IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

SPECIAL SECTION ON VISUAL ANALYSIS FOR CPS DATA

Received January 15, 2020, accepted February 25, 2020, date of publication March 3, 2020, date of current version March 13, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2978113

Analysis of the Impact of Combined Information-Physical-Failure on Distribution Network CPS

XIA ZHOU[1,2], ZHOU YANG[1], MING NI[2], (Senior Member, IEEE), HUSHENG LIN[1], MANLI LI[2], AND YI TANG[3], (Senior Member, IEEE)

[1]Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[2]State Grid Electric Power Research Institute, NARI Group Corporation, Nanjing 211106, China
[3]School of Electrical Engineering, Southeast University, Nanjing 210096, China

Corresponding author: Zhou Yang (yang_zhou0207@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61833008, in part by the National Key Research and Development Plan under Grant 2017YFB090300, and in part by the Fund and State Key Laboratory Project about Smart Grid Protection and Operation Control under Grant SGNR0000GZJS1808074.

ABSTRACT With the rapid development of ICT technology and automation control technology, the distribution network has gradually transformed into a distribution network cyber-physical system (distribution network CPS) with highly coupled information and physical systems. The information system supports the stable operation of the physical system but also brings about certain security risks to the distribution network CPS. Therefore, information impact should be considered in the original anticipated physical fault assessment. This paper proposes a security analysis and evaluation method for distribution network CPS considering anticipated combined information-physical fault screening. First, based on the CPS structure of the distribution network, a CPS correlation matrix model of the distribution network that can reflect the power-information coupling characteristics is established. Then, we analyze the correlation between information failure and physical failure, and we construct an initial anticipated combined information-physical-fault set according to topology and service correlations. Next, based on the fault recovery rate ordering, the key anticipated combined information-physical fault is selected. Finally, for the selected combination of anticipated failures, an assessment of the distribution network CPS security assessment indicators is carried out and verified via example.

INDEX TERMS Distribution network CPS, association matrix, combined failure, information-physical combination.

I. INTRODUCTION

Given the advancement of smart grid and energy internet strategies, a high degree of coupling of information and physics has become a key feature of smart distribution networks [1]. The addition of information systems improves the operation of the distribution network CPS but also brings certain risks and impacts to the security of the distribution network CPS operation [2]. In severe cases, this can cause chain failures through the information-physical coupling mechanism, causing the whole CPS of the distribution network to become paralyzed, thereby impacting daily life and industry. From March 7 to 27, 2019, two large-scale blackouts occurred in the Venezuelan power grid in succession [3]. Attackers controlled computer equipment, cut off communication equipment and directly destroyed substations using network [4]–[6] and electromagnetic attacks. This caused a long-term large-scale power outage in the urban distribution network, triggered social unrest, and affected the entire country. In the distribution network CPS, the degree of influence of information on the physical system mainly depends on the role of information functions in power grid fault handling and recovery [7]–[9]. When a physical system fails, the simultaneous failure of information affects the fault handling process and deteriorates the system state. For example, after a system failure, the failure of the

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

feeder circuit breaker control function will cause a cascade failure [10].

In the current operating state of the distribution network CPS, if it is greatly disturbed, to quickly analyze and evaluate the security of the distribution network CPS, it is necessary to first establish an anticipated failure set. Anticipated failure analysis [11] is based on the experience and existing knowledge of the operation dispatcher to establish a set of expected failure sets according to various possible failure locations and types of failures and to perform a safety and stability analysis of each of the expected failures in the anticipated failure set. This method is currently widely used in the field of large power grids, and only a failure on the physical side is generally considered. In the field of distribution networks, due to its small scale, there are few studies using the anticipated failure analysis method. However, given the utilization of information systems and new energy systems, the scale of CPS in distribution networks is constantly expanding; thus, it is feasible to adopt the method. Since information physics is highly coupled, the impact on the information side cannot be ignored. It is necessary to consider anticipated combined information-physical faults to anticipate failures.

Research has been performed on distribution network CPS, from initials architecture [12], [13] and modeling [14], [15], to risk assessment [16], and then to the impact analysis of information attacks [16], [17]. These studies have become increasingly thorough; however, there are few studies on the impact of information-physical failures on the CPS security of distribution networks. In the actual operation of distribution network CPS, most safety problems are caused by a failure of internal functions such as the failure of information collection equipment, the refusal or misoperation of secondary equipment control, and the interruption or delay of the transmission of information. The failure of the functions undertaken by these information systems will induce a combined failure when the physical system of the distribution network CPS fails, which will affect the recovery of the distribution network CPS and bring secondary losses to the distribution network CPS.

Given the above background, this paper takes the failure recovery process of the distribution network CPS as the starting point; the indirect impact of information system failure on the physical system is analyzed, the distribution network CPS correlation matrix model reflecting the power-information coupling characteristics is established and based on the $k(N-1+1)$ security analysis criteria of the distribution network, and an information-physical combination anticipated fault set is constructed. The above method can quickly analyze the impact of information- physical-failure on Distribution Network CPS.

II. SECURITY EVALUATION PROCESS

To study the security of distribution network CPS, this paper proposes a method based on the idea of ''model establishment - anticipated fault generation and screening - security evaluation index''.

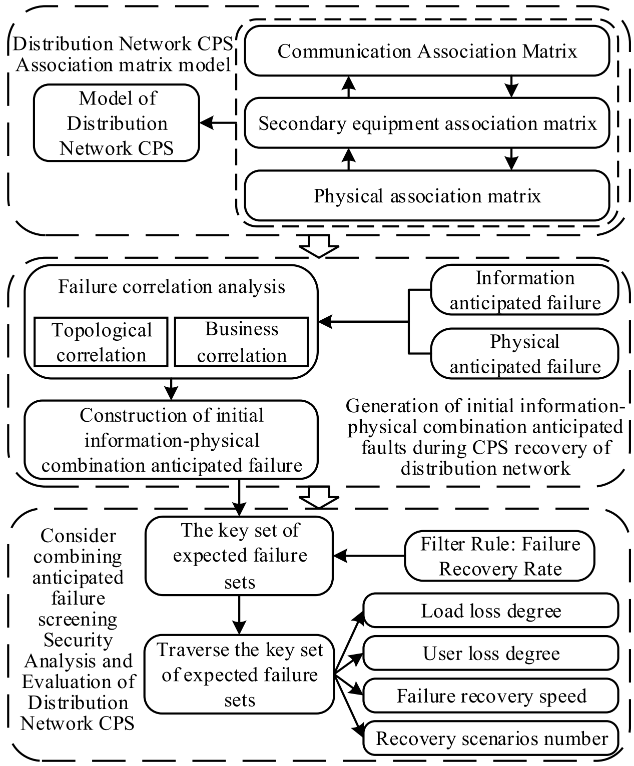

FIGURE 1. Flow chart of security assessment of distribution network CPS.

III. MODELING OF DISTRIBUTION NETWORK CPS

A. STRUCTURE OF DISTRIBUTION NETWORK CPS

The distribution network CPS mainly includes a backbone layer, an access layer and a terminal layer. They correspond to the control decision center, the communication network/secondary equipment network, and the physical network [18]. The backbone layer obtains the distribution network operation and equipment data, processes them, makes decisions, and issues those decisions. The access layer implements real-time communication and control between power distribution terminals and electronic stations. The communication network mainly includes communication equipment and communication protocols. The secondary equipment network mainly refers to the power intelligent control network of the distribution network. The terminal layer includes traditional power primary equipment (such as lines, switches, and loads), distributed power sources (photovoltaics, wind turbines, etc.) and energy storage equipment, as shown in Figure 2.

B. ASSOCIATION MATRIX MODEL OF DISTRIBUTION NETWORK CPS

In this paper, the association matrix model is used to accurately describe the topological association relationship (structure) and logical association relationship (control logic) between the layers.

(1) Physical correlation matrix P. A directed topology matrix is used, and the position relationship of the physical

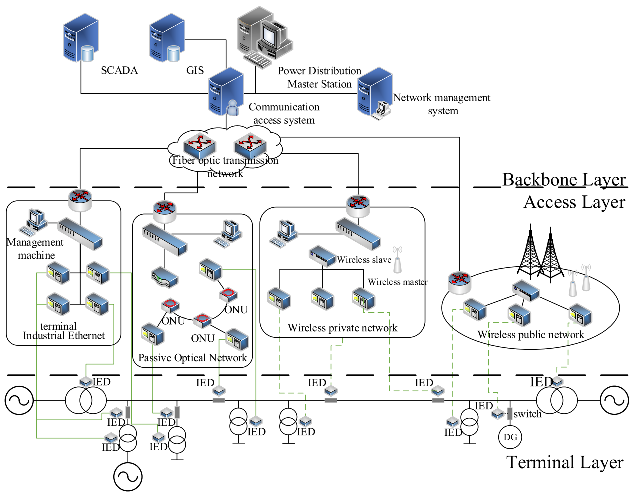

FIGURE 2. Hierarchical structure of distribution network CPS.

nodes in the distribution network topology is represented by two logical elements: "0" and "1".

$$P = \begin{bmatrix} p_{11} & \cdots & p_{1j} & \cdots & p_{1m} \\ \vdots & & & & \vdots \\ p_{i1} & \cdots & p_{ij} & \cdots & p_{im} \\ \vdots & & & & \vdots \\ p_{m1} & \cdots & p_{mj} & \cdots & p_{mm} \end{bmatrix} \tag{1}$$

where p_{ij} is the element in the physical association matrix, which represents the relationship between nodes i and j. $i = j$ represents the physical node itself: $p_{ij} = 1$. If node i is connected to node j and node i is upstream of node j, $p_{ij} = 1$. If node i and node j are not connected, $p_{ij} = 0$.

(2) Communication association matrix C. Similarly, a communication network with n communication nodes is represented by a bidirectional topology matrix $C_{n\times n}$. When $i = j$, c_{ij} means an information node; when $c_{ij} = 0$, it means that there is no connection between nodes; and when $c_{ij} = 1$, it means that there is a connection between nodes.

$$C = \begin{bmatrix} c_{11} & \cdots & c_{1j} & \cdots & c_{1n} \\ \vdots & & & & \vdots \\ c_{i1} & \cdots & c_{ij} & \cdots & c_{in} \\ \vdots & & & & \vdots \\ c_{n1} & \cdots & c_{nj} & \cdots & c_{mn} \end{bmatrix} \tag{2}$$

(3) Secondary equipment association matrix S. For a network with n secondary devices, we build a matrix as follows:

$$S = \begin{bmatrix} s_{11} & \cdots & s_{1j} & \cdots & s_{1k} \\ \vdots & & & & \vdots \\ s_{i1} & \cdots & s_{ij} & \cdots & s_{ik} \\ \vdots & & & & \vdots \\ s_{k1} & \cdots & s_{kj} & \cdots & s_{kk} \end{bmatrix} \tag{3}$$

where s_{ij} represents the nodes and channels of a secondary device network. If $i = j$, s_{ij} represents a secondary device network node; otherwise, s_{ij} represents a secondary device channel. When $s_{ij} = 0$, it means that there is no connection between nodes; when $s_{ij} = 1$, it means that there is a connection between nodes.

(4) The secondary device-physical correlation matrix indicates whether there is an information transfer link between the information node and the physical node.

$$P \leftrightarrow S = \begin{bmatrix} p \leftrightarrow s_{11} & \cdots & p \leftrightarrow s_{1j} & \cdots & p \leftrightarrow s_{1k} \\ \vdots & & \vdots & & \vdots \\ p \leftrightarrow s_{i1} & \cdots & p \leftrightarrow s_{ij} & \cdots & p \leftrightarrow s_{ik} \\ \vdots & & \vdots & & \vdots \\ p \leftrightarrow s_{m1} & \cdots & p \leftrightarrow s_{mj} & \cdots & p \leftrightarrow s_{mk} \end{bmatrix} \tag{4}$$

(5) The secondary device-communication association matrix indicates the association relationship between a secondary device node and a communication node.

$$P \leftrightarrow S = \begin{bmatrix} p \leftrightarrow s_{11} & \cdots & p \leftrightarrow s_{1j} & \cdots & p \leftrightarrow s_{1k} \\ \vdots & & \vdots & & \vdots \\ p \leftrightarrow s_{i1} & \cdots & p \leftrightarrow s_{ij} & \cdots & p \leftrightarrow s_{ik} \\ \vdots & & \vdots & & \vdots \\ p \leftrightarrow s_{m1} & \cdots & p \leftrightarrow s_{mj} & \cdots & p \leftrightarrow s_{mk} \end{bmatrix} \tag{5}$$

IV. ANTICIPATE FAULT SCREENING

A. CORRELATION ANALYSIS OF CYBER PHYSICAL FAILURE

The above modeling process mainly describes the topological association relationship (connection structure) and business association relationship (control logic) between the layers. Therefore, the propagation of faults between information systems and physical systems also has topological and business relevance.

1) TOPOLOGICAL CORRELATION

In the distribution network CPS, the topology represents the connection relationship between information nodes and physical nodes, and faults can be transmitted through the topology. For example, the failure of information collection equipment prevents the status of the physical nodes to be obtained in a timely manner.

2) BUSINESS RELEVANCE

Information systems undertake all types of business-related tasks for physical systems. The occurrence of information failure will affect the execution of power business tasks. After a physical node fails, the information system is responsible for power restoration services and needs to perform fault location and fault isolation operations. If the information node is interrupted, services cannot be delivered.

B. FAILURE RECOVERY ANALYSIS CONSIDERING THE IMPACT OF INFORMATION SYSTEMS

In the distribution network CPS, the degree to which information affects the physical system mainly depends on the role of information functions in power grid fault handling and recovery. Therefore, from the perspective of communication network failure and secondary equipment network failure, this paper considers the impact of information systems on the distribution network CPS failure recovery.

1) IMPACT OF COMMUNICATION NETWORK FAILURE

The communication network performs data transmission services for various service information of the CPS of the distribution network [5], [19]. The optical fiber communication method based on SDH technology has very high reliability. If any single communication link fails, the transmission of power services in the communication network will not be affected. However, when multiple communication links fail simultaneously, the damage to the communication network will be severe.

When the communication network fails, the fault-localization phase is as follows: The failure to transmit fault monitoring information results in losses, and the information system cannot correctly judge the physical system status. Fault isolation stage: The release of isolation instructions or the loss of feedback information will lead to fault isolation errors, and the scope of the fault may expand. Power restoration phase: The loss of power restoration instruction causes transfer failures. These effects will make the fault recovery operation have to enter the manual link, greatly increasing the time for fault recovery.

2) IMPACT OF SECONDARY EQUIPMENT NETWORK FAILURE

The information monitoring equipment obtains real-time and non-real-time operational information of the distribution network and provides data support for various real-time and non-real-time services of the power system [20]. A failure of the information monitoring equipment will not cause a direct change in the physical system topology; however, when other failures occur simultaneously, the dispatcher will no longer correctly judge the state of the physical system of the distribution network, and the operation will be improper, thereby increasing the impact of the failure. During the restoration of the distribution network CPS, after a fault occurs, the distribution control center needs to perform fault identification and fault localization based on the collected fault information. At this time, if the information monitoring equipment fails, accurate information about the affected physical system cannot be obtained. This may cause a failure to locate the fault; in the fault isolation phase, a failure of the information monitoring equipment may cause a failure to obtain information about the isolation switch action, and it would be impossible to determine whether the isolation action is completed. As shown in Figure 3, the actual location of the fault is between nodes 2 and 3. If the upstream fault detection

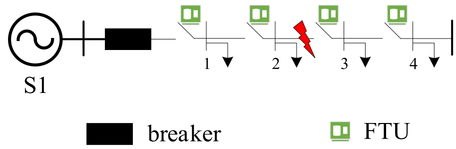

FIGURE 3. Fault state analysis of distribution network CPS.

signal acquisition of the upstream switch node 2 fails in the fault section and the monitoring signal acquisition of node 1 is successful, the fault location will be between nodes 1 and 3. The non-fault sections of nodes 1 and 2 are powered off to expand the scope of the power outages and increase the number of users experiencing a power outage.

The node control equipment completes tasks such as adjusting the operating status of the distribution network and executing emergency control commands based on local information or network information instructions [18]. In the fault recovery process, power supply recovery mainly includes an off-grid mode and a grid-connected mode. The grid connection method is to transfer the load through the contact switch between the feeders to restore the power supply of the non-faulty section. A failure of the node control equipment will cause the contact switch to fail, and it will be necessary to manually operate the contact switch to increase the power outage time of the non-faulty section. The off-grid method can fully utilize the support capabilities of the distributed power in the non-faulty section to form an island. If the distributed power supply's feedback and control fail, it will also cause the island power supply to fail, and users in the island area will lose power.

C. ANTICIPATED FAULT SET GENERATION METHOD

The safety of traditional distribution networks is analyzed using the $k(\mathrm{N}-1+1)$ criterion [21]. After a line fails and is cut off, a switch needs to be closed first to restore power to the load in the non-fault power failure area. In actual operation, this process is not a simple operation but rather a process in which information systems and physical systems participate together. Therefore, when constructing an expected fault set, both information and physical faults need to be considered. From the perspective of distribution network fault recovery, this paper combines information and physical anticipated faults. This method screens out the associated information-physical-combination failure, which greatly reduces the number of unrelated failure.

1) PHYSICALLY ANTICIPATED FAILURE SETS

The physical expected failure is mainly for the disconnection of the line of the topology, and the lines between the physical nodes are disconnected one by one, and the power supply is restored.

2) INFORMATION PREDICTION FAULT SET

Information systems are responsible for various business tasks. The occurrence of information failures may lead to the

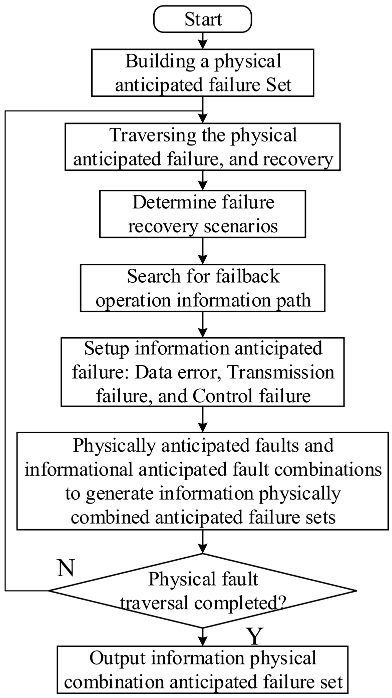

FIGURE 4. Flow chart of anticipated combined information-physical fault.

failure of business task execution, which will affect the safe operation of physical systems [7]. In the model constructed in this paper, the expected faults that may occur during the information transfer process can be divided into three categories: information monitoring device data collection errors, communication network transmission failures (delays and interruptions), and node control device control failures (refusal to move and misoperations).

3) THE COMBINATION OF EXPECTED FAILURES IN INFORMATION PHYSICS

Based on the literature [22], [23], the initial combined information-physical expected fault set is constructed from the perspective of CPS fault recovery of the distribution network, as shown in Figure 4.

Step1: Physically anticipated failures occur one by one.

Step2: Perform recovery operations for physical expected failures and set information for expected failures during the recovery process.

a: DATA COLLECTION ERRORS

The overcurrent fault information matrix uploaded by each physical node F:

$$F = \begin{bmatrix} f_{p_1} & f_{p_2} & \cdots & f_{pi} \end{bmatrix} \tag{6}$$

where f_{pi} represents the overcurrent information on the physical node, in which 1 means that there is current flowing and 0 means that no current is flowing.

According to the fault information matrix F and the physical correlation matrix P, fault localization can be performed, and a fault location matrix D can be generated.

$$D = \begin{bmatrix} d_{p_1} & d_{p_2} & \cdots & d_{p_i} \end{bmatrix} \tag{7}$$

where d_{pi} represents physical fault state information for a node pi, in which 1 indicates a normal physical node and 0 indicates a failure of the physical node.

The data collection error of the information monitoring equipment mainly affects the accuracy of fault localization during the CPS fault recovery process of the distribution network. Therefore, one can set the fault location error matrix by changing the 0/1 value in the fault location matrix.

b: TRANSMISSION FAILURE

During the CPS recovery process of the distribution network, the communication network assumes the two functions of uploading fault information and issuing control instructions. After the physical predicted failure of the distribution network CPS occurs, a path search is used to determine the feasible communication path for uploading the fault information and the control instructions, that is, to determine the communication nodes and communication paths related to the physical predicted failure.

$$L = \varphi(c_{ij}) \tag{8}$$

where c_{ij} represents nodes and links on the communication path; ϕ is a set.

A transmission fault can be set on this communication path. When one or more communication nodes or one or more communication links fails, the nodes or links are removed to determine whether the communication path can transmit normally.

c: CONTROL FAILURE

The secondary equipment (circuit breaker, contact switch, etc.) executes the recovery operation according to the recovery operation instruction issued by the decision analysis layer.

The decision analysis layer formulates a recovery plan based on the received fault information and generates a control instruction matrix H, including a fault isolation instruction matrix H_1 and a power supply restoration instruction matrix H_2.

$$H_1 = \begin{bmatrix} h_{p_1} & h_{p_2} & \cdots & h_{p_i} \end{bmatrix} \tag{9}$$

where h_{pi} represents the instruction operation on the segment switch, expressed as 0/1, in which 1 indicates that the section switch of the physical node i is closed and 0 means that the segment switch of the physical node i is on, that is, the physical node i of the fault zone is isolated.

$$H_2 = \begin{bmatrix} h_{s_1} & h_{s_2} & \cdots & h_{s_i} \end{bmatrix} \tag{10}$$

where s_i represents contact switch and distributed power switch. h_{si} indicates the command operation on the contact switch and distributed power switch, represented by 0/1, where 1 indicates that the switch is closed, and 0 indicates that the switch is open.

The control fault is constructed by the control instruction execution matrix H', including the fault isolation execution matrix H_1' and the power supply recovery execution matrix H_2'. For control instructions, we set the control failure and malfunction.

D. ANTICIPATE FAULT SCREENING

According to the CPS safety of the power distribution network (under the current operation mode of the power distribution network CPS, N devices are expected to fail one by one, and under the premise of ensuring the safe operation of the power grid, we determine whether the non-fault power outage can be fully restored), this paper proposes the failure recovery rate index as a fast screening index for the expected failure set of the information-physical combination. This paper calculates the failure recovery rate and determines the serious combined failure set.

$$\rho_{\mathrm{rec}} = \frac{\sum\limits_{i \in \varphi(M+N)} w_i P_i T(a,b)}{\sum\limits_{i \in \varphi(M+N)} w_i L_i T(a,b)} \times 100\% \tag{11}$$

where P_i is the actual recovered power of node i, L_i is the original power demand of node i, w_i is the hierarchical weight of the node load, $T(a,b)$ is the recovery time after the information failure, a indicates the location of the information failure, and b indicates the type of information failure that caused the failure in the recovery process, representing either data collection errors, transmission failures, or control failures.

E. SAFETY EVALUATION INDEX

According to the needs of the CPS user side of the distribution network, there are industrial areas, commercial areas, and residential areas. More detailed evaluation indicators should be proposed for each area to analyze their security.

(1) The load loss degree is the most important indicator in the security assessment of the power grid.

$$\rho_{\mathrm{load}} = \frac{\sum\limits_{i \in S_m} w_i P_i + \sum\limits_{i \in S_n} w_i P_i}{\sum\limits_{i \in S} w_i P_i} \times 100\% \tag{12}$$

where P_i is the level weight of node i, w_i is the active power load of node i, and M, N, and S are load node sets of the fault zone, non-fault zone and all zones, respectively.

(2) The user loss degree is reflected in the degree of impact on the user after failure, including the proportion of power outages and the proportion of user power losses.

$$\rho_{\mathrm{user}} = (w_1 \frac{X}{Y} + w_2 \frac{\sum\limits_{\mathrm{j} \in X} \mu_{\mathrm{j}}}{\sum\limits_{\mathrm{j} \in Y} \mu_{\mathrm{j}}}) \times 100\% \tag{13}$$

w_1 and w_2 are the weighting factors for the proportion of power outages and the proportion of user power outage losses, respectively; μ_j is the rating factor of user j; and X and Y are the total number of lost users and the total number of users in the system after the failure.

(3) Failure recovery speed. To reduce the load loss and shorten the power outage time for users, the distribution network requires timely power supply recovery for non-faulty sections as well as rapid repairs to the faulty sections after a fault occurs to ensure timely restoration of the entire network.

$$T_{\mathrm{fault}} = T_1 + T_2 + T_3 \tag{14}$$

where T_1, T_2 and T_3 are the fault zone positioning time, fault isolation and non-fault zone recovery time and fault segment repair time, respectively.

(4) Number of failure recovery scenarios.

$$K_{\mathrm{fault}} = k \tag{15}$$

where k is the number of solutions that can be fully recovered after the failure.

V. CASE STUDY

Figures 5 and 6 show the topology of the physical and information sides of the example. The physical side contains 33 load nodes, two contact switches, and a distributed power source. The information side is a 50-node network. For specific parameters, see Appendix Tables 3 and 4.

The anticipated physical failures are mainly the disconnection of the lines, and 32 anticipated physical failures are constructed. For specific anticipated physical failures, see Appendix 5. Information failures are mainly data collection errors, transmission failures, and control failures, including a total of 156 information failures, as shown in Appendix 6, 7 and 8. If they are randomly combined one by one, one obtains 3968 information-physical combinations that are anticipated to fail. However, most of these faults are not correlated and have minimal impact. For each anticipated physical failure, we search for the information nodes involved in the fault recovery process, set the anticipated information failure, and complete the generation of the anticipated combined information-physical failures, including a total of 850 anticipated combined failures, as shown in Appendix 9. The screening of anticipated combined information-physical failures uses the failure recovery rate as the screening rule, and the key anticipated combined information-physical failures are calculated by formula (11) and sorted from small to large, as shown in Table 1.

TABLE 1. Screeening result of key informatin-physical combination anticipated failure.

NO.	Combination failure	Failure recovery rate
1	C1+E37/F35	0.487
2	C2+E37/F35	0.532
3	C1+E38/F36	0.540
4	C2+E38/F36	0.547
5	C3+E37/F35	0.559

Table 1 shows that the faults screened out are mainly the combination of upstream physical node faults and contact switch control faults. Due to the interruption of the communication link connected to the contact switch and the

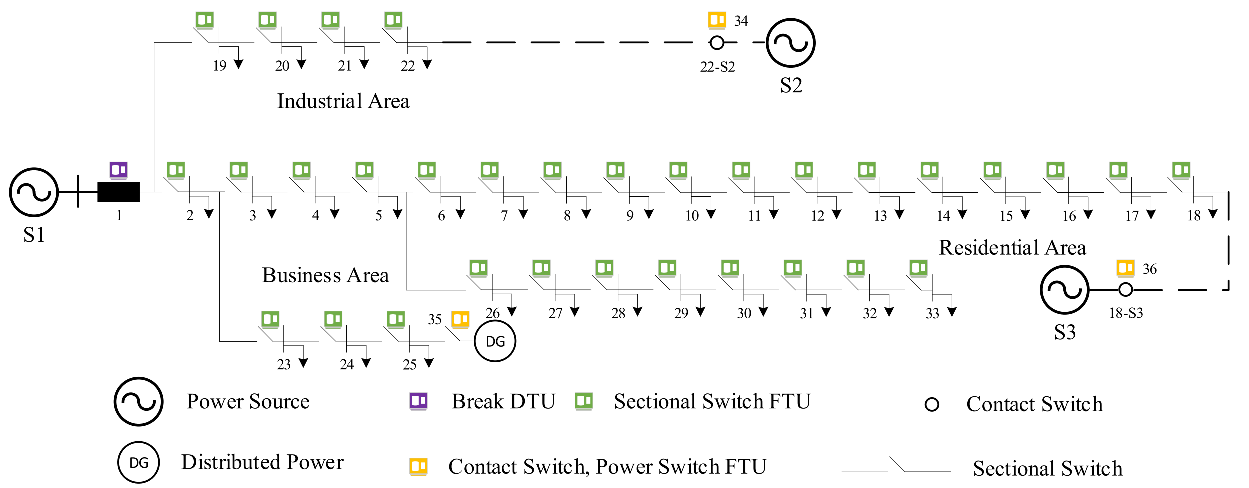

FIGURE 5. Topological structure of the physical side.

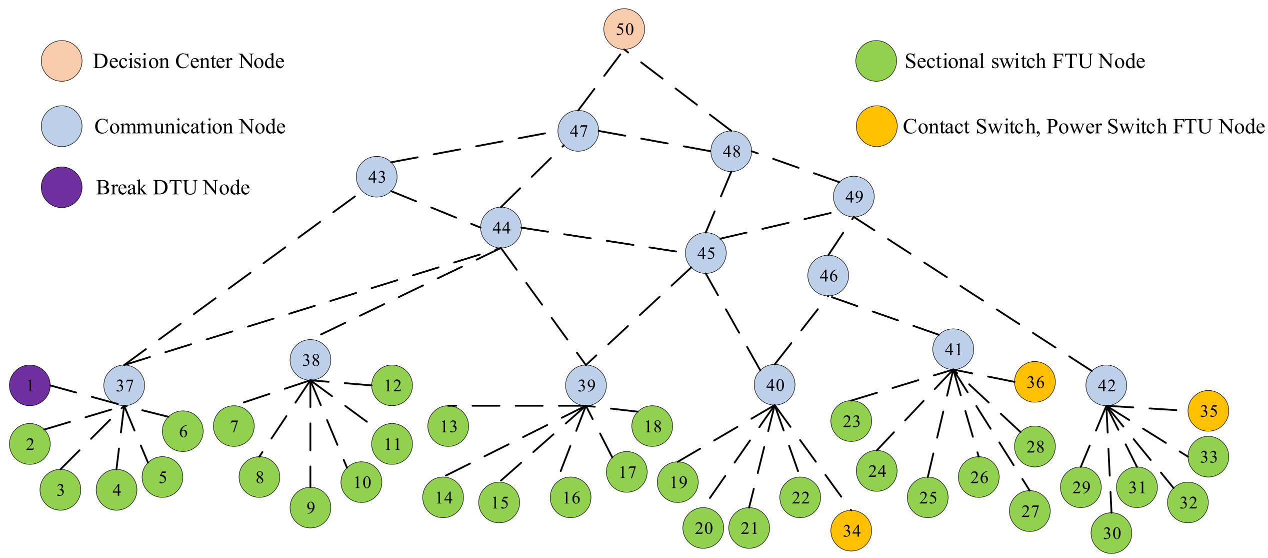

FIGURE 6. Topological structure of the information side.

refusal of the contact switch, power supply recovery cannot be performed in the non-faulty section. These loads will be cut off during the repair of the faulty section, expanding the power outage and increasing the number of users affected. The normal operation of the contact switch is fundamental to ensuring that the non-faulty section can be fully restored; thus, the dispatcher needs to take strict precautions.

For the expected failures of the screened combined information-physical systems, we calculate the safety indicators and analyze the impact on the load side, user side, and fault recovery capabilities.

From Table 2, among the information faults in the screened combinations of anticipated faults, most of them are contact switches that refuse to operate. Because the contact switch refuses to operate, power restoration cannot be performed on the non-faulty section, and the number of recovery plans

TABLE 2. Calculation results of security index.

NO.	Combination failure	ρ_{load}	ρ_{user}	T_{fault}/h	K_{fault}
1	C1+E37/F35	0.575	0.816	1.78	0
2	C2+E37/F35	0.509	0.785	1.66	0
3	C1+E38/F36	0.427	0.202	1.70	0
4	C2+E38/F36	0.425	0.218	1.61	0
5	C3+E37/F35	0.476	0.704	1.70	0
6	C3+E38/F36	0.404	0.546	1.65	0

is zero. Comparing combined faults 1 and 2 and combined faults 3 and 4, the most obvious difference is the degree of user loss, which is due to the different user sides corresponding to the two branches; one side is a residential area, and the other side is an industrial area. Therefore, the combination of faults 1 and 2 has a greater impact on the degree of user loss. In terms of failure recovery speed indicators, due to the refusal of the contact switch, the power recovery of the

TABLE 3. Physical network load data.

Node	Active power /kVA	Reactive power /kVA	Node	Active power /kVA	Reactive power /kVA	Node	Active power /kVA	Reactive power /kVA
1	100	60	12	60	35	23	420	200
2	90	40	13	120	80	24	420	200
3	120	80	14	60	10	25	60	25
4	60	30	15	60	20	26	60	25
5	60	20	16	60	20	27	60	20
6	200	100	17	90	40	28	120	70
7	200	100	18	90	40	29	200	600
8	60	20	19	90	40	30	150	70
9	60	20	20	90	40	31	210	100
10	45	30	21	90	40	32	60	40
11	60	35	22	90	50	33	60	20

TABLE 4. Physical network importance and users number.

Node	Importance	User number	Node	Importance	User number	Node	Importance	User number
1	10	0	12	2	50	23	10	40
2	8	200	13	5	10	24	9	20
3	8	80	14	3	200	25	2	20
4	4	50	15	3	100	26	2	60
5	7	60	16	3	80	27	2	40
6	5	30	17	4	40	28	5	100
7	5	20	18	5	72	29	7	40
8	2	10	19	6	17	30	6	80
9	2	80	20	6	10	31	7	20
10	1	100	21	6	10	32	2	60
11	4	70	22	7	20	33	2	20

TABLE 5. Set of anticipated physical failures.

NO.	Anticipated physical failures	NO.	Anticipated physical failures	NO.	anticipated physical failures	NO.	Anticipated physical failures
C1	1-2	C9	9-10	C17	17-18	C25	5-26
C2	2-3	C10	10-11	C18	1-19	C26	26-27
C3	3-4	C11	11-12	C19	19-20	C27	27-28
C4	4-5	C12	12-13	C20	20-21	C28	28-29
C5	5-6	C13	13-14	C21	21-22	C29	29-30
C6	6-7	C14	14-15	C22	2-23	C30	30-31
C7	7-8	C15	15-16	C23	23-24	C31	31-32
C8	8-9	C16	16-17	C24	24-25	C32	32-33

non-faulty zone must wait until the faulty zone is repaired before power can be supplied. Thus, it has a great impact on the speed of failure recovery.

Among the fault combinations that have not been screened out, the segmented switches that were disconnected due to fault isolation and refused to operate caused the adjacent segmented switches to be opened to ensure the removal of the fault; however, the scope of the power failure was expanded. After a fault occurs, the circuit breaker and the section switch are disconnected to isolate the fault. After the isolation is completed, the circuit breaker fails and cannot accept the closing command to make the circuit breaker refuse to move.

TABLE 6. Set of anticipated information failures(data collection errors).

NO.	Anticipated information failures	NO.	Anticipated information failures	NO.	Anticipated information failures	NO.	Anticipated information failures
D1	1-2→1-3	D9	9-10 →10-11	D17	17-18→16-18	D25	5-26 → 5-27
D2	2-3→2-4	D10	10-11→10-12	D18	1-19 → 1-20	D26	26-27→26-28
D3	3-4→3-5	D11	11-12→11-13	D19	19-20→19-21	D27	27-28→27-29
D4	4-5→4-6	D12	12-13→12-14	D20	20-21→20-22	D28	28-29→28-30
D5	5-6→5-7	D13	13-14→13-15	D21	21-22→20-22	D29	29-30→29-31
D6	6-7→6-8	D14	14-15→14-16	D22	2-23 → 2-24	D30	30-31→30-32
D7	7-8→7-9	D15	15-16→15-17	D23	23-24→23-25	D31	31-32→31-33
D8	8-9→8-10	D16	16-17→16-18	D24	24-25→23-25	D32	32-33→31-33

TABLE 7. Set of anticipated information failures (transmission failures).

NO.	Anticipated information failures	NO.	Anticipated information failures	NO.	Anticipated information failures	NO.	Anticipated information failures
E1	1-37 break	E15	15-39 break	E29	27-42 break	E43	40-46 break
E2	2-37 break	E16	16-39 break	E30	28-42 break	E44	41-46 break
E3	3-37 break	E17	17-39 break	E31	29-42 break	E45	42-49 break
E4	4-37 break	E18	18-39 break	E32	30-42 break	E46	43-44 break
E5	5-37 break	E19	19-40 break	E33	31-42 break	E47	43-47 break
E6	6-37 break	E20	20-40 break	E34	32-42 break	E48	44-45 break
E7	7-38 break	E21	21-40 break	E35	33-42 break	E49	44-47 break
E8	8-38 break	E22	22-40 break	E36	34-42 break	E50	45-48 break
E9	9-38 break	E23	34-40 break	E37	35-42 break	E51	45-49 break
E10	10-38 break	E24	23-41 break	E38	36-41 break	E52	46-49 break
E11	11-38 break	E25	24-41 break	E39	37-44 break	E53	47-48 break
E12	12-38 break	E26	25-41 break	E40	38-44 break	E54	47-50 break
E13	13-39 break	E27	26-41 break	E41	39-45 break	E55	48-49 break
E14	14-39 break	E28	37-43 break	E42	40-45 break	E56	48-50 break

TABLE 8. Set of anticipated information failures (control failures).

NO.	Anticipated information failures	NO.	Anticipated information failures	NO.	Anticipated information failures
F1	Break 1 DTU refuse	F13	Sectional switch 13 FTU	F25	Sectional switch 25 FTU
F2	Sectional switch 2 FTU	F14	Sectional switch 14 FTU	F26	Sectional switch 26 FTU
F3	Sectional switch 3 FTU	F15	Sectional switch 15 FTU	F27	Sectional switch 27 FTU
F4	Sectional switch 4 FTU	F16	Sectional switch 16 FTU	F28	Sectional switch 28 FTU
F5	Sectional switch 5 FTU	F17	Sectional switch 17 FTU	F29	Sectional switch 29 FTU
F6	Sectional switch 6 FTU	F18	Sectional switch 18 FTU	F30	Sectional switch 30 FTU
F7	Sectional switch 7 FTU	F19	Sectional switch 19 FTU	F31	Sectional switch 31 FTU
F8	Sectional switch 8 FTU	F20	Sectional switch 20 FTU	F32	Sectional switch 32 FTU
F9	Sectional switch 9 FTU	F21	Sectional switch 21 FTU	F33	Sectional switch 33 FTU
F10	Sectional switch 10 FTU	F22	Sectional switch 22 FTU	F34	Contact switch 11-S2
F11	Sectional switch 11 FTU	F23	Sectional switch 23 FTU	F35	Contact switch 18-S3
F12	Sectional switch 12 FTU	F24	Sectional switch 24 FTU	F36	Switch of DG

The closing operation is not performed, which leads to the position from the front end of the feeder to the fault point. This causes a loss of power for users.

The interruption of a single information transmission link does not affect the transmission of power services and has little impact on security. An impact will only occur if the

TABLE 9. Set anticipated combined information-physical failures.

C	D	E	F
C1	D1	E1、E2、E38、E39、E41、E42、E43、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F1、F2、F34、F35、F36
C2	D2	E2、E3、E38、E39、E41、E42、E43、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F2、F3、F34、F35、F36
C3	D3	E3、E4、E38、E39、E41、E42、E43、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F3、F4、F34、F35、F36
C4	D4	E4、E5、E38、E39、E41、E42、E43、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F4、F5、F34、F35、F36
C5	D5	E5、E6、E38、E39、E41、E42、E43、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F5、F6、F34、F35、F36
C6	D6	E6、E7、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F6、F7、F34、F35、F36
C7	D7	E7、E8、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F7、F8、F34、F35、F36
C8	D8	E8、E9、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F8、F9、F34、F35、F36
C9	D9	E9、E10、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F9、F10、F34、F35、F36
C10	D10	E10、E11、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F10、F11、F34、F35、F36
C11	D11	E11、E12、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F11、F12、F34、F35、F36
C12	D12	E12、E13、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F12、F13、F34、F35、F36
C13	D13	E13、E14、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F13、F14、F34、F35、F36
C14	D14	E14、E15、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F14、F15、F34、F35、F36
C15	D15	E15、E16、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F15、F16、F34、F35、F36
C16	D16	E16、E17、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F16、F17、F34、F35、F36
C17	D17	E17、E18、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F17、F18、F34、F35、F36
C18	D18	E1、E19、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F1、F19、F34、F35、F36
C19	D19	E19、E20、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F19、F20、F34、F35、F36
C20	D20	E20、E21、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F20、F21、F34、F35、F36
C21	D21	E21、E22、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F21、F22、F34、F35、F36
C22	D22	E2、E24、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F2、F24、F34、F35、F36
C23	D23	E24、E25、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F24、F25、F34、F35、F36
C24	D24	E25、E26、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F25、F26、F34、F35、F36
C25	D25	E5、E27、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F5、F26、F34、F35、F36
C26	D26	E27、E29、E38、E39、E40、E41、E42、E43、E44、E45、	F26、F27、F34、F35、

TABLE 9. ***(Continued.)*** **Set anticipated combined information-physical failures.**

		E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F36
C27	D27	E29、E30、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F27、F28、F34、F35、F36
C28	D28	E30、E31、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F28、F29、F34、F35、F36
C29	D29	E31、E32、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F29、F30、F34、F35、F36
C30	D30	E32、E33、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F30、F31、F34、F35、F36
C31	D31	E33、E34、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F31、F32、F34、F35、F36
C32	D32	E34、E35、E38、E39、E40、E41、E42、E43、E44、E45、E46、E47、E48、E49、E50、E51、E52、E53、E54、E55、E56	F32、F34、F35、F36

TABLE 10. **Failure recovery time T/h.**

anticipated physical failures	recovery time of fault location, fault isolation, non-fault zone	repair time of failure section	anticipated physical failures	recovery time of fault location, fault isolation, non-fault zone	repair time of failure section
C1	0.16	1.62	C17	0.13	1.66
C2	0.13	1.53	C18	0.14	1.49
C3	0.14	1.56	C19	0.11	1.54
C4	0.16	1.55	C20	0.16	1.56
C5	0.12	1.51	C21	0.17	1.55
C6	0.17	1.54	C22	0.18	1.57
C7	0.09	1.56	C23	0.19	1.52
C8	0.12	1.58	C24	0.15	1.51
C9	0.15	1.59	C25	0.10	1.53
C10	0.18	1.51	C26	0.13	1.55
C11	0.19	1.52	C27	0.14	1.48
C12	0.19	1.53	C28	0.16	1.61
C13	0.13	1.55	C29	0.15	1.56
C14	0.12	1.50	C30	0.12	1.53
C15	0.17	1.54	C31	0.17	1.55
C16	0.12	1.52	C32	0.12	1.56

interruption of the information link connected to the secondary device will cause the control instructions to be unacceptable. In terms of data errors, due to the uncertainty of this fault, the data errors in this article only consider expanding the faulty section, which will cause a power failure in a few non-faulty sections and cannot be recovered in time, increasing load and user losses. This has no impact on the speed of failure recovery.

VI. CONCLUSION

The high degree of coupling of information physics makes the security analysis of distribution network CPS focus on the impact of information systems. This paper mainly analyzes the security of distribution network CPS by generating information-physical combinations of anticipated faults and screening, and we draw the following conclusions.

(1) A set of information and anticipated physical faults is constructed, and the two are combined according to the topological correlation and business task correlation to quickly screen out the associated expected information-physical faults, which greatly reduces the number of anticipated combined faults.

(2) We propose the fault recovery rate as a screening rule for the rapid screening of anticipated faults, and we use the load loss degree, user loss degree, fault recovery speed, and number of fault recovery schemes as indicators for the security evaluation of the distribution network CPS. These can be

used to quickly and quantitatively evaluate the distribution network CPS security.

(3) In fault anticipation using the constructed information, it can be found that a single communication link interruption has minimal effect on the fault recovery operation. In addition, controlling the fault (rejection or misoperation) will greatly reduce the safety of the distribution network CPS.

This paper only considers the combination of a single expected information-physical failure. In actual systems, the impact of multiple failures is greater. Therefore, studying the impact of multiple anticipated information-physical failures is our future work. Moreover, for physical failures on the feasible power supply path after fault recovery, physical combinations can be formed to analyze anticipated failures.

APPENDIX

See Tables 3–10.

REFERENCES

[1] M. D. Ilic, L. Xie, and U. A. Khan, "Modeling of future cyber–physical energy systems for distributed sensing and control," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 40, no. 4, pp. 825–838, Jul. 2010.

[2] S. Massoud Amin and B. F. Wollenberg, "Toward a smart grid: Power delivery for the 21st century," *IEEE Power Energy Mag.*, vol. 3, no. 5, pp. 34–41, Sep. 2005.

[3] H. Lin, Z. T. Kalbarczyk, and R. K. Iyer, "RAINCOAT: Randomization of network communication in power grid cyber infrastructure to mislead attackers," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4893–4906, Sep. 2019.

[4] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Yang Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[5] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems-attacks, impacts, and defense: A survey," *IEEE Trans Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[6] M. N. Kurt, Y. Yilmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 2015–2030, Aug. 2018.

[7] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1686–1696, Jul. 2015.

[8] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[9] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[10] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, Mar. 2015.

[11] P. Hines, I. Dobson, and P. Rezaei, "Cascading power outages propagate locally in an influence graph that is not the actual grid topology," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 958–967, Mar. 2017.

[12] E. Handschin, F. C. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power App. Syst.*, vol. 94, no. 2, pp. 329–337, Mar. 1975.

[13] P. Palensky, E. Widl, and A. Elsheikh, "Simulating cyber-physical energy systems: Challenges, tools and methods," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 44, no. 3, pp. 318–326, Mar. 2014.

[14] M. D. Galus, R. A. Waraich, F. Noembrini, K. Steurs, G. Georges, K. Boulouchos, K. W. Axhausen, and G. Andersson, "Integrating power systems, transport systems and vehicle technology for electric mobility impact assessment and efficient control," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 934–949, Jun. 2012.

[15] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sep. 2015.

[16] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability modeling and evaluation of active cyber physical distribution system," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 7096–7108, Nov. 2018.

[17] Q. Dai, L. Shi, and Y. Ni, "Risk assessment for cyberattack in active distribution systems considering the role of feeder automation," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3230–3240, Jul. 2019.

[18] K. Huang, C. Zhou, Y.-C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 8153–8162, Oct. 2018.

[19] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580, Mar. 2017.

[20] T. Facchinetti and M. L. Della Vedova, "Real-time modeling for direct load control in cyber-physical power systems," *IEEE Trans Ind. Informat.*, vol. 7, no. 4, pp. 689–698, Nov. 2011.

[21] L. Thurner, A. Scheidler, F. Schafer, J.-H. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun, "Pandapower—An open-source Python tool for convenient modeling, analysis, and optimization of electric power systems," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6510–6521, Nov. 2018.

[22] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.

[23] A. Zidan and E. F. El-Saadany, "A cooperative multiagent framework for self-healing mechanisms in distribution systems," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1525–1539, Sep. 2012.

XIA ZHOU received the master's and Ph.D. degrees from the Harbin Institute of Technology, Harbin, China, in 2002 and 2017, respectively. She is currently with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. Her main research interests include renewable energy systems and power system planning.

ZHOU YANG is currently pursuing the M.S. degree with the Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include power system operation, and control and power system risk analysis.

MING NI (Senior Member, IEEE) received the B.S. and Ph.D. degrees in electrical engineering from Southeast University, Nanjing, China, in 1991 and 1996, respectively. He is currently the Special Expert with NARI Technology Company Ltd., Nanjing. His current research interests include cyber physical power systems (CPPS), stability analysis, and the control of power systems.

HUSHENG LIN is currently pursuing the M.S. degree with the Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include power system operation, and control and power system risk analysis.

MANLI LI received the B.S. and M.S. degrees from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2012 and 2015, respectively. He is currently an Engineer with NARI Technology Company Ltd., Nanjing. His primary research interests include cyber physical power systems (CPPS), stability analysis, and the control of power systems.

YI TANG (Senior Member, IEEE) received the Ph.D. degree from the Harbin Institute of Technology, Harbin, China, in 2006. He is currently an Associate Professor with Southeast University, Nanjing, China. His research interests include smart grid, power system security, power system stability analysis, renewable energy systems, and cyber physical systems.