IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 20 October 2022, accepted 22 November 2022, date of publication 28 November 2022,
date of current version 28 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3224953

RESEARCH ARTICLE

Expected Failure Method and Its Analysis for Safety Evaluation in a Cyber-Physical Power System

YAN WANG [1], CHENGCHENG FENG [1], YAN LI [1], (Member, IEEE), TIANQI XU [1], AND MENGMENG ZHU [2]

[1] Key Laboratory of Cyber-Physical Power System of Yunnan Colleges and Universities, Yunnan Minzu University, Kunming 650504, China
[2] Intelligent Perception Innovation Studio in Power Science Research Institute, Yunnan Power Grid Company Ltd., Kunming 650000, China

Corresponding author: Yan Li (yan.li@ymu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 62062068.

ABSTRACT With the development of communication technology, power and information systems have become deeply coupled and have become the most massive and complex cyber-physical power systems (CPPSs), resulting in certain risks to the safe operation of power systems. In this paper, a CPPS security assessment method based on the expected failure method and considering combined information attacks is proposed. Due to the large number of nodes in modern information systems, enumerating all possible combinations of system failures for evaluation and analysis is unrealistic. By considering the topological relationship of the CPPS and the electrical properties of coupled physical nodes, the idea of first screening information nodes is proposed in this paper to filter the information nodes. The impact of combined information attacks on the expected physical fault handling process is analyzed, and a safety evaluation index for the distribution network is provided. In addition, the proposed method is applied to the IEEE-118 system and compared with previous evaluation methods to verify its effectiveness.

INDEX TERMS Expected failure analysis, coordinated information attack, first screening, combined failures.

I. INTRODUCTION

With the development of communication technology, the modern power system has gradually evolved into a cyber-physical power system (CPPS) [1], in which the information network and the physical network are deeply integrated. Compared with traditional power systems, modern CPPSs can perceive and analyze the operating status of the power system and have more advantages in optimal power flow distribution, fault handling and recovery, and voltage and load control [2], [3], [4]. However, the deep integration of the power and communication systems also brings new threats to the safe operation of the power system [5], and cyberattacks are one of the main threats facing smart grids. Additionally, cyberattacks against power grid information systems have recently become more frequent, such as the Stuxnet worm attack on the Iranian nuclear power plant network [6], the Ukrainian blackout [7], and the 814 blackout in the United States and Canada. The Iranian Stuxnet worm attack was a single cyberattack, i.e., an attack on a single information node, and its impact and scope were relatively small. The power outage in Ukraine was a combined information attack, i.e., a simultaneous launching of different types of network attacks on multiple information nodes, resulting in paralysis of multiple substations in Ukraine and power outages for hundreds of thousands of people [8]. These two events show that combined information attacks pose a more serious threat to the safe operation of power systems. However, most CPPS research has primarily been aimed at single cyberattacks. Therefore, carrying out research on combined information attacks is necessary.

Currently, the expected failure method [9], [10], [11], [12], [13] is usually used in power system stability control and fault screening research in the power field [14]. However, there are

The associate editor coordinating the review of this manuscript and approving it for publication was Vahid Vahidinasab.

fewer applications in CPPS safety assessment of a distribution network. Reference [13] is based on the expected failure method, starting from the perspective of the cyber-physical combination of expected failures to evaluate the safety of the CPPS in the distribution network. This method has two flaws: First, the establishment of the combined fault set is based on the enumeration method, which considers all the communication paths through which the fault information is uploaded and issued. Since the information nodes in each path are set to fail one by one to construct the information-physical combined fault set, when the number of nodes in the network increases, the number of enumerated faults exponentially increases. As a result, the efficiency of this evaluation method is greatly affected by the scale of the system. Second, the expected failure type is too unvarying since it is simply the failure of a single information node.

However, the real forms of network attacks actually include false data injection (FDI) attacks [15], denial of service (DoS) attacks [16], and delay attacks [17]. Furthermore, the blackout in Ukraine can be confirmed to have actually originated from combined information attacks, which have a more serious impact on the power grid. Therefore, the expected failure method has low applicability to a power grid. Based on the above analysis, a new CPPS security evaluation method for distribution networks is proposed, and it is based on the expected failure method and considers combined information attacks. The main contributions of this paper are as follows:

- Critical node identification ideas are applied to expected failure methods. To solve the problem of the low efficiency of enumeration screening, the information node to be attacked is screened at the beginning. Based on the topological characteristics of the information node and the electrical characteristics of the coupled physical node, an information node screening algorithm is proposed to filter out the key information nodes, which greatly reduces the number of combined failures that need to be enumerated. In addition, to verify the rationality of the screening method, the traditional betweenness and the classical node deletion sorting method are used for comparison in simulations.
- More than one type of attack is considered in this paper. In terms of fault types, based on the physical fault isolation process, the situation in which multiple information nodes are simultaneously attacked is considered, and it is assumed that the attack types are DoS and FDI attacks. This method fills the gap in the application of expected failure methods to combined information attacks.
- The approach is more applicable to modern power systems. The traditional failure prediction method lacks the analysis of multi-information physical failure, The proposed method compensates for this defect. It is less restricted by the system scale after the fault screening algorithm and can be used for safety assessment of modern complex power systems. This method is applied to the analysis the IEEE-118 system, and the feasibility and effectiveness of the evaluation method are evaluated.

II. MODELING OF EXPECTED COMBINED ATTACKS

A. CPPS MODELING OF DISTRIBUTION NETWORKS

The structure of a node power network can be represented by $G = (V_P, E_P, H_P)$, where V_P is the set of all nodes in the grid, E_P is the set of transmission lines in the network, and H_P is the grid correlation matrix. A node information network is represented by $C = (V_C, E_C, H_C)$, where V_C is the set of information network nodes, E_C is the set of links and H_C is the correlation matrix of the information network; both networks are bidirectional networks, propagating the flow of energy and information. The connection relationship between nodes in a CPPS network can be represented by an adjacency matrix A.

$$A = \begin{bmatrix} H_{P\,m\times m} & D_{m\times n} \\ I_{n\times m} & H_{C\,n\times n} \end{bmatrix} = (a_{ij})_{(m+n)\times(m+n)}, \tag{1}$$

where a_{ij} indicates whether there is an edge between nodes; if an edge exists, this value is 1, and it is 0 otherwise. $D_{m\times n}$ and $I_{n\times m}$ represent the dual network coupling matrix.

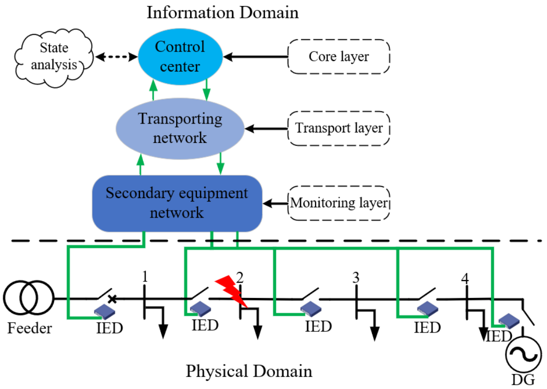

FIGURE 1. Structure diagram of the cyber-physical power system.

Figure 1 shows a structural diagram of the CPPS, in which the information network is divided into a core layer, a transport layer and a monitoring layer. The physical network is composed of various electrical components. The secondary equipment network is directly connected to the grid to monitor the operating status of the power system in real time, upload the grid data to the control center via the transmission network, analyze the status of the power system, and adjust the power system in real time.

B. COMBINED INFORMATION ATTACK MECHANISM

For CPPSs, the main targets of DoS attacks are the transmission nodes and monitoring nodes in the information network. By constantly sending forged data packets, the resources of the information node are exhausted, the information node is paralyzed, and the information flow transmission is blocked. It is assumed that when an information node suffers a DoS attack, the node completely fails [18]. In addition, we assume that the node cannot be repaired. Furthermore, the matrix that denotes the node states after the DoS attack is named Z_{DoS}.

$$Z_{DoS} = \left[Z_{c1}\ Z_{c2}\ Z_{c3} \cdots Z_{cm} \right], \tag{2}$$

where Z_{ci} indicates whether a node has experienced a DoS attack; $Z_{ci} = 1$ indicates that node i has been attacked, and $Z_{ci} = 0$ indicates that node i is operating normally.

FDI attacks tamper with the monitoring data, which affects the state estimation process of the control center and causes the state estimator to output the wrong value to the system operator, which may lead to the wrong control decision [19], [20]. Additionally, it is assumed that the attacker is allowed to completely control the information node; that is, the monitoring data or instructions of the node can always be tampered with. The network state matrix Z_{FDI} after an FDI attack is

$$Z_{FDI} = \left[Z_{d1}\ Z_{d2}\ Z_{d3}\ \cdots\ Z_{dm}\right], \tag{3}$$

where Z_{di} indicates whether a node has experienced an FDI attack, with $Z_{di} = 2$ indicating that node i has been attacked and $Z_{di} = 0$ indicating that node i is operating normally.

When a DoS attacks a communication device, it will continue to occupy a large bandwidth for sending fake data packets, which hinders normal data transmission. If the fake data packet contains FDI information, and the dispatch center accepts and trusts the data, one piece of communication equipment will be subjected to both DoS and FDI attacks. After a communication devices experiences a DoS attack and an FDI attack simultaneously, the network state matrix Z_{DF} is:

$$Z_{DF} = [Z_{e1} \quad Z_{e2} \quad Z_{e3} \quad \cdots \quad Z_{em}], \tag{4}$$

where Z_{ei} indicates whether the node has experienced both DoS and FDI attacks, $Z_{ei} = 3$ indicates that node i has been attacked, and $Z_{ei} = 0$ indicates that the node is operating normally.

Due to the high security level of control center nodes and the low success rate of malicious attacks, this article considers only the situation in which the transmission and monitoring nodes are attacked; that is, DoS and FDI attacks are carried out on multiple information nodes simultaneously. The network state matrix can be expressed as

$$Z = Z_{DoS} + Z_{FDI} + Z_{DF}, \tag{5}$$

$$Z = \left[Z_1\ Z_2\ Z_3\ \cdots\ Z_m\right]. \tag{6}$$

Since different types of attacks are assumed to be launched against different nodes, the nodes have three states at this time, which can be expressed as

$$z_i = \begin{cases} 1, & \text{node } i \text{ is attacked by a DoS,} \\ 2, & \text{node } i \text{ is attacked by an FDI,} \\ 3, & \text{node } i \text{ is attacked by a DoS and an FDI,} \\ 0, & \text{node } i \text{ is running normally.} \end{cases} \tag{7}$$

III. EVALUATION MODEL ESTABLISHMENT

A. PHYSICAL FAILURE SET CONSTRUCTION

The construction of the physical fault set is based on sequential faults of grid nodes. A fault isolation strategy is developed according to the location of the fault node. As shown in Figure 2, the fault is located on node 3, and the secondary equipment located on nodes 1, 2, 4, and 5 detects the fault information, uploads the data to the information network, and sends an instruction to disconnect the switches of these 4 lines to isolate the fault. In this manner, the physical expected failure set F is established.

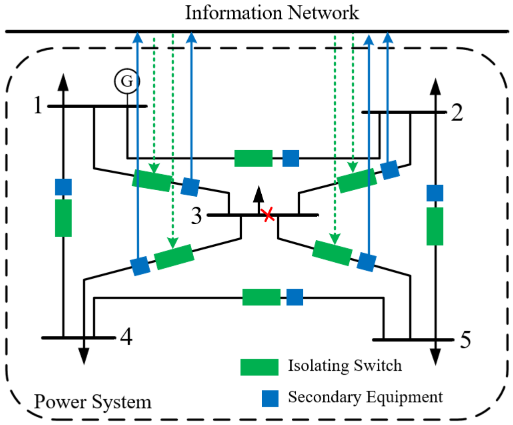

FIGURE 2. Physical fault isolation strategy.

$$F = \left(f_{p1}\ f_{p2}\ f_{p3} \cdots f_{pm}\right), \tag{8}$$

where f_{pi} represents physical node i failure.

B. INFORMATION FAILURE SET CONSTRUCTION

1) FIRST SCREENING

When the information network is too complex, the use of enumeration to traverse all communication paths and record all the nodes in them is very time consuming. Therefore, based on the topological characteristics of information nodes and the electrical characteristics of coupled physical nodes, a calculation formula for the intial screening of information nodes is proposed.

First, based on the CPPS adjacency matrix model of distribution network, the information side takes the link utilization as the weight, and the physical side takes the transmission line impedance as the weight. The importance of the physical node $I_P(v_i)'$ is

$$I_P(v_i)' = 1 - \alpha(G_p)/\alpha(G_p') \tag{9}$$

where $\alpha(G_p)$ represents the condensation degree of physical network, and $\alpha(G_p')$ represents the condensation degree after node shrinkage [21]. $I_P(v_i)$ is obtained by normalization:

$$I_P(v_i) = \frac{I_P(v_i)' - I_P(v_i)'_{min}}{I_P(v_i)'_{max} - I_P(v_i)'_{min}} \tag{10}$$

where v_i represents the nodes in the network. Similarly, the normalized importance degree of information network nodes $I_c(v_i)$ can be obtained. Second, according to the interdependence relationship between information and physical networks, the dependency adjacency matrix F_{P-c} is constructed to represent the influence of communication on power grid. Based on the dependence theory, the node importance degree of power communication network $I(v_i)$ is

$$I(v_i) = I_c(v_i) + I_P(v_i)\sum_{j=1}^{n} F_{P-c}(v_i, u_j), \tag{11}$$

where u_j represents the dependent edge of communication node i.

At the same time, the rationality of the scheme in this paper is verified by the supplementary comparison scheme of the PE index. The PE index is used to find key nodes based on the node removal method [22]. The formula of the importance index PE is:

$$PE = C_o(dE(i) + dP(i)), \tag{12}$$

where dE and dP represent the change in network efficiency and change in load capacity after removing the communication node i, respectively. C_o is the normalization coefficient derived from practical experience, $C_o = 7.74$, $PE \in (0, 1)$.

The relative importance of each node is obtained by passing the values through different node-filtering methods. The information nodes are sorted according to their values from large to small. Furthermore, according to the network scale and user requirements, set C_{attack} of the information nodes to be attacked is determined.

2) INFORMATION FAILURE SET ESTABLISHMENT

After obtaining set C_{attack} with m elements, considering that n nodes are attacked at the same time, there are l combinations, and the calculation formula is as follows:

$$l = \frac{n!}{(n-m)! \times m!} \times 2^n. \tag{13}$$

The network state matrix is recorded after each combined attack, and the node state for each attack is recorded according to the values 0, 1, 2, and 3 in matrix Z. An FDI attack on node j is denoted as F_j, and a DoS attack on node k is denoted as D_k. The information failure set is denoted as

$$C_s(i) = \sum_{j,k \in C_{attack}} \left(F_j + D_k\right), \tag{14}$$

where $C_s(i)$ represents an information attack combination.

C. CONSTRUCTION OF THE COMBINED FAULT SET

In this paper, the complexity of the information network is considered relatively high, and the average degree of each node is greater than 2; that is, a node is connected to at least two edges so that disconnecting one of the edges will not affect the upload and delivery process. According to reference [13], the depth-first traversal algorithm shows that all paths between any two nodes will traverse all nodes; that is, the information fault combined with each physical fault covers all the nodes in the information network. Clearly, the scale of this fault set is very large, and it is of little significance.

The information fault is combined with the physical fault to obtain the combined fault, and it is stored in the collection $H(i)$:

$$H(i) = f_{pi} + C_s(i), \tag{15}$$

where $H(i)$ represents a cyber-physical combined failure. A flow chart for establishing the combined fault set is given in Algorithm 1.

Algorithm 1 Combined Fault Set Establishment Process

```
Input: $V_p$: the set of grid nodes; $C_s$: the expected attack
    combination;
Output: $H$: the information-physical combination fault set;
  Traverse all nodes in $V_p$ in order;
  Number the nodes according to the location of the grid
    fault, recorded as $f_{pi}$;
  Generate an information-physical combination failure as
    $f_{pi} + F_i + D_j$;
  All elements in collection $C_s$ are traversed;
  Store the combined failures in collection $H(i)$;
  Node traversal in set $V_p$ is complete;
  Return $H$.
```

D. ESTABLISHING THE PHYSICAL NETWORK DAMAGE MECHANISM

1) DOS AND FDI ATTACK MECHANISMS

Under a DoS attack, the communication device denies service, which leads to a change in the transmission path of the system status information from the physical side, and thus affects the data transfer time. This leads to the considerable and controllable performance degradation of the dispatch center. Accordingly, the DoS attack mechanism considered in this paper is as follows. The attacked communication node is permanently invalid, causing the communication path of some nodes to change. The information delay rate is calculated according to the new and original paths. The calculation formula of the delay rate is expressed as

$$DE_i = (Path_{new} - Path_{origin})/Path_{origin}, \tag{16}$$

When the delay rate exceeds the threshold of 0.6, the circuit breakers of adjacent lines cannot isolate the fault in time, resulting in physical fault propagation. If the system does not have new communication paths, physical failures will proliferate.

Under an FDI attack, the communication node uploads false data, and the default false data range is within the trusted data range of the dispatch center. Therefore, the dispatch center will change the power generation output, which will cause the line to be overloaded and expand the fault. Accordingly, the FDI attack mechanism of this paper is as follows: The attacked communication node only causes the failure scope of the physically faulty node to propagate to the neighbor nodes and does not hinder other data transmissions.

Under the simultaneous DoS and FDI attacks, the communication equipment will not be able to transmit normal data and will transmit false data at the same time. If this information is trusted by the dispatch center and the dispatch command is issued accordingly, the physical failure that has already occurred will expand. Accordingly, the simultaneous DoS attack and FDI attack mechanism in this paper is as follows: the attacked communication node is permanently disabled, and the failure of the original physical node is propagated to adjacent nodes. Different from simply superimposing the faults caused by separate FDI and DOS attacks, in the subsequent process, whenever the shortest path for the transmission of new physical fault isolation information includes this communication device, the probability of physical fault expansion is 100%.

2) FAULT SCOPE EXPANSION MECHANISM

Figure 2 shows that the physical fault isolation strategy is divided into two stages, fault information upload and instruction issuance, and in this process, the transmission path of the information flow is considered the shortest path. Selecting an element in $H(i)$, the physical fault is f_{pi}, and the information fault is $C_s(i)$. Based on the fault isolation process of f_{pi}, its neighboring nodes monitor the fault information, upload it to the control center, and wait for the instruction to disconnect the switch to isolate the fault. The node set of the shortest path for uploading physical fault information and issuing instructions to the isolation switch is J. If $(i, j) \in C_s(i) \cap J \neq \varnothing$, it indicates that the uploading and issuing process is hindered, and the uploading or issuing process fails.

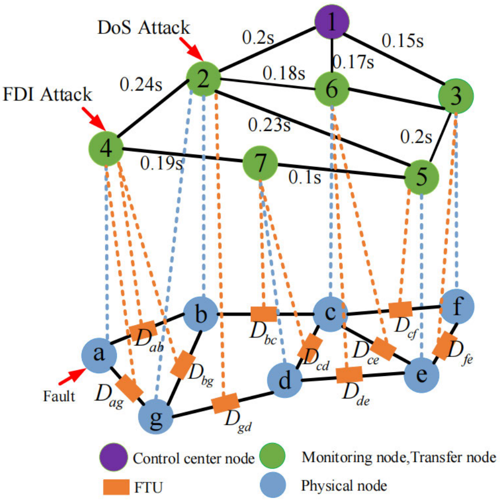

FIGURE 3. Physical failure propagation process.

For example, in the CPPS model of the distribution network shown in Figure 3, the combined fault is set to $f_{p1} + F_4 + D_2$; that is, the physical node is faulty, and information nodes 4 and 2 are subjected to FDI and DoS attacks. According to the damage mechanism of the physical network, the failure propagation process is as shown in Table 1, and a fault isolation strategy can be developed. Specifically, b and g are determined to be faulty after detecting the fault information and uploading it to the control center, and a disconnection instruction is issued to D_{ab} and D_{ag}; the shortest transmission paths in the upload and delivery process include nodes 2 and 4. Since the DoS attack acts on the No. 2 node and there is no other path through for uploading the fault, the information transmission is blocked, resulting in the refusal of the isolation switch, and the fault range is expanded to b and g. Since the FDI attack acts on node 4, the physical fault is directly propagated to b, g.

In the subsequent process of physical fault diffusion, whenever the shortest path for information transmission passes through node 2, it is necessary to determine whether there are other paths to the dispatch center. If there are no other paths, it is necessary to determine the information delay rate. If the delay rate exceeds the threshold, the physical isolation of the fault fails, and the failure expands further. Whenever the shortest path of information transmission passes through node 4, it can still communicate with the dispatch center normally. After spreading twice, the fault is removed, and nodes a, b, g and d are finally removed.

TABLE 1. Combined fault set establishment process.

Times	Quantity	FTU nodes	Forward	Backward
0	a	D_{ab}, D_{ag}	b-2-1,g-2-1	1-2-4-D_{ab},1-2-4-D_{ag}
1	a b g	D_{bc}, D_{gd}	c-6-1,d-7-5-3-1	1-2-D_{gd},1-3-5-7-D_{bc}
2	a b g d	D_{cd}, D_{de}	c-6-1,e-5-3-1	1-6-D_{de},1-3-5-7-D_{cd}

3) SAFETY EVALUATION METRICS

To comprehensively evaluate the damage degree of the distribution network, based on the electrical and topological characteristics, safety is evaluated from two perspectives: the degree of system loss and the connectivity of the power grid, which include the degree of system loss P_{lost}, the degree of expansion of the fault area P_{area} and the power grid connectivity E_{power}.

$$P_{lost} = \frac{H(m)(\sum_{i \in \omega} p_i + s_i)}{\sum_{j \in V_p}(p_j + s_j)}, \tag{17}$$

where ω represents the set of all faulty nodes; V_p is the set of power network nodes; p_i, p_j represent the power of physical nodes i, j; s_i, s_j represent the power generation of physical nodes i, j; and $H(m)$ represents the type of combined fault.

Moreover, the degree of loss in nonfaulty areas is proposed. The impact of combined faults on the nonfaulty areas of the physical network is analyzed, and the power grid is quantitatively evaluated. $P_{lost}(m)$ is defined as the system loss degree for the combined fault m, and $P_{lost}(i)$ is the loss degree for the original fault i.

$$P_{area} = \frac{P_{lost}(m) - P_{lost}(i)}{\sum_{j \in V_p}(p_j + s_j)}. \tag{18}$$

The damage degree of the physical network is analyzed from the topological structure, and the initial connectivity of the power network is defined as $E_{conn}(N)$. After the attack process is completed, the network connectivity is $E_{conn}(N-\omega)$, and the calculation formula is expressed as

$$E_{power} = \frac{E_{conn}(N) - E_{conn}(N-\omega)}{E_{conn}(N)}, \tag{19}$$

the specific formula of $E_{conn}\,(N)$ is expressed as

$$E_{conn}\,(N) = \frac{1}{N\,(N-1)} \sum_{i\in U,k\in W} \frac{1}{d_{ik}}, \tag{20}$$

where N is the number of power nodes, d_{ik} is the shortest path from power node i to power generation node k, W is the power generation node set of power nodes, and U is the power node set.

IV. EXAMPLE ANALYSIS

A. SCENE CONSTRUCTION

According to the typical binary heterogeneous structure of *CPPS* and the scale-free characteristics of the information space, this paper selects the following model to analyze and verify the method: for the physical side and the information side, the standard IEEE-118 node power network data and the scale-free network based on the complex network are used respectively, and the *CPPS* dependent network model is established by one-to-one coupling through the adjacency matrix. The three information nodes with the highest degree are selected to be connected to the three dispatch centers,and a power grid correlation matrix H_P, information network correlation matrix H_c and dependency matrix D are generated. Finally, a three-layer distributed cyber-physical power system represented by the hybrid matrix A is formed, as shown in Figure 4.

B. SIMULATION DESIGN

The priority of the information streams uploaded to the control center nodes is defined to be the same; that is, the 3 control center nodes analyze the information flow, and when 2 or more of them receive the same information flow, the information is "true", whereas it is "false" otherwise. To verify the rationality of the information combination fault screening mechanism, this article also uses the traditional betweenness sorting algorithm to filter the information nodes to be attacked, and the node betweenness is defined as the ratio of the number of shortest paths through a node to the total number of all shortest paths in the network. It usually indicates the importance and influence of the node in the entire network. Table 2 presents the results of the betweenness sorting algorithm, node deletion algorithm and the algorithm in this paper as well as the data for the first 10 nodes.

According to Table 2, there are differences in the three sorting results. The reason is that the betweenness sorting algorithm starts from the topological structure of the information network. Compared with the betweenness sorting method, the node deletion method considers the change in the active power of the power grid and the change in the network efficiency of the entire network after the deletion of the information node. This algorithm considers the electrical parameters to a certain extent but ignores the heterogeneity of the complex network. The difference is that the algorithm in this paper starts from the *CPPS* interdependence theory, combines the network topology parameters and electrical distribution parameters, and uses the coupling characteristics between networks, which can better reflect the impact of the physical domain on the information domain.

TABLE 2. Sorting results of the three algorithms.

No.	Node	$I(v_i)$	Node	Betweenness	Node	PE
1	49	0.637	8	0.209	110	1
2	80	0.590	9	0.126	19	0.963
3	69	0.572	10	0.095	116	0.929
4	54	0.545	27	0.081	68	0.912
5	59	0.533	2	0.077	90	0.819
6	56	0.522	22	0.076	80	0.739
7	66	0.448	25	0.072	112	0.705
8	34	0.403	49	0.071	86	0.665
9	89	0.401	1	0.071	3	0.663
10	19	0.385	20	0.067	107	0.661

The fault screening and evaluation of combined faults is mainly based on the characteristics of the physical network, so the screening algorithm in this paper takes the influence of the physical domain into greater consideration. There are control center nodes in the screening results, but this article does not consider the situation of the control center being attacked, thus, the control center nodes are replaced in the results. Below, the specific manifestations of the differences between the two screening algorithms are explored, the screening results are simulated and analyzed, and the impact on the physical network topology and electrical characteristics is studied.

C. SIMULATION ANALYSIS

After constructing the cyber-physical combined fault set, based on the impact of the combined faults on the electrical characteristics and topological structure of the power grid, the six combined faults with the greatest threat are screened out. The degree of system loss obtained by the three algorithms is shown in Figure 5, and the fault combination is shown in Table 3.

Figure 5 shows that most of the physical nodes coupled with the information nodes obtained by the algorithm in this paper are the key nodes of the physical network, including hub nodes, heavy load nodes, and large generator set nodes. When a coordinated information attack occurs, the coupled physical node directly fails, its adjacent line switch refuses to operate, and the scope of the fault expands. The traditional betweenness sorting method considers only the topological importance of nodes and ignores the topological importance and electrical characteristics of coupled physical nodes. Therefore, the evaluation results do not reflect the most severely damaging combination fault. Additionally, the PE algorithm does not fully consider the characteristics of the interdependent network, so the resulting

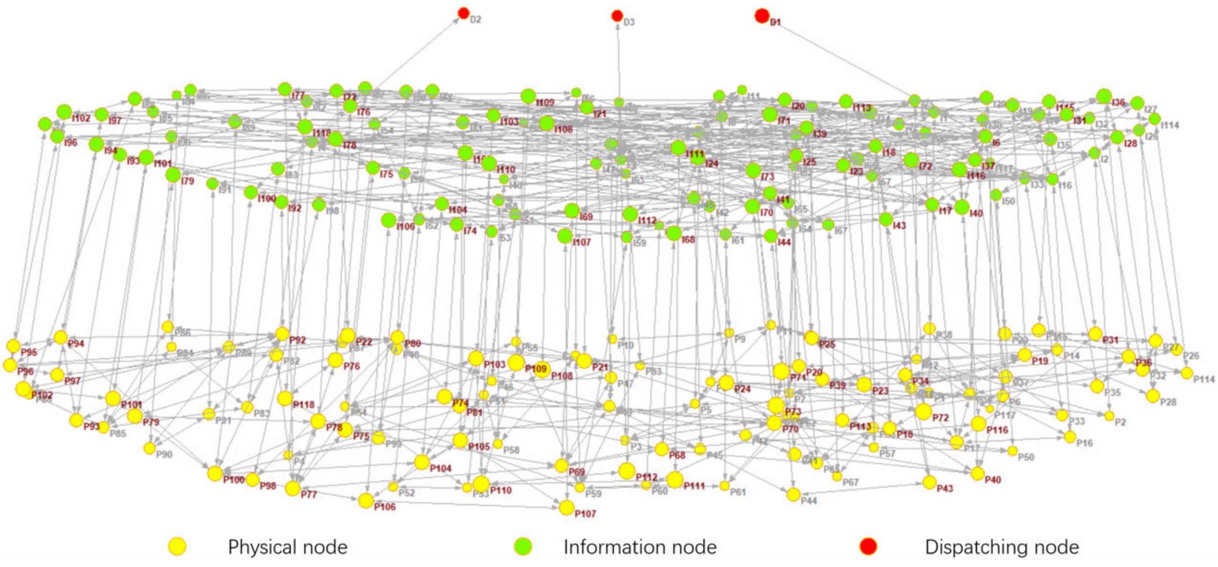

FIGURE 4. CPPS network structure schematic.

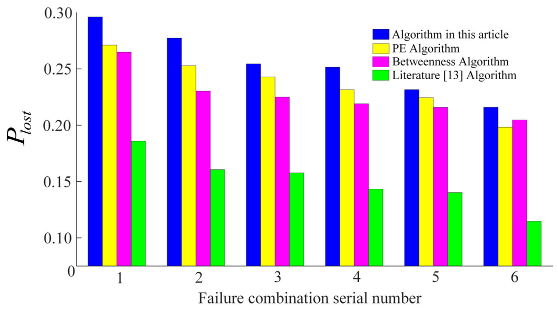

FIGURE 5. System loss degree.

information-physical combination failure is not the most serious. The evaluation algorithm in reference [13] considers only the failure of a single information node. When the information network is sufficiently complex, the failure of a single information node will not seriously affect the operation of the system. According to Table 3, physical faults are nodes with high power generation and heavy loads, while information faults are information nodes directly coupled to them, and the evaluation results are not of high reference value.

The analysis of the influence of different screening mechanisms on the propagation of physical faults is shown in Figure 6 and Table 4, considering the relationship between the original physical fault load and the physical load that must be lost, and the figure shows that the combined faults obtained by the screening algorithm in this paper have a greater impact on the nonfaulty area. This is because the other three algorithms implement a single idea of information fault screening and do not consider the overall nature of the *CPPS*. It can also be seen from the figure that the betweenness algorithm considering the network structure is not always less influential than the PE algorithm considering the network efficiency and electrical parameters. At the same time, the result of the betweenness sorting algorithm is different from that of reference [13]. Although the betweenness sorting algorithm considers that two nodes are attacked, the impact of certain combinations is not as great as the failure of a single information node. Because the algorithm in reference [13] uses deep traversal, the most impactful combination can be found according to different evaluation indicators, while the betweenness sorting algorithm considers only the topological characteristics of the information network, which is more limited. The algorithm in this paper considers three network characteristics simultaneously, so it has better accuracy than the other two algorithms.

TABLE 3. Analysis of failure combinations for the system loss degree.

No.	The algorithm of this article		PE algorithm	
1	fp54 + D59 + F49	0.2994	fp49 + D37 + F49	0.2704
2	fp56 + D54 + F49	0.2811	fp77 + D3 + F3	0.2540
3	fp59 + D56 + F49	0.2582	fp54 + D22 + F54	0.2419
4	fp49 + D59 + F54	0.2561	fp59 + D19 + F19	0.2324
5	fp32 + D56 + F59	0.2350	fp98 + D3 + F3	0.2243
6	fp59 + D68 + F69	0.2172	fp80 + D20 + F6	0.2150
	Betweenness algorithm		Reference [13] algorithm	
1	fp22 + D27 + F27	0.2651	fp10 + D10	0.1856
2	fp6 + D25 + F25	0.2529	fp89 + D89	0.1618
3	fp11 + D11 + F22	0.2238	fp80 + D80	0.1579
4	fp12 + D69 + F80	0.2187	fp65 + D65	0.1442
5	fp5 + D49 + F21	0.2149	fp66 + D66	0.1418
6	fp53 + D34 + F49	0.1911	fp90 + D90	0.2041

To study the impact of information-physical combined faults on the topology of the physical network, the connectivity impact diagram and combined fault set are given, as shown

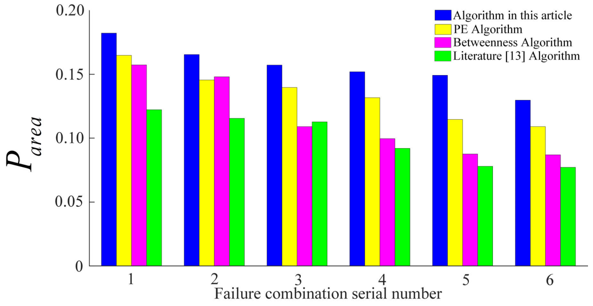

FIGURE 6. Loss in the nonfaulty area.

TABLE 4. Analysis of the spread of the physical failure range.

No.	The algorithm of this article		PE algorithm	
1	fp49 + D62 + F49	0.1986	fp54 + D49 + F49	0.1633
2	fp54 + D49 + F56	0.1739	fp56 + D2 + F11	0.1473
3	p49 + D27 + F49	0.1628	fp55 + D37 + F17	0.1434
4	fp56 + D21 + F56	0.1626	fp54 + D6 + F6	0.1318
5	fp59 + D32 + F26	0.1596	fp49 + D22 + F6	0.1179
6	fp80 + D89 + F80	0.1424	fp77 + D23 + F3	0.1137
	Betweenness algorithm		Reference [13] algorithm	
1	fp6 + D5 + F5	0.1540	fp6 + D6	0.1218
2	fp54 + D49 + F49	0.1496	fp80 + D80	0.1204
3	fp21 + D22 + F20	0.1103	fp89 + D89	0.1146
4	fp49 + D80 + F49	0.1049	fp49 + D49	0.9454
5	fp12 + D69 + F80	0.0920	fp22 + D22	0.0744
6	fp11 + D11 + F11	0.0906	fp110 + D110	0.0712

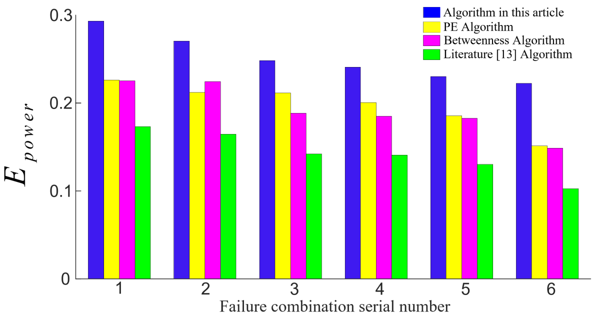

FIGURE 7. Connectivity impact.

TABLE 5. Combined fault connectivity analysis.

No.	The algorithm of this article		PE algorithm	
1	fp49 + D59 + F49	0.2925	fp87 + D37 + F2	0.2306
2	fp80 + D69 + F77	0.2726	fp111 + D22 + F22	0.2148
3	fp49 + D32 + F34	0.2485	fp112 + D2 + F22	0.2143
4	fp12 + D66 + F49	0.2394	fp10 + D37 + F19	0.2001
5	fp59 + D49 + F56	0.2288	fp109 + D37 + F17	0.1847
6	fp77 + D92 + F80	0.2203	fp109 + D35 + F59	0.1501
	Betweenness algorithm		Reference [13] algorithm	
1	fp11 + D11 + F12	0.2302	fp11 + D11	0.1768
2	fp54 + D69 + F49	0.2291	Fp92 + D92	0.1685
3	fp32 + D32 + F46	0.1899	fp80 + D80	0.1420
4	fp49 + D80 + F49	0.1846	fp49 + D49	0.1413
5	fp100 + D49 + F81	0.1819	fp59 + D59	0.1304
6	fp70 + D69 + F80	0.1488	fp77 + D77	0.1018

in Figure 7 and Table 5. The histogram shows that the combined faults selected by the algorithm in this paper have a greater impact on the topology of the power system than those selected by the other two algorithms. This is because the topology of the physical network is considered when constructing the set of information nodes to be attacked. The larger the set is, the worse the connectivity of the network, and the higher the topological importance of disconnected physical nodes. The combined fault set based on the betweenness sorting method considers only the topological importance of information nodes unilaterally and ignores the topology of the physical network, so the combined faults with the greatest impact are not obtained. Based on the PE sorting algorithm, because the PE parameters include the influence of deleting information nodes on the performance of the entire network, the combined faults screened out from this are better than those obtained from the betweenness sorting algorithm. However, the PE algorithm simply adds the network efficiency and electrical load parameters after weighting, which does not fully reflect the coupling characteristics between the two networks. Therefore, compared with the algorithm in this paper, the impact on the network efficiency changes is small. Reference [13] did not consider the topological structure or electrical characteristics. By traversing all information and physical nodes, a combined failure set is obtained. The combined faults selected by this method are the nodes with a larger node degree in the power grid and the information nodes coupled with them, and for a complex CPPS, the failure of a single physical node and information node will not have a major impact on the system topology.

Comparisons of Table 3, 4 and 5 show that when the evaluation objects are different, the combined fault sets obtained by the screening algorithm in this paper are basically the same, whereas those obtained by the betweenness sorting algorithm and the algorithm in reference [13] are completely different, which demonstrates that the algorithm in this paper can maintain high applicability when the evaluation index varies.

V. CONCLUSION

In this paper, a safety evaluation model for a CPPS is constructed through an expected failure analysis method, and the impact of multi-information physical failures on the CPPS is clarified. Compared with the traditional betweenness method and the classic node deletion method, the effectiveness of the method proposed in this paper for screening information fault nodes is demonstrated. Moreover, we found that compared with the single information physical fault analysis method, the multi-information physical fault will cause multiple damages to the system, which can better reflect the situation of the actual power system. In the future, supplementing new fault scenarios, specifying power flow and information flow models, and optimizing information node screening methods will help to achieve more accurate CPPS safety assessments.

REFERENCES

[1] M. Abdelmalak, V. Venkataramanan, and R. Macwan, ‘‘A survey of cyber-physical power system modeling methods for future energy systems,’’ *IEEE Access*, vol. 10, pp. 99875–99896, 2022.

[2] Y. Han, Z. Li, C. Guo, and Y. Tang, ‘‘Improved percolation theory incorporating power flow analysis to model cascading failures in cyber-physical power system,’’ in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[3] G. Wu, M. Li, and Z. S. Li, ‘‘Resilience-based optimal recovery strategy for cyber–physical power systems considering component multistate failures,’’ *IEEE Trans. Rel.*, vol. 70, no. 4, pp. 1510–1524, Dec. 2021.

[4] R. Zhou, M. Peng, and X. Gao, ‘‘Vulnerability assessment of power cyber-physical system considering nodes load capacity,’’ in *Proc. 6th Int. Conf. Intell. Comput. Signal Process. (ICSP)*, Apr. 2021, pp. 1438–1441.

[5] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, ‘‘Analyzing the cyber-physical impact of cyber events on the power grid,’’ *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[6] IEA-ETSAP and IRENA, ‘‘Renewable energy integration in power grids,’’ Technol. Brief, Abu Dhabi, United Arab Emirates, Apr. 2015.

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

[8] Q. Zhao, X. Qi, M. Hua, J. Liu, and H. Tian, ‘‘Review of the recent blackouts and the enlightenment,’’ in *Proc. Berlin Workshop (CIRED)*, 2020, pp. 312–314.

[9] C. Long, Y. Teng, Z. Jiang, J. Wu, P. Zhang, and S. Jing, ‘‘A method of identifying shift switch of expected failure isolation,’’ in *Proc. Int. Conf. Smart Grid Clean Energy Technol. (ICSGCE)*, May 2018, pp. 72–78.

[10] Y. Jia, R. Liu, P. Wang, and X. Han, ‘‘Risk assessment of cascading failures in power grid based on complex network theory,’’ in *Proc. 14th Int. Conf. Control, Autom., Robot. Vis. (ICARCV)*, Nov. 2016, pp. 1–6.

[11] M. Sang, X. Wu, H. Wang, D. Zhou, Z. Wang, Z. Li, and Y. Ding, ‘‘Assessment of power system cascading failure under the background of direct power purchase by large consumers,’’ in *Proc. IEEE Sustain. Power Energy Conf. (iSPEC)*, Nov. 2019, pp. 1417–1422.

[12] S. He, Y. Zhou, Y. Zhou, J. Wu, M. Zheng, and T. Liu, ‘‘Fast identification of vulnerable set for cascading failure analysis in power grid,’’ *IEEE Trans. Ind. Informat.*, early access, Aug. 30, 2022, doi: 10.1109/TII.2022.3202917.

[13] X. Zhou, Z. Yang, M. Ni, H. Lin, M. Li, and Y. Tang, ‘‘Analysis of the impact of combined information-physical-failure on distribution network CPS,’’ *IEEE Access*, vol. 8, pp. 44140–44152, 2020.

[14] X. Gao, M. Peng, R. Zhou, and Y. Deng, ‘‘Cascading failure analysis with load uncertainty in cyber-physical power systems,’’ in *Proc. Int. Conf. Power Syst. Technol. (POWERCON)*, Dec. 2021, pp. 1817–1821.

[15] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, ‘‘A framework for cyber-topology attacks: Line-switching and new attack scenarios,’’ *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1704–1712, Mar. 2019.

[16] R. Fu, X. Huang, Y. Xue, Y. Wu, Y. Tang, and D. Yue, ‘‘Security assessment for cyber physical distribution power system under intrusion attacks,’’ *IEEE Access*, vol. 7, pp. 75615–75628, 2019.

[17] K. S. Xiahou, Y. Liu, and Q. H. Wu, ‘‘Robust load frequency control of power systems against random time-delay attacks,’’ *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 909–911, Jan. 2021.

[18] Z. Wang, L. Li, H. Sun, C. Zhu, and X. Xu, ‘‘Dynamic output feedback control of cyber-physical systems under DoS attacks,’’ *IEEE Access*, vol. 7, pp. 181032–181040, 2019.

[19] R. Lai, X. Qiu, and J. Wu, ‘‘Robustness of asymmetric cyber-physical power systems against cyber attacks,’’ *IEEE Access*, vol. 7, pp. 61342–61352, 2019.

[20] B. Chen, Z. Yang, Y. Zhang, Y. Chen, and J. Zhao, ‘‘Risk assessment of cyber attacks on power grids considering the characteristics of attack behaviors,’’ *IEEE Access*, vol. 8, pp. 148331–148344, 2020.

[21] Y. J. Tan, J. Wu, and H. Z. Deng, ‘‘Evaluation method for node importance based on node contraction in complex networks,’’ (in Chinese), *Syst. Eng. Theory Pract.*, vol. 11, no. 11, pp. 79–83, 2006.

[22] X. Sun, S. Zhao, and Y. Li, ‘‘Weighted power network node importance evaluation based on node deletion method,’’ in *Proc. Int. Conf. Adv. Electr. Equip. Reliable Operation (AEERO)*, Oct. 2021, pp. 1–4.

YAN WANG received the bachelor’s degree in electrical engineering and automation from the Anhui Institute of Information Technology, in 2020. He is currently pursuing the master’s degree with Yunnan Minzu University, Kunming, China. His main research interests include smart grids and cyber-physical power systems.

CHENGCHENG FENG received the bachelor’s degree in automation and electrical engineering from Luoyang Normal University, in 2020. He is currently pursuing the master’s degree with Yunnan Minzu University, Kunming, China. His main research interests include protection and risk analysis of cyber-physical power systems.

YAN LI (Member, IEEE) received the Ph.D. degree in communication and information systems from the Huazhong University of Science and Technology, Wuhan, China, in 2008. She is currently a Professor with the School of Electrical and Information Engineering, Yunnan Minzu University, Kunming, Yunnan, China. She is also the Head of the Key Laboratory of Cyber-Physical Power System of Yunnan Province. Her research interests include wireless networks, smart grids, and communication systems for power systems.

TIANQI XU received the B.S. degree in electrical engineering and automation and the Ph.D. degree in electrical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2000 and 2009, respectively. He was a Postdoctoral Fellow at the Centre for Urban Energy, Ryerson University, Toronto, ON, Canada, from 2011 to 2013. He is currently a Professor with the School of Electrical and Information Engineering, Yunnan Minzu University, Kunming, China. His research interests include smart grids, relay protection, and communication systems for power systems.

MENGMENG ZHU received the B.S. and M.S. degrees from the Kunming University of Science and Technology, in 2010 and 2013, respectively. He is currently working as the Director and a Senior Engineer with the Intelligent Perception Innovation Studio in Power Science Research Institute, Yunnan Power Grid Company Ltd. He has published more than 30 papers in the fields of ac and dc transformer inspection and fault diagnosis technology, fault detection and protection of distribution networks, and power metering device verification. He won the Special Prize of the Yunnan Province Technology Invention, the Third Prize of Yunnan Province Science and Technology progress, and other awards.