINES

IED Number	Defense resource allocation coefficient of lines			
	0.40	0.80	1.20	1.60
F1.1	1.61	2.05	2.54	2.91
F1.2	0.52	0.67	0.82	0.95
F1.3	0.43	0.53	0.67	0.75
F1.4	0.27	0.34	0.43	0.47
F1.5	0.23	0.29	0.36	0.41
F1.6	0.32	0.41	0.50	0.58
F1.7	0.31	0.40	0.49	0.57
F1.8	1.07	1.35	1.69	1.91
F2.1	1.52	1.93	2.39	2.73
F2.2	0.32	0.40	0.50	0.56
F2.3	0.23	0.29	0.36	0.40
F2.4	0.31	0.38	0.49	0.54
F2.5	0.30	0.39	0.48	0.56
F2.6	0.28	0.36	0.45	0.50
F2.7	0.99	1.26	1.55	1.78
F3.1	1.47	1.86	2.32	2.63
F3.2	0.32	0.40	0.52	0.57
F3.3	0.29	0.37	0.46	0.52
F3.4	0.31	0.39	0.48	0.55
F3.5	0.32	0.41	0.50	0.59
F3.6	0.21	0.27	0.33	0.38
F3.7	0.98	1.23	1.54	1.75
F_{BAT1}	0.06	0.08	0.09	0.11
F_{PV1}	0.06	0.08	0.09	0.11
F_{BAT2}	0.07	0.09	0.11	0.13
F_{PV2}	0.07	0.08	0.11	0.12
F_{BAT3}	0.06	0.08	0.10	0.11
F_{PV3}	0.06	0.08	0.10	0.11
Line1	3.20	2.54	1.79	1.26
Line2	0.77	0.61	0.43	0.31
Line3	0.43	0.34	0.24	0.17
Line4	0.49	0.39	0.28	0.20
Line5	0.59	0.47	0.33	0.24
Line6	0.65	0.52	0.37	0.25
Line7	0.34	0.27	0.19	0.14
Line8	3.05	2.43	1.71	1.20
Line9	0.37	0.29	0.20	0.14
Line10	0.45	0.36	0.25	0.17
Line11	0.40	0.31	0.22	0.15
Line12	0.38	0.30	0.22	0.16
Line13	0.40	0.32	0.23	0.16
Line14	3.09	2.46	1.73	1.22
Line15	0.42	0.34	0.23	0.16
Line16	0.46	0.36	0.26	0.18
Line17	0.42	0.33	0.23	0.16
Line18	0.49	0.39	0.28	0.20
Line19	0.60	0.48	0.34	0.24

In summary, it can be seen from the above simulation that the attack/defense resource conversion coefficient of components will affect the probability of successful attacks, which will affect the allocation of defense resources. Consequently, the defender should adjust the allocation of defense resources according to the actual system to minimize system risks.

D. The Impact of Attack/Defense Resource Conversion Coefficient on System Risk

In the simulation of subsection B, it is assumed that the attack resource conversion coefficient and defense resource conversion coefficient both are 1. In actual systems, the attack resources conversion coefficient and the defense resource conversion coefficient are generally not equal. This subsection analyzes the impact of the above parameter changes on the CPDS risk. The initial simulation parameters are the same as the previous subsection, and the system risk under different resource conversion coefficient combinations $(h^{\mathrm{A}}, h^{\mathrm{D}})$ are shown in Fig. 6.

As can be seen from Fig. 6: 1) The system risk increases as the attack resource conversion coefficient increases, but the rate of risk increase gradually slows down; 2) The system risk decreases as the defense resource conversion coefficient increases, but the rate of risk decrease gradually slows down; and 3) When the defense resource conversion system is relatively large, even if the attack resource conversion coefficient increases rapidly, the system can maintain a low-risk level. Consequently, defenders can significantly enhance the ability of CPDS to resist risks by increasing the defense resource conversion coefficient.

VI. CONCLUSION

This paper has proposed risk assessment and defense re-

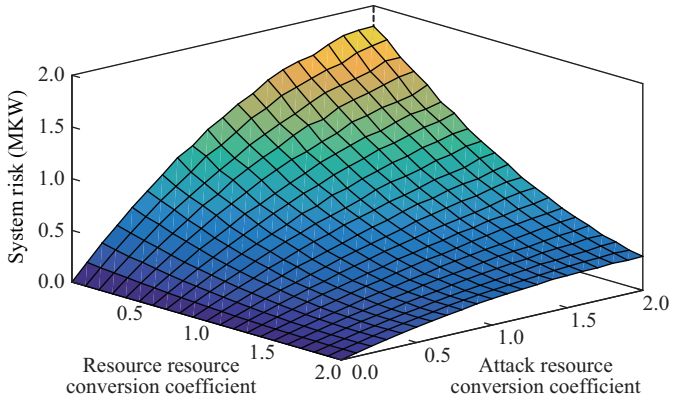

Fig. 6. Three-dimensional diagram of the impact of attack/defense resource conversion coefficient on system risk.

source allocation methods for CPDS under the threat of DoS attack and physical attack. Specifically, this paper analyzed the CPDS fault processing process under DoS attacks, established a risk assessment method based on a dynamic attack-defense game model, and proposed a resource optimization allocation method under limited defense resources. Then, the CPDS risk under the established attacker and defender resources was analyzed by using MATLAB and OPNET co-simulation, and the effectiveness of the proposed method was verified. Summarizing the research of this paper, the following conclusions are obtained:

1) There are some key cyber and physical components in CPDS. Just as attackers can attack these key components to increase the probability of the attack success; correspondingly, rational defenders would also focus on the key components to enhance their attack protection capabilities. The above-mentioned key components are usually determined by the topology and control method of CPDS.

2) Some key parameters, including IED's attack cost conversion coefficient and line defense resource conversion coefficient, have a greater impact on the tendency of defense resource allocation and the CPDS risk. Therefore, in the simulation process of CPDS risk assessment and defense resource allocation, appropriate parameters need to be selected according to the actual distribution network.

Finally, although the research is aimed at CPDS, a physical attack only considers the line attack, and cyber-attacks only considers the DoS attack. The follow-up study can further conduct modeling research on cyber and physical systems.

APPENDIX

TABLE AI
LOAD DATA OF PHYSICAL SYSTEM (KW)

Number	Load	Number	Load	Number	Load
1	40.5	22	87	43	60
2	50	23	60	44	60
3	40	24	60	45	120
4	60	25	60	46	100
5	100	26	70	47	100
6	100	27	60	48	100
7	85	28	100	49	130
8	100	29	60	50	80
9	100	30	100	51	100
10	94	31	120	52	100
11	100	32	120	53	135
12	100	33	110	54	135
13	63	34	90	55	130
14	95	35	60	56	40
15	95	36	140	57	120
16	90	37	120	58	90
17	75	38	120	59	55
18	80	39	90	60	60
19	85	40	100	61	90
20	80	41	90	62	60
21	80	42	90	–	–

REFERENCES

[1] Y. J. Cao, Q. Li, Y. Tan, Y. Li, Y. Y. Chen, X. Shao, and Y. Zou, "A comprehensive review of Energy Internet: basic concept, operation and planning methods, and research prospects," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 3, pp. 399–411, May 2018.

[2] H. B. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, Dec. 2016.

[3] D. Liu, W. X. Sheng, Y. Wang, Y. M. Lu, and C. Sun, "Key technologies and trends of cyber physical system for power grid," *Proceedings of the CSEE*, vol. 35, no. 14, pp. 3522–3531, Jul. 2015.

[4] K. H. Wu, J. W. Li, Y.Y. Zhu, S. W. Miao, S. X. Zhu and C. J. Zhou, "Interactive visual analysis on the attack and defense drill of grid cyber-physical systems," *CSEE Journal of Power and Energy Systems*, vol. 7, no. 1, pp. 45–56, Jan. 2021.

[5] M. Ni, D. Liu, and C. Singh, "Guest editorial: Special section on cyber physical power systems (CPPS)," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 843–845, Sep.2018.

[6] Y. Tang, Q. Chen, M. Y. Li, Q. Wang, M. Ni, and Y. Liang, "Overview on cyber-attacks against cyber physical power system," *Automation of Electric Power Systems*, vol. 40, no. 17, pp. 59–69, Sep. 2016.

[7] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1515–1524, Sep. 2012.

[8] B. Falahati and Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1677–1685, Jul. 2014.

[9] Y. An, D. Liu, F. Chen, and W. W. Xu, "Risk analysis of cyber physical distribution network operation considering cyber attack," *Power System Technology*, vol. 43, no. 7, pp. 2345–2352, Jul. 2019.

[10] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, Jul./Aug./Sep. 2016.

[11] H. Zhang, Y. F. Qi, J. F. Wu, L. K. Fu, and L. D. He, "DoS attack energy management against remote state estimation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 383–394, Mar. 2018.

[12] Y. Q. Han, J. Guo, C. X. Guo, and H. Huang, "Intelligent substation security risk assessment of cyber physical power systems incorporating software failures," *Proceedings of the CSEE*, vol. 36, no. 6, pp. 1500–1508, Mar. 2016.

[13] T. Zhao, D. Wang, D. X. Lu, Y. Zeng, and Y. L. Liu, "A risk assessment method for cascading failure caused by electric cyber-physical system (ECPS)," in *2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*, Changsha, China, 2015, pp. 787–791.

[14] Y. F. Wang, Y. L. Liu, and J. E. Li, "Deducing cascading failures caused by cyberattacks based on attack gains and cost principle in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 6, pp. 1450–1460, Nov. 2019.

[15] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted attacks," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1000–1009, Aug. 2011.

[16] L. F. Wei, A. H. Moghadasi, A. Sundararajan, and A. I. Sarwat, "Defending mechanisms for protecting power systems against intelligent attacks," in *2015 10th System of Systems Engineering Conference (SoSE)*, San Antonio, TX, USA, 2015, pp. 12–17.

[17] L. Xie, Y. L. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[18] W. Chen, D. R. Ding, H. L. Dong, and G. L. Wei, "Distributed resilient filtering for power systems subject to denial-of-service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1688–1697, Aug. 2019.
[19] Q. Wang, M. Y. Li, Y. Tang, and M. Ni, "A review on research of cyber-attacks and defense in cyber physical power systems part one modelling and evaluation," *Automation of Electric Power Systems*, vol. 43, no. 9, pp. 9–21, May 2019.
[20] P. J. Phillips and G. Pohl, "Prospect theory and terrorist choice," *Journal of Applied Economics*, vol. 17, no. 1, pp. 139–160, May 2014.
[21] L. B. Shi and Z. Jian. "Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model," *Automation of Electric Power Systems*, vol. 40, no. 17, pp. 99–105, Sep. 2016.
[22] Q. Peng, X. L. Wang, Y. Kuang, Y. F. Wang, H. Y. Zhao, Z. C. Wang, and J. H. Lyu, "Hybrid energy sharing mechanism for integrated energy systems based on the Stackelberg game," *CSEE Journal of Power and Energy Systems*, vol. 7, no. 5, pp. 911–921, sept. 2021.

Han Qin received a B.S. degree from Harbin University of Science and Technology, Harbin, China, in 2014, and an M.S. degree from the Harbin Institute of Technology (Shenzhen), Shenzhen, China, in 2016. He is currently pursuing a Ph.D. degree with the Department of Electrical Engineering, Shanghai Jiao Tong university, Shanghai, China. His research interests include smart grid, and cyber-physical systems for the power grid.

Jiaming Weng received B.S. and M.S. degrees in 2008 and 2011, from Shanghai Jiao Tong University, China, and a Ph.D. degree in 2018 from Shanghai Jiao Tong University, China. He is currently a Lecturer with the Electrical Engineering Department of Shanghai Jiao Tong University, China. His research interests include smart grid, and cyber-physical systems for the power grid.

Dong Liu received B.S. and M.S. degrees in 1989 and 1994 respectively from Sichuan University, China, and a Ph.D. degree in 1997 from Southeast University, China. He is currently a Professor with the Electrical Engineering Department of Shanghai Jiao Tong University, China. His research interests include smart grid, and cyber-physical systems for the power grid.

Donglian Qi received a Ph.D. degree in Control Theory and Control Engineering from Zhejiang University, Hangzhou, China, in 2002. Since 2002, she has been with Zhejiang University, where she is currently a Full Professor of Control Science and Engineering. Her research interests include nonlinear systems and control, with applications to energy/power systems, cooperative control, and cyber-physical systems.

Yufei Wang is a Senior Engineer of China Electric Power Research Institute, and obtained a Ph.D. degree from the Wuhan University in 2023. His research interests include grid cyber-physical systems and cyber security.