Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2021) 29: 1479 – 1494

doi:10.3906/elk-1912-68

A cross-space cascading failure hazard assessment method considering betweenness centrality and power loss

Ruzhi XU, Dawei CHEN*, Qizhuo ZONG, Jia LUO
School of Control and Computer Engineering, North China Electric Power University, Beijing, China

Received: 12.12.2019 • **Accepted/Published Online:** 30.10.2020 • **Final Version:** 31.05.2021

Abstract: In order to accurately assess the hazard caused by cross-space cascading failure in the cyber-physical power system, we propose a quantitative assessment method. This method builds a comprehensive framework of assessment that takes into account the betweenness centrality of attack graph and the consequences of failure. The betweenness centrality of each node in the attack graph is used to characterize the frequency of failure. By calculating the number of all nodes on each attack path, the frequency of a certain fault is calculated. The power loss of physical node caused by each cross-space cascading failure is used to characterize the consequences of the fault, which is combined with the frequency of failure and the urgency of troubleshooting to calculate the hazard assessment value of the cross-space cascading failure. Finally, a variety of cross-space cascading failures are implemented in the simulation environment of local cyber-physical power system and their hazards are evaluated. The effectiveness of the proposed assessment method is verified.

Key words: Cyber-physical power system, cyberattack, cross-space cascading failure, fault hazard assessment

1. Introduction

The Cyber-physical power system (CPPS) is a two-dimensional heterogeneous system that realizes the deep coupling of power physical system and cyber space. Its power flow and information flow are interactive and cooperative [1]. As a new form of power system development, CPPS will be an important way to realize smart grid and energy internet [2, 3]. With the increasing integration of the information side and the physical side of the power system, attacks in the cyber space may eventually trigger failures in the physical space. Such failures are called cross-space cascading failures. For example, in February 2006, the U.S. Department of Homeland Security organized a drill to simulate power system anomalies in multiple states caused by the cyberattacks [4]. In 2010, the "Stuxnet" virus attacked the nuclear centrifuge in Iran's power plant and caused severe damage to nuclear industrial infrastructures [5]. Combining the characteristics of failures with mathematical methods to accurately evaluate the hazards of CPPS cross-space cascading failures is of great significance in the current industrial applications of smart grids.

In early research, the security of CPPS was discussed only at a macrolevel: For example, reference[6] demonstrated the possibility of large-scale power outages due to cyberattacks; reference [7] explores the connection between cyberattacks and power system disturbances, and points out that attacks on information systems may disrupt the transient stability of the power system. Some researchers have conceived several typical types of cross-space cascading failures based on actual power business scenarios and deduced their generation pro-

*Correspondence: chendawei@ncepu.edu.cn

cesses. References [8, 9] construct cross-space cascading failures for electrical primary and secondary equipment such as circuit breakers, flexible alternative current transmission systems (FACTS), automatic voltage con-trol (AVC) in smart substations. Combined with the IEEE 39-node model, it was confirmed that cyberattacks can cause power secondary equipment or system failure, and then induce power system disturbances, endangering the normal operation of CPPS. However, the above researches have certain limitations. On the one hand, it is only proposed at macrolevel that CPPS will face greater security risks after the deep integration of cyber space and power systems, and it does not detail all possible categories of cross-space cascading failures. On the other hand, the research results of cross-space cascading failures in specific business scenarios lack universality and there are too many constraints.

At present, some research results have been made in the causes and hazard assessments of cross-space cascading failures: For example, reference [10] discussed the harms of delay, interruption, bit errors and other factors in power communication network on operation of power system; references [11–15] used attack graphs, complex networks, game theory and other methods to assess the hazard of cross-space cascading failures to power systems.

The current research on hazard assessment of cross-space cascading failures is mainly from two perspectives. On the one hand, researchers only pay attention to the construction of attack graph in power systems or cyber-physical power systems and discuss the dangers of their connectivity to system operation [16–18]. On the other hand, researchers only pay attention to the direct damage caused by faults that present on the operation of the power system and grid cyber-physical system (GCPS). In references [19–21], the failures' impact of the power system is assessed respectively according to the stability change of system transient, change of load, change of energy consumption and migration of tidal current. A series of methods for evaluating the credibility indicators of software of cyber-physical system (CPS) is proposed in references [22, 23]. By analyzing the dynamic and multistage characteristics of CPPS cascading failures, based on multiple indicators such as change of tidal current and topological integrity, the hazard of cascading failures have been evaluated in reference [24]. According to the evolution mechanism of cross-space cascading failures, a detection method combining misuse detection and anomaly detection is proposed in references [25, 26]. However, the above researchers only consider one certain factor that affects the magnitude of the failure hazard. The scope of the research has great limitations. On the one hand, some researches only pay attention to the connectivity of cascading failures attack graphs, caused the lack of quantitative calculation indicators that can directly reflect the final physical loss caused by the failure. On the other hand, in some other works, the degree of hazard is reflected only by the migration of tidal current, variation of power or load loss that is explicitly displayed in the final physical space. The characteristics of the attack graphs are not combined, so it could not reflect the important characteristics of the CPPS cross-space cascading failures affected by the cyber-physical interaction.

In order to accurately and comprehensively assess the hazards of cross-space cascading failures on the safand stable operation of CPPS, this paper proposes a hazard assessment method that comprehensively considers the betweenness centrality of attack graph and the power loss of the attack target.

The main contributions of this paper are as follows:

1)We proposed a quantitative assessment framework of hazard assessment , which takes into account the ratio of power loss of attack target and the betweenness centrality of attack paths in attack graph. The index system adopted in this assessment framework includes two kinds of indicators that can reflect the frequency and the impact of the final consequences of failures.

2) Based on the attack graph model of CPPS cross-space cascading failure, the fault transmission process

is analyzed in detail. Meanwhile, considering the influence of constraints on the results of hazard assessment, the disturbance trigger probability P_c is introduced into the assessment method, and the influence of different values of P_c on the results of fault hazard assessment is thoroughly discussed.

3) With the model of 110 kV smart substation as reference, a local CPPS experimental environment is built, and three typical cross-space cascading failures caused by cyberattacks are simulated. Consequently, the effectiveness of the assessment method is verified by quantifying the hazard assessment results of simulation failures and comparing it with those obtained by the assessment method proposed in this paper.

2. The betweenness centrality of attack graph

2.1. The definition of betweenness centrality

Betweenness centrality is a global property of directed graph that is closely related to the connectivity. The shortest path is to use Dijkstra algorithm [27] or Floyd algorithm [28] to calculate the shortest path between any two points on the weighted directed graph. Betweenness centrality reflects the influence of certain nodes or edges on the connectivity of the entire network. Thus it has important practical significance in the fields of community relations, allocation of resource and topology analysis of cyber security, etc. [29].

The betweenness centrality of nodes is one of the main indicator used in the assessment method proposed in this paper. The larger the betweenness centrality of a node, the more frequently the node is used by the shortest path in the entire network, which indicates that the node is more critical to the overall network structure. As shown in Figure 1, it is a six-node weighted directed graph. The betweenness centrality is related to the shortest path. According to the formula derived from the Dijkstra algorithm of the weighted directed graph, the betweenness centrality of nodes A, D, and C are 0, 0, 2. For example, because the number of shortest paths through node D is 0, the betweenness centrality of node D is 0. The betweenness centrality of node A is 0 because A is the starting point of the path. The betweenness centrality of node B is 4, which is the largest (i.e. the proportion of the shortest paths through node B to the total number of shortest paths is the largest). Therefore, the node B is the "key node" of the directed graph.

2.2. The calculation of the betweenness centrality

2.2.1. The betweenness centrality of node

If there are n nodes in a directed graph, the betweenness centrality of the i-th node (i.e. $bc(i)$) can be calculated by Formula (1):

$$bc(i) = \sum_{s \neq i \neq t}^{n} \frac{\sigma_{st}(i)}{\sigma_{st}}. \tag{1}$$

In Formula (1), σ_{st} denotes the total number of all shortest paths from node s to node t, and $\sigma_{st}(i)$ denotes the number of shortest paths through node i in the shortest paths from node s to node t. The practical meaning of $bc(i)$ is the ratio of the number of shortest paths from node s to node t through node i to the total number of all shortest paths from node s to node t.

The calculating process of Formula (1) is similar to Floyd shortest path algorithm, therefore, $bc(i)$ can be calculated by improving the Floyd algorithm:

1) It can consider the attack graph as a weighted directed graph with all edge weights of 1. Firstly, we solve the shortest path between any two nodes s and t of attack graph based on its adjacency matrix, and

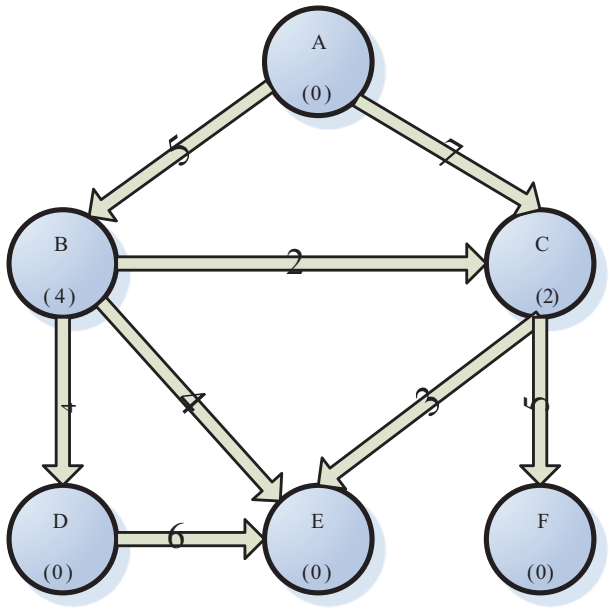

Figure 1. Illustrates the betweenness centrality of nodes and edges in diagraph.

count the sum of shortest paths between every pair of nodes s and t (i.e. σ_{st}).

2) For any node i, if and only if the $D(s,t)$, which means the distance between nodes s and t, match the condition that $D(s,t) = D(s,i) + D(i,t)$ and $\sigma_{st} \neq 0$, then the node i is on the shortest path between s and t. $\sigma_{st}(i)$ is calculated.

3) For all n nodes on the attack graph, the sum $\sum_{s\neq i\neq t}^{n} \frac{\sigma_{st}(i)}{\sigma_{st}}$ is calculated.

2.2.2. The betweenness centrality of edge

If there are m edges in a directed graph, the betweenness centrality of the j-th edge (i.e. bc_j) can be calculated by Formula (2):

$$bc_j = \sum_{p,q\in n}^{m} \frac{\delta_{pq}(j)}{\delta_{pq}}. \tag{2}$$

In Formula (2), δ_{pq} denotes the total number of shortest paths from node p to node q, and $\delta_{pq}(j)$ denotes the number of shortest paths through the j-th edge in the shortest path from node p to node q. In addition, bc_j denotes the proportion of the number of shortest paths through node i from node p to node q to the total number of all shortest paths from node p to node q. The calculation of bc_j is similar to that of $bc(i)$, which can be solved by improving the shortest path algorithm.

3. Cross-space cascading failure hazard assessment method

3.1. General framework of assessment method

{Ci} denotes any node in the cyber space, {Pi} denotes any node in the physical space. Based on the analysis of the causes of CPPS failures, it is known that the occurrence of cross-space cascading failures is closely related

to the information-physical interaction. Therefore, its transmission path is consistent with the transmission path of the information-physical coupling event chain. It all starts from several nodes {Ci} in the cyber space, and propagates through the information-power flow to several nodes {Pi} in the physical space that have a mapping relationship with {Ci}. Then the power flow spreads from {Pi} to other power nodes, eventually causing large-scale cascading failures. Therefore, the starting point of the cross-space cascading failure is the cyberattack on the information topology node, and the end point is the disturbance generated by the physical topology node. So, the attack graph model representing cross-space cascading failures is vertical in space and orthogonal to the horizontal topology network of CPPS, as shown in Figure 2.

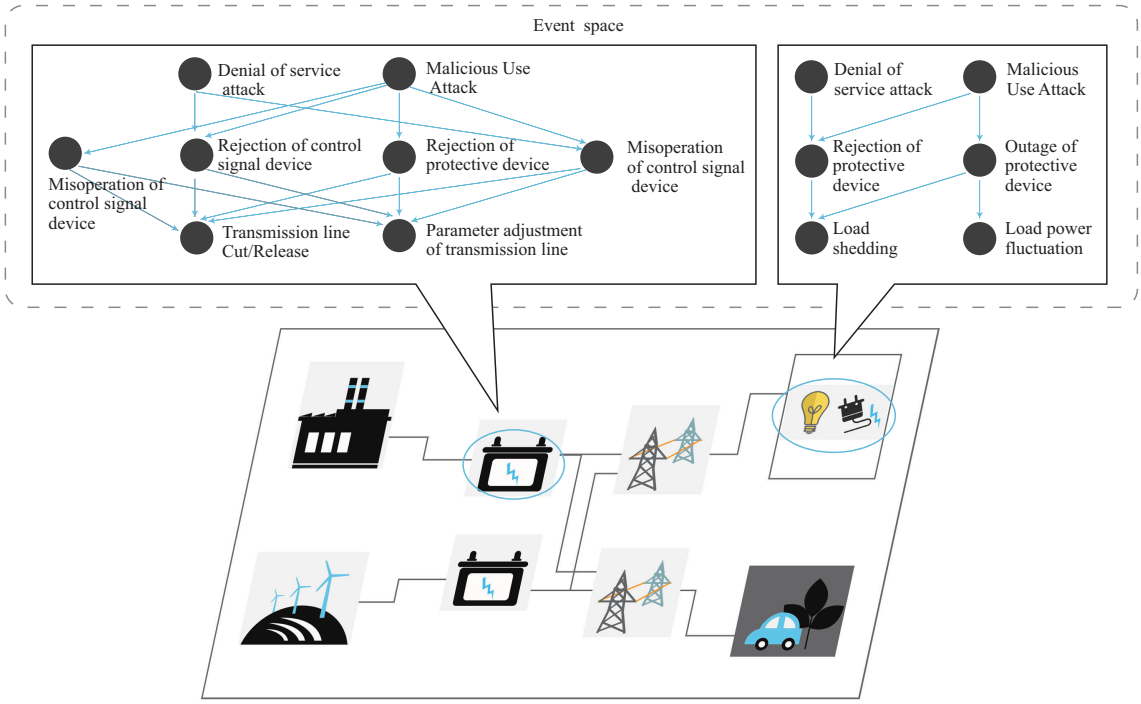

Figure 2. Orthogonal relationship between CPPS physical topology and attack graph.

3.1.1. Mapping of attack graph on CPPS physical topology

Attack graph and attack subgraph. As shown in Figure 3, each node on the attack graph represents an cyberattack, secondary equipment fault or a primary disturbance. Each directed edge in the graph represents the driving relationship between the failure events. If a node of cyberattack is connected with the secondary equipment fault by the directed edge, it indicates that the attack step can be implemented. Each attack path must satisfy the following conditions: It starts from the node of cyberattack of the L_1 layer, passes through the node of secondary equipment fault of the L_2 layer, and reaches the node of primary disturbance of the L_3 layer, and finally converges on the node of the L_4 layer representing "N-1 disturbance of the power system". The specific fault names represented by each node in Figure 3 are shown in Table 1.

By mapping the attack graph of cross-space cascading failures shown in Figure 3 to the actual physical topology of CPPS, a local attack subgraph can be obtained. It reveals the types and evolutionary relationships of cross-space cascading failures that exist in the CPPS topological operating environment. This paper chooses the

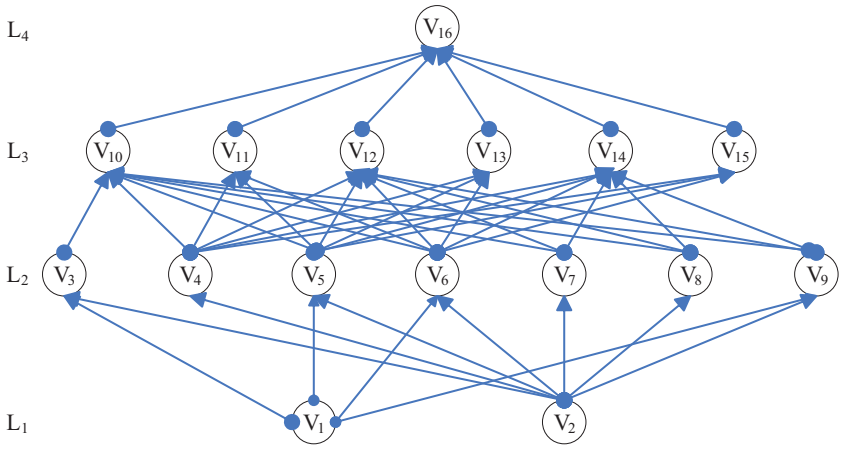

Figure 3. CPPS attack graph.

Table 1. The specific fault name represented by the attack graph nodes.

Node	Specific fault name	Node	Specific fault name
V_1	Denial of service attack	V_9	Outage of protective equipment
V_2	Exploitative attack	V_{10}	Engine cut/release
V_3	Measurement deviation of measuring equipment	V_{11}	Variation of operating parameters of power supply
V_4	Misoperation of control signal device	V_{12}	Transmission line cut/release
V_5	Rejection of control signal device	V_{13}	Variation of operating parameters of transmission
V_6	Outage of control signal device	V_{14}	load cut/release
V_7	Misoperation of protective equipment	V_{15}	Variation of operating parameters of load
V_8	rejection of protective equipment	V_{16}	"N-1" disturbance in power system

operating topology of intelligent substation which conforms to IEC 62351 standard [30]. The attack subgraph obtained by mapping the attack graph of cross-space cascading failure to this topology is shown in Figure 4.

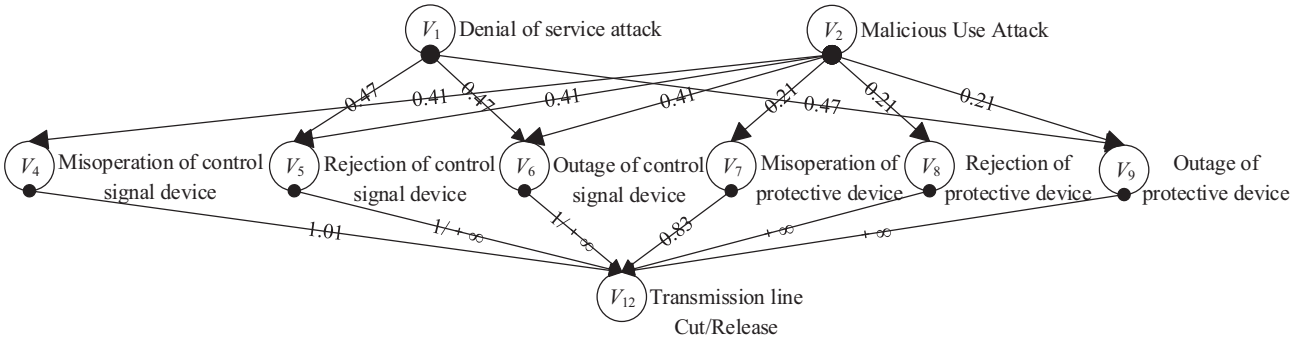

Figure 4. Subgraph of CPPS attack graph.

Edge weight of attack graph. The reciprocal of attack profit or loss for each attack step can be used as the edge weights of attack subgraphs. It is used for subsequent calculation of the betweenness centrality of each directed edge. The definition and calculation method of attack profit or loss are elaborated in reference [31]. Using the calculation method proposed in reference [31], the value of attack profit or loss of each single-step attack in the attack subgraph shown in Figure 4 is calculated. The reciprocal of attack profit or loss value of each single-step attack is used as the weight on each directed edge. The edge with an edge weight of "$1/+\infty$" indicates that the corresponding secondary equipment fault will be latent in the system with a hidden failure that occurs in non-real time, and a transient disturbance will be triggered with a certain conditional probability in the subsequent process.

During the propagation of CPPS cross-space cascading failures, the fault will eventually cause the "N-1" failure of the power physical system (i.e. any independent physical device or power line is cut off) . For example, a tampering attack on the communication network of a substation caused the protective device to malfunction. As a result, the breaker of the substation mistakenly cut the bus line. The final consequence can be manifested by the obvious power loss of affected bus line [32]. Therefore, the assessment method proposed in this paper adds the amount of power loss as one of the assessment indicators.

3.1.2. The hazard factor and assessment framework

According to the failure mode of general industrial system, effects and criticality analysis (FMECA), the index system for failure hazard assessment includes three basic factors: frequency of failure, impact of consequence and emergency degree of troubleshooting. The general method of failure hazard classification is to calculate the hazard level of the failure synthetically by three factors. But in the transmission process of specific cross-space cascading failure in CPPS, if a single fault exists in multiple attack paths, it proves that such a fault is more likely to cause severe system disturbances. The scope of such a fault will be lager, and the overall consequences are generally more serious [15].

The key idea of the failure hazard assessment method proposed in this paper is to combine the betweenness centrality of attack paths with the power loss factor. Then we can obtain a unified evaluation value to quantify the hazard level of cross-space cascading failures. This unified evaluation value is named "cross-space cascading failure hazard factor", and the calculation method is explained in detail below.

According to mentioned above, the framework considers both the frequency of failure and the power loss of attacking target. It is necessary to establish a formula for calculating the failure hazard factor with these two indicators as variables. In order to indicate the proportion of the impact of each indicator on the failure hazard factor, the calculation method is to multiply the frequency factor with the power loss factor.

As showing in Figure 3, each attack path represents a certain cross-space cascading failure, which starts from the node V_1 or V_2 of L_1 and converges to the node V_{16} of L_4. There are nine attack paths in Figure 4. To assess the cross-space cascading failure hazard represented by k-th attack path, the hazard factor of this attack path is defined as R_k, as Formula (3), $k\epsilon\{1, 2, \cdots, 9\}$:

$$R_k = BC_k \times \Delta P_k. \tag{3}$$

In Formula (3), BC_k denotes the total betweenness centrality of the k-th attack path, which is calculated by the product of the betweenness centrality of all nodes and the betweenness centrality of all edges in the path k. ΔP_k denotes the comprehensive fault influence factor caused by cross-space cascading failures represented by the path k. The detailed calculation methods of BC_k and ΔP_k are given in Sections 3.2 and 3.3, respectively.

3.2. The total betweenness centrality of attack path: BC_k

According to the above, the attack path, representing certain kind of cross-space cascading failure, is a multimode event chain model composed of multiple attack paths. Each attack path consists of several independent fault nodes. Each directed edge connecting the precursor node and the successor node on the attack path represents the driving relationship of single-step attack. The weighted value of the directed edge is the profit or loss value of the single-step attack, which indicates the difficulty of the single-step attack.

A strong correlation logic is formed between attacking nodes. Therefore, the cumulative multiplication of betweenness centrality of all independent fault nodes passing through each attack path is taken as the frequency factor of cross-space cascading failures represented by the total betweenness centrality of the attack path. The cumulative multiplication of the betweenness centrality of all edges in the attack path is taken as the emergency degree factor of the cross-space cascading failure removal represented by the total betweenness centrality of the attack path. The total betweenness centrality value BC_k of each attack path is obtained by the two kinds of betweenness centrality. The calculation method of BC_k is as follows Formula (4).

$$BC_k = \prod_{i=i}^{x} bc(i) \times \prod_{i=j}^{y} bc_j \tag{4}$$

In Formula (4), x is the number of nodes passing through the k-th attack path, and $bc(i)$ is the value of betweenness centrality of the $i-th$ node on this attack path. When calculating the betweenness centrality of each node, the number of paths with the node itself as the starting point or end point is not counted (i.e. the value of $bc(i)$ of the start and end points of each attack path is always 0) . Therefore, when using Formula (4) to calculate the BC_k of every attack path, only the betweenness centrality of intermediate nodes on the path are multiplied. y is the number of directed edges passing through the k-th attack path, and bc_j is the value of betweenness centrality of the $j-th$ directed edge on this attack path.

3.3. Influence factor of failure consequence: ΔP_k

P_c is the conditional probability of electric primary disturbance. According to the attack graph of CPPS, it can be known that after the occurrence of secondary equipment fault, there is some certain external constraint for the triggering of the relevant primary disturbance. Some of the disturbances will occur immediately after the secondary equipment fault, such as the circuit breaker malfunction caused by the malicious control command, resulting in the transmission line to be disconnected. In addition to this, the other secondary equipment faults cause the primary disturbances in the indirect and nonreal-time way. For example, after a protective device is failed by the DoS attack, a disturbance will be triggered only when the power load changes and the protective device needs to operate.

We define the conditional probability of electric primary disturbances as P_c , and the value of P_c is determined by the topology of power system and the power measurement value of the CPPS physical side. Generally, if a certain secondary fault can instantly trigger a primary disturbance, the value of condition probability (i.e. P_c) is 1.

Δp is the ratio of power loss. In order to calculate the power loss factor, we define Δp as the ratio of power loss due to a kind of disturbances caused by cross-space cascading failures. The calculation method of

Δp is shown as Formula (5).

$$\Delta p = \frac{|p - p^{'}|}{p} \tag{5}$$

In Formula (5), p is the initial power of the target system, and $p^{'}$ is the power of the system after a disturbance occurs. Combining the Δp with P_c, we can define the power loss factor of the k-th attack path in the attack graph as ΔP_k. ΔP_k can be calculated using Formula (6).

$$\Delta P_k = P_c \times \Delta p \tag{6}$$

3.4. The calculation of failure hazard assessment factor

Using Formula (1), the values of the betweenness centrality of each node in Figure 4 can be calculated, and the betweenness centrality of each edge can be calculated according to Formula (2). According to Formula (4), the BC_k of each attack path in Figure 4 can be calculated by combining the betweenness centrality of node and the betweenness centrality of edge.

For nodes in Figure 4, the conditional probability that V_5, V_6, V_8, and V_9 trigger the primary disturbance is P_c, and the value range of P_c is [0,1). However, other secondary faults, such as misoperation of control signal device and misoperation of protective device, represented by nodes V_6 and V_7 on L_2 layer will instantly trigger the steady state of the power system changing to unsteady state, so the value of P_c of V_3, V_4 and V_7 is 1. After mapping the attack graph to the actual local topology of CPPS, the specific type of primary disturbance can be determined, and the Δp can be calculated by Formula (5). In this paper, the power loss caused by the primary disturbance on the transmission represented by node V_{12} in Figure 4 is abbreviated as Δp_{trans}.

The conditional probability of electric primary disturbance P_c and the ratio of power loss Δp of each attack path are substituted into the Formula (6). The power loss factors of nine cross-space cascading failure attack paths in Figure 4 are calculated, as shown in Table 2.

By substituting the results in Table 1 into Formula (3), the hazard factor R_k of cross-space cascading failure represented by each attack path in Figure 4 is calculated, as shown in Table 3.

Table 2. The power loss factors of nine cross-space cascading failure attack paths in Figure 4.

The path of cross-space failure	R_k	The path of cross-space failure	R_k
(V_1, V_5, V_{12})	$P_c \cdot \Delta p_{trans}$	(V_2, V_5, V_{12})	$P_c \cdot \Delta p_{trans}$
(V_1, V_6, V_{12})	$P_c \cdot \Delta p_{trans}$	(V_2, V_6, V_{12})	$P_c \cdot \Delta p_{trans}$
(V_1, V_9, V_{12})	$P_c \cdot \Delta p_{trans}$	(V_2, V_7, V_{12})	Δp_{trans}
(V_2, V_4, V_{12})	Δp_{trans}	(V_2, V_8, V_{12})	$P_c \cdot \Delta p_{trans}$
(V_2, V_9, V_{12})	$P_c \cdot \Delta p_{trans}$	-	-

4. Experiment

4.1. The implement of simulation environment

In order to verify the rationality of the failure hazard assessment method proposed in this paper, the CEPRI-36 node simulation environment based on an 110kV intelligent substation structure is selected to build a local

Table 3. The hazard factor R_k of cross-space cascading failure represented by each attack path in Figure 4.

The path of cross-space failure	R_k	The path of cross-space failure	R_k
(V_1, V_5, V_{12})	$0.89P_c{\cdot}\Delta p_{trans}$	(V_2, V_5, V_{12})	$0.67P_c \cdot \Delta p_{trans}$
(V_1, V_6, V_{12})	$0.89P_c \cdot \Delta p_{trans}$	(V_2, V_6, V_{12})	$0.67P_c \cdot \Delta p_{trans}$
(V_1, V_9, V_{12})	$1.22P_c \cdot \Delta p_{trans}$	(V_2, V_7, V_{12})	$0.17\Delta p_{trans}$
(V_2, V_4, V_{12})	$0.17\Delta p_{trans}$	(V_2, V_8, V_{12})	$0.39P_c \cdot \Delta p_{trans}$
(V_2, V_9, V_{12})	$1.37P_c \cdot \Delta p_{trans}$	-	-

CPPS model, as shown in Figure 5. The detailed components of the simulation environment are described in Appendix.

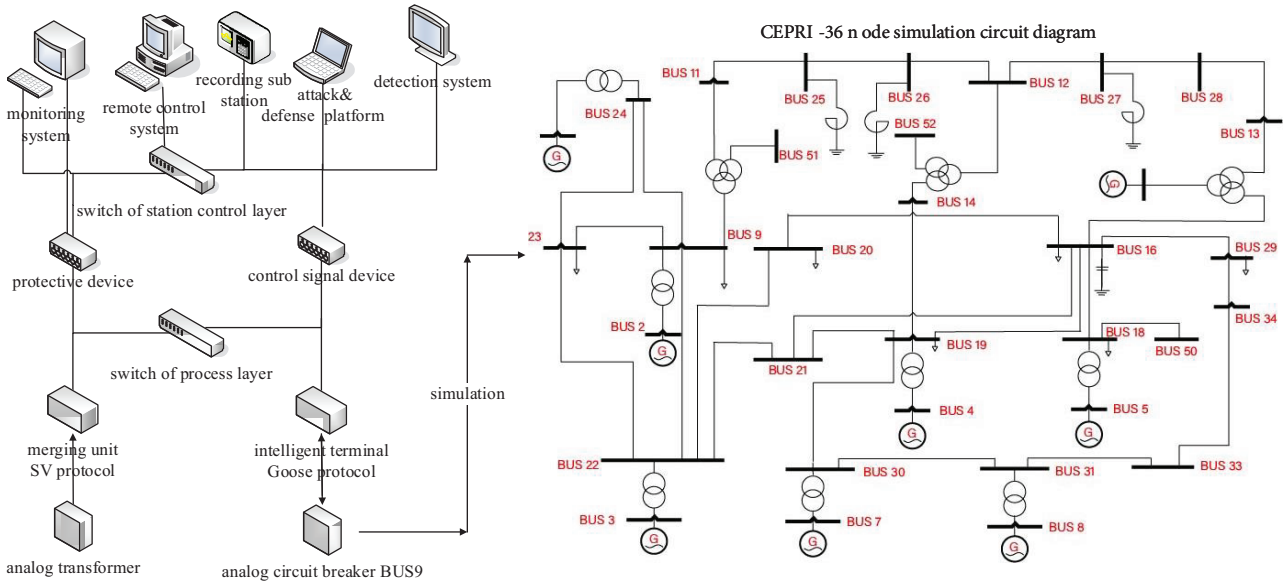

Figure 5. The simulation environment of CPPS based on the CEPRI-36 node simulation environment of 110 kV intelligent substation structure.

In the initial simulation environment, the CEPRI-36 node system is in normal operating state. The position where the disturbance occurs is selected as the i-terminal of the BUS9 node, and the circuit breaker action is simulated to control the open and closure of the BUS9. The simulation cyberattack types include DoS (denial of service) attack and malicious exploit attack, and real-time capture and analysis of communication message in controlling layer are implemented at the same time to record the entire process of cyberattack.

Because the simulation environment is based on the structure of smart substation, and the target equipment is selected as control signal device and protective device of controlling layer. The attack subgraph of attack paths is considered same as Figure 4.

4.2. Cross-space cascading failure simulation

In order to more intuitively and accurately reflect the performance of this assessment method, it is necessary to select cyberattack types that occur as frequently as possible in the CPPS simulation environment for exper-

iments. According to the historical statistics of various kinds of cyberattacks in CPPS simulation environment, buffer overflow attack, DoS attack and fuzzing attack are selected to carry out simulations of cross-space cascading failures. In this experiment, different cyberattacks will finally cause different cross-space cascading failures, which can be divided into three types:

4.2.1. Buffer overflow attack

Firstly, the IP address of the target host and the communication port of control message are determined by the IP address and port scanning tool of the mobile attack and defense platform. Then the host is intruded by buffer overflow attack, and malicious control program is implanted into the host through remote control software. Finally, wrong operation commands are sent to the intelligent terminal connected to the target host, resulting in misoperation of simulated circuit breaker.

As shown in Figure 6, after the malicious control attack is carried out, some attack messages are intercepted by the packet capture tool. It can be seen that the message contains commands leading to misoperation of the simulated circuit breaker.

No.	Time	Source	Destination	Protocol	Length	Info
80	7.357486000	192.168.1.14	192.168.1.16	TCP	60	startron > irdmi [PSH, ACK] Seq=324 Ack=72 Win=46523 Len=4
81	7.358038000	192.168.1.14	192.168.1.16	TCP	1514	startron > irdmi [PSH, ACK] Seq=328 Ack=72 Win=46523 Len=1460
82	7.358041000	192.168.1.14	192.168.1.16	TCP	1514	startron > irdmi [ACK] Seq=1788 Ack=72 Win=46523 Len=1460
83	7.358057000	192.168.1.14	192.168.1.16	TCP	1514	startron > irdmi [ACK] Seq=3248 Ack=72 Win=46523 Len=1460
84	7.358203000	192.168.1.14	192.168.1.16	TCP	1514	startron > irdmi [ACK] Seq=4708 Ack=72 Win=46523 Len=1460
85	7.358525000	192.168.1.14	192.168.1.16	TCP	1514	startron > irdmi [ACK] Seq=6168 Ack=72 Win=46523 Len=1460
86	7.358527000	192.168.1.16	192.168.1.14	TCP	60	irdmi > startron [ACK] Seq=72 Ack=1788 Win=256 Len=0

Figure 6. Specific information such as the time, source and destination IP of the malicious control attack message.

4.2.2. Denial of service attack

By using UDP flood tool, a large number of protocol messages of false user packets are sent to the protective device at the same time, which could run out the communication bandwidth of the protective device, thus paralyzing the whole communication system. As a result, the Goose/SV message can no longer be sent and received normally, thus making the remote control center unable to control the circuit breaker through protective device. Once the operating status of the power system changes, the protective device needs to operate. But the circuit breaker is actually out of control, a power primary disturbance will occur subsequently.

4.2.3. Fuzzing attack

To carry out fuzzing attack through the mobile attack and defense platform, a large number of deformed messages which violate the IEC 61850 protocol [33] are sent to the protective device. If the protective device fails to handle the deformed messages properly, it will be down and restart. Cyclic restart within a certain period of time will cause the communication function between the protective device and the simulated circuit breaker to be paralyzed, causing the protective device to lose control of the simulated circuit breaker. Generally, fuzzing attack messages have malformed features such as a overlong length, invalid SPDU filler characters or illegal MAC destination addresses. For example, the message "03 00 B3 90 11 E0 00 00 00 04 00 C1 02 00 01 C2 02 00 01 C0 01 0A" whose "packet length" field value "B3 90" exceeds the range, which means this is a deformed message that cannot be parsed by the protective device.

4.3. Analysis of experimental results

By using transient analysis tools of power system, it can be know that in the simulation environment of CEPRI-36 bus system in the initial operating state, the proportion of power loss caused by disconnection of BUS9 node due to the malfunction of the circuit breaker is 38.16%, which means the value of Δp_{trans} in Table 2 is 0.3816. With the accurate value of Δp_{trans}, the value R_k in Table 3 of all cross-space cascading failures in the current simulation environment can be calculated, as shown in Table 4.

Table 4. The values of R_k of simulated cascading failures attack paths.

The path of attack	R_k	The path of attack	R_k
(V_1, V_5, V_{12})	$0.89 * 0.3816 P_c$	(V_2, V_6, V_{12})	$0.67 * 0.3816 P_c$
(V_1, V_6, V_{12})	$0.89 * 0.3816 P_c$	(V_2, V_7, V_{12})	$0.17 * 0.3816$
(V_1, V_9, V_{12})	$1.22 * 0.3816 P_c$	(V_2, V_8, V_{12})	$0.39 * 0.3816 P_c$
(V_2, V_4, V_{12})	$0.17 * 0.3816$	(V_2, V_9, V_{12})	$1.37 * 0.3816 P_c$
(V_2, V_5, V_{12})	$0.67 * 0.3816 P_c$	-	-

In the local CPPS simulation environment, three attack paths $\langle V_1, V_5, V_{12}\rangle$, $\langle V_2, V_4, V_{12}\rangle$ and $\langle V_2, V_8, V_{12}\rangle$ are selected to represent the simulated attacks. Based on the simulation results, the hazard of these three cross-space cascading failures is evaluated to verify the effectiveness of the proposed failure hazard assessment method, as shown in Table 5.

Table 5. The ranking of the cross-space cascading failure hazard factor R_k represented by the three attack paths could be determined by the value range of P_c.

The path of attack	R_k	The process of cross-space cascading failure simulation	External conditions for triggering power primary disturbance of electric
(V_1, V_9, V_{12})	$1.22 * 0.3816 P_c$	The protective device is attacked by DoS and the communication function is paralyzed. It cannot process the status information sent back by the simulated circuit breaker.	Changes in the operating status of the power system
(V_2, V_4, V_{12})	$0.17 * 0.3816$	The control signal device is attacked by buffer overflow and receives the wrong line monitoring data, which causes the misoperation of simulated circuit breaker.	None
(V_2, V_8, V_{12})	$0.39 * 0.3816 P_c$	Protective devices are attacked by Fuzzing attack and lose control of simulated circuit breakers	Changes in the operating status of the power system

Table 5 shows that the ranking of the cross-space cascading failure hazard factor R_k represented by the three attack paths could be determined by the value range of P_c. In this experiment, focusing on the cross-domain effect of fault, the comprehensive fault influence factor is taken the form of modulo of the complex number, and the value range of Pc is divided into the following two cases:

Case 1: $0.39*0.3816P_c \leq 0.17*0.3816 \leq 1.22*0.3816P_c$. By solving the inequality of Case 1, the range of P_c is [0.14,0.43) . It shows that when the conditional probability of electric primary disturbance P_c is in [0.14,0.43), the attack path with the highest value of failure hazard assessment is $\langle V_1, V_9, V_{12}\rangle$, while the attack path with the lowest value of failure hazard assessment is $\langle V_2, V_8, V_{12}\rangle$.

Case 2: $0.17*0.3816+0.25i \leq 0.39*0.3816P_c \leq 1.22*0.3816P_c$. By solving the inequality of Case 2, the range of P_c is [0.43,1] . It shows that when P_c is in [0.43,1] , the attack path with the highest failure hazard assessment is $\langle V_1, V_9, V_{12}\rangle$, while the attack path with the lowest failure hazard assessment is $\langle V_2, V_4, V_{12}\rangle$.

Through the analysis of the above simulation results, the following conclusions can be drawn:

1) According to the steps of simulation experiments, the cause and evolution of cross-space cascading failures are closely related to the coupling interaction between cyber space and physical space. The evolution process of most cross-space cascading failures has a causal relationship of "cyber disturbance → power secondary equipment fault → power primary disturbance" , which represents a typical event chain model.

2) From the perspective of cyberattack methods, the cross-space cascading failures caused by DoS attack and fuzzing attack will trigger a perturbation only when the operating status of power system changes (i.e. only when P_c=1, the damage of the failure will be explicit on the primary side of the power system, and the simulated circuit breaker will trigger a primary disturbance due to out-of-control) . When the power system is in steady state, the secondary equipment faults caused by these two types of cyberattacks will be hidden in the system in the form of non-real-time invisible faults. Therefore, during the corresponding failure hazard assessment, the value of P_c needs to be discussed. For the malfunction of control devices caused by malicious control attacks, a corresponding disturbance will be triggered directly. Although the value of P_c is not considered, the implementation of malicious control attacks is more difficult than DoS attack. Therefore, the betweenness centrality of this attack path reflected the frequency of failure and the emergency degree of troubleshooting is low, and the assessment value R_k of malicious control attack is not necessarily higher than that caused by DoS attack.

3) By analyzing the failure hazard assessment results of three simulated attacks, the total betweenness centrality of each attack path representing each failure is regarded as the first coefficient of R_k. The larger the coefficient, the greater the comprehensive evaluation value of the frequency of failure and the emergency degree of troubleshooting. After adding the power loss factor to R_k, the ranking of failure hazard assessment values may change. Some types of cross-space cascading failure do not show high frequency and emergency, but the direct impact consequences to cyber space or physical space are greater. Interruption and isolation measures should be taken to deal with these cross-space cascading failures which cause large power loss on physical side.

4) In this simulation experiment, a local CPPS model is built by referencing the intelligent substation environment, and the disturbance of transmission lines caused by cross-space cascading failures is simulated. Analogously, cross-space cascading failures can also cause N-1 disturbances at other locations of primary side such as generators and loads. If multiple cross-space cascading failures concurrently occur in the same local CPPS environment, multiple devices on primary side will be disturbed at the same time, finally resulting in power N-X disturbances. In the future work, if it is necessary to assess the N-X disturbances caused by cooperative cyberattacks, it may be achieved by improving the assessment framework proposed in this paper.

5. Conclusion

The operation of CPPS depends on the mechanism of coupling and interaction between cyber space and physical space, but it also brings security problems to be solved urgently, especially the harm caused by cross-space

cascading failures. In this paper, based on the attack graph model of CPPS cross-space cascading failures, a method for hazard assessment of cross-space cascading failures is proposed, which considers the betweenness centrality of attack graph and power loss of the target. This method can be used to quantify the hazards of various cross-space cascading failures in CPPS.

To further improve this quantitative assessment method of CPPS cross-space cascading failures, adding other factors into the index system and exploring the monitoring mechanism of cross-space cascading failures combined with machine learning and data mining will be the focus of the next phase of research.

References

[1] Ilic MD, Xie L, Khan UA,Moura JMF. Modeling of future cyber–physical energy systems for distributed sensing and control. IEEE Transactions on Systems,Man,and Cybernetics-Part A: Systems and Humans 2010; 40 (4): 825-838. doi: 10.1109/TSMCA.2010.2048026

[2] Shi X, Li Y, Cao Y, Tan Y. Cyber-physical electrical energy systems: challenges and issues. CSEE Journal of Power and Energy Systems 2015; 1 (2): 36-42. doi: 10.17775/CSEEJPES.2015.00017

[3] Xue Y, Yu X. Beyond smart grid—cyber–physical–social system in energy future [point of view]. Proceedings of the IEEE 2017; 105 (12): 2290-2292. doi: 10.1109/JPROC.2017.2768698

[4] Zeller M. Myth or reality—Does the aurora vulnerability pose a risk to my generator? In: IEEE 64th Annual Conference for Protective Relay Engineers; College Station, TX, USA; 2011. pp. 130-136. doi: 10.1109/CPRE.2011.6035612

[5] Langner R. Stuxnet: dissecting a cyberwarfare weapon. IEEE Security & Privacy 2011; 9(3): 49-51. doi: 10.1109/MSP.2011.67

[6] Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature 2010; 464 (7291): 1025-1028. doi: 10.1038/nature08932

[7] Sridhar S, Hahn A, Govindarasu M. Cyber–physical system security for the electric power grid. Proceedings of the IEEE 2011; 100 (1): 210-224. doi: 10.1109/jproc.2011.2165269

[8] Liu S, Chen B, Zourntos T, Kundur D, Butler-Purry KL. A coordinated multi-switch attack for cascading failures in smart grid. IEEE Transactions on Smart Grid 2014; 5 (3): 1183-1195. doi: 10.1109/TSG.2014.2302476

[9] Chen B, Butler-Purry KL, Kundur D. Impact analysis of transient stability due to cyber attack on FACTS devices. In: IEEE 2013 North American Power Symposium (NAPS); Manhattan, KS, USA; 2013. pp.1-6. doi: 10.1109/NAPS.2013.6666849

[10] Cai Y, Cao Y, Li Y, Huang T, Zhou B. Cascading failure analysis considering interaction between power grids and communication networks. IEEE Transactions on Smart Grid 2015; 7(1): 530-538. doi: 10.1109/TSG.2015.2478888

[11] Xiang Y, Truong M. Acquisition of causal models for local distributions in Bayesian networks. IEEE transactions on cybernetics 2013; 44 (9): 1591-1604. doi: 10.1109/tcyb.2013.2290775

[12] Srivastava A, Morris T, Ernster T, Vellaithurai C, Pan S et al. Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Transactions on Smart Grid 2013; 4 (1): 235-244. doi: 10.1109/TSG.2012.2232318

[13] Chen TM, Sanchez-Aarnoutse JC, Buford J. Petri net modeling of cyber-physical attacks on smart grid. IEEE Transactions on Smart Grid 2011; 2 (4): 741-749. doi: 10.1109/tsg.2011.2160000

[14] Law Y W, Alpcan T, Palaniswami M. Security games for risk minimization in automatic generation control. IEEE Transactions on Power Systems 2014; 30 (1): 223-232. doi: 10.1109/tpwrs.2014.2326403

[15] Vellaithurai C, Srivastava A, Zonouz S, Berthier R. CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures. IEEE Transactions on Smart Grid 2015; 6 (2): 566-575. doi: 10.1109/TSG.2014.2372315

[16] Yufei W, Kunlun G, Ting Z, Jian Q. Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph. Proceedings of The Chinese Society for Electrical Engineering 2016; 36 (6): 1490-1499 (in Chinese). doi: 10.13334/j.0258-8013.pcsee.2016.06.004

[17] Dichen L, Xingpei J, Bo W, Fei T. Topological vulnerability analysis and countermeasures of electrical communication network based on complex network theory. Power System Technology 2015; 39 (12): 3615-3621 (in Chinese). doi: 10.13335/j.1000-3673.pst.2015.12.042

[18] Zhaoyang Q, Tengyue Z, Yu Z, Nan Q, Yuqing L et al. A method for determining risk propagation threshold of power cyber physical system network based on percolation theory. Automation of Electric Power Systems 2020; 44 (4):16 (in Chinese). doi: 10.7500/AEPS20190227002

[19] Wei J, Kundur D. Two-tier hierarchical cyber-physical security analysis framework for smart grid. In: IEEE 2012 Power and Energy Society General Meeting; San Diego, California, USA; 2012. pp.1-5. doi: 10.1109/PESGM.2012.6345633

[20] Kolacinski R, Loparo K. A mathematic framework for analysis of complex cyber-physical power system. In: IEEE 2012 Power and Energy Society General Meeting; San Diego, California, USA; 2012. pp. 1-8. doi: 10.1109/PESGM.2012.6344956

[21] Xia Z, Zhou Y, Ming N, Chengjie B, Husheng L et al. Security evaluation of distribution network CPS considering cyber-physical combinations for anticipated fault screening. Electric Power 2020; 53 (1): 40-48 (in Chinese). doi: 10.11930/j.issn.1004-9649.201911139

[22] Mei R. Trustworthiness evaluation method for CPS software based on multi-attributes. Computer Science 2013; 40 (11): 187-190 (in Chinese). doi: 10.3969/j.issn.1002-137X.2013.11.039

[23] Yuzhen S, Kan Z, Guangquan Z, Mingcai C, Xiaogang S et al. A trustworthiness evaluation framework for CPS software. Computer and Digital Engineering 2012; 40 (10): 51-54 (in Chinese). doi: 10.3969/j.issn.1672-9722.2012.10.016

[24] Yuqi H, Chuangxin G, Bingquan Z, Lizhong X. Model cascading failures in cyber physical power system based on improved percolation theory. Automation of Electric Power Systems 2016; 40 (17): 30-37 (in Chinese). doi: 10.7500/AEPS20160411004

[25] Yufei W, Yanli L, June L. 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 2019; 7 (6): 1450-1460. doi: 10.1007/s40565-019-0500-2

[26] Yufei W, Jian Q, June L. A station level early warning method of cascading failures across space based on attack gain and cost principle in GCPS. Electric Power 2020; 53 (1): 92-99 (in Chinese). doi: 10.11930/j.issn.1004-9649.201912082

[27] Dijkstra EW. A note on two problems in connexion with graphs. Numerische Mathematik 1959; 1 (1): 269-271. doi: 10.1007/BF01386390

[28] Floyd RW. Algorithm 97: shortest path. Communications of the ACM 1962; 5 (6): 345. doi: 10.1145/367766.368168

[29] Zhuoqun X, Wenhuan L, Lalin J, Ming X. Path analysis attack prediction method for electric power CPS. Journal Publishing Center of Tsinghua University Press 2018; 58 (02): 157-163 (in Chinese). doi: 10.16511/j.cnki.qhdxxb.2018.26.012

[30] IEC 62351: Power systems management and associated information exchange - Data and communication security - All parts. Geneva, Switzerland: International Electrotechnical Commission, 2020.

[31] Yufei W, June L, Jian Q, Yanli L. A novel selection sorting method of cascading failures across space considering attack gain and cost. Power System Technology 2018; 12 (12): 3926-3934 (in Chinese). doi: 10.13335/j.1000-3673.pst.2018.1130

[32] Yin Z, Xianyong X, Changsong L. Vulnerability analysis and improvement strategy of power-information coupled networks considering cyber physical interaction. Power System Technology 2018; 42 (10): 3136-3147 (in Chinese). doi: 10.13335/j.1000-3673.pst.2017.2602

[33] IEC 61850: Communication networks and systems in substations. Montreal, Canada: International Electrotechnical Commission, 2004.

Appendix A: 1.Introduction of CPPS simulation environment based on CEPRI-36 The simulation environment consists of an 110 kV intelligent substation (including the actual system of information equipment and secondary equipment, the simulation device of primary equipment) and the classical power system examples (IEEE, CEPRI) in the form of simultaneous digital-analog hybrid simulation. The interaction between cyber space and physical space in local CPPS can be restored to a limited extent. The simulated circuit breaker in the simulation environment of intelligent substation is located at the i-terminal of bus BUS9 of CEPRI-36 bus system.

Mobile attack platform is chosen as the tool to implement cyberattacks, which contains a variety of software to simulate cyberattacks, such as AdVanced Scanner, remote tool of malicious control, UDP flooder and fuzzing attack. The attack tools are used to attack the information nodes in the local CPPS model (monitor and protective device of controlling layer) , and the message grabbing tools (Wireshark, etc.) are used to capture and analyze the network communication messages between the controlling layer and the processing layer. In addition, in order to simplify the calculation of perturbation effect of the cyberattack on the local CPPS model, the attacker is restricted to use limited resources (i.e. the global topology of local CPPS simulation model cannot be fully grasped, and only a single node can be attacked).