IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON KEY ENABLING TECHNOLOGIES FOR PROSUMER ENERGY MANAGEMENT

Received June 1, 2020, accepted June 29, 2020, date of publication July 6, 2020, date of current version July 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007477

Elaborate Reliability Evaluation of Cyber Physical Distribution Systems Considering Fault Location, Isolation and Supply Restoration Process

DAN LIN[1,2], QIANJIN LIU[1,2], (Member, IEEE), ZHUOHUAN LI[1,2], GUANGXUAN ZENG[1,2], ZIYAO WANG[1,2], TAO YU[1,2], (Member, IEEE), AND JUNXIAO ZHANG[3]

[1]School of Electric Power, South China University of Technology, Guangzhou 510640, China
[2]Guangdong Key Laboratory of Clean Energy Technology, South China University of Technology, Guangzhou 510641, China
[3]Grid Planning & Research Center, Guangdong Power Grid Company Ltd., CSG, Guangzhou 510030, China

Corresponding author: Tao Yu (taoyu1@scut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 51777078, and in part by the Technical Projects of China Southern Power Grid under Grant GDKJXM20172942.

ABSTRACT The existing reliability models of the cyber physical distribution systems, which are mostly based on some simplified assumptions, cannot accurately evaluate the reliability of complex cases in practical engineering applications. To solve this problem, an elaborate reliability evaluation method considering the whole process of fault location, isolation and supply restoration is proposed. This paper establishes reliability models of components and the two systems, summarizes the mapping relationship between various cyber system failures and the physical fault handling into several laws, proposes the reliability evaluation procedure in the framework of Monte Carlo method, and verifies the feasibility and effectiveness of the method in an actual distribution network cyber physical system. In the proposed method, the multiple component characteristics, complex topological structure, coupling relationship of the cyber-physical distribution systems, and the actual human-computer joint participation are considered in the analysis of fault location, isolation and supply restoration process, which provides a effective and accurate theory for the application of reliability evaluation in the actual distribution network and prosumer energy management system.

INDEX TERMS Reliability evaluation, cyber physical distribution system, intelligent electronic device, fault location, isolation and supply restoration process.

ABBREVIATIONS

DER	Distributed energy resource
CPDS	Cyber physical distribution system
CPS	Cyber physical system
IED	Intelligent electronic device
FLISR	Fault location, isolation and supply restoration process
CB	Circuit breaker
SS	Section switch
TS	Tie switch
LFI	Local fault indicator
RFI	Remote fault indicator
RMC	Remote monitoring and control
LFI-IED	IED with local fault indicator
RFI-IED	IED with remote fault indicator
RMC-IED	IED with remote monitoring and control
EPON	Ethernet passive optical network
OLT	Optical line terminal
POS	Passive optical splitter
ONU	Optical network unit
DA	Distribution automation
MS	Manual switch
Ass-IED	Associated IED
InS	Incoming switch
OutS	Outgoing switch
RA	Remote area
OA	Onsite area
RPIA	Relay protection isolation area
ARFLA	Actual remote fault location area
CRFLA	Correct remote fault location area
ERFLA	Error remote fault location area
PFIA	Preliminary fault isolation area
AFIA	Actual feeder inspection area

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

CFIA	Correct feeder inspection area
EFIA	Error feeder inspection area
FFLA	Final fault location area
SAIDI	System average interruption duration index
SAIFI	System average interruption frequency index
CAIDI	Customer average interruption duration index
ASAI	Average service availability index
EENS	Expected energy not supplied

I. INTRODUCTION

The access of a large number of renewable distributed energy resources (DERs)[1], [2] makes the distribution network become an multi-energy system [3]. The normal working states of measurement automation system, distribution automation system, distribution dispatching system and other information platforms is a strong guarantee for the monitoring, operation and management of distribution network with the prosumers such as photovoltaics [4], electric vehicles, energy storage and heat pump devices. However, the high dependence of the distribution network on the cyber system makes the physical system inevitably affected by the failures of the cyber system. Therefore, studying the planning, operation and control of the distribution networks from the perspective of cyber physical distribution system (CPDS) [5] have become new hot topics, and reliability evaluation research is one of them. Studying the reliability of CPDS has certain significance for the operation and management of prosumers.

In recent years, many scholars have focused on the reliability analysis method of power grid cyber physical system(CPS). In the early stage of the field, the researches mainly focused on setting up the structure and model of the cyber system, and revealing the coupling relationship between the two systems by discussing the direct and indirect effects of the cyber system on the physical system [6]–[8]. Subsequently, aiming at the direct effects, some scholars established some analytic method frameworks for CPS reliability evaluation on modifying component availability by qualitative or quantitative analysis methods [9]–[11]. At present, many scholars take the specific business function scenarios of the cyber system as the breakthrough points, and refine the reliability model of indirect effect from many aspects. Reference [12] focuses on the performance of information transmission, establishes the reliability model of communication links considering topology, delay and code error, and applies it to the reliability evaluation of active CPDS in simulation method in. In [13], [14], the microgrid is taken as a specific application scenario to establish the CPS reliability analysis methods. Reference [15]–[17] establish the reliability models of cyber system considering cyber attacks in different ways, and incorporate them into the CPS reliability evaluation.

Currently, the research in this field is in the theoretical development stage, and there is still some distance before engineering application. From a theoretical point of view, it is mainly because the following problems in complex scenarios of actual distribution networks have yet to be solved:

1) The reliability models of components and systems are not accurate enough. Intelligent electronic device (IED) has many components [18], such as relay protection module, fault detection module, communication transceiver module, electric control module and independent power module. The simultaneous failure of one or more components may make the IED show multiple working states, and the simple two-state model is not enough to describe the reliability of the IED. Moreover, most of the existing CPDS reliability analysis methods adopt the unified numerical value to quantify the time effect of IED failures on fault location, isolation and supply restoration(FLISR) process, whereas the more accurate method should consider the effect of the fault type of IEDs and the specific relationship between IEDs and physical system fault.

2) The description of the fault handling process in the existing methods deviates from the actual situation. Now, power grid enterprises do not adopt a fully automated approach to fault handling. In order to ensure that the automation platform software makes appropriate decisions on fault handling and avoids erroneous power outages, the task of quickly shielding the fault current is usually handed over to the automation system, while the work of fault location and isolation is realized by human assistance and confirmation of the judgment of the automation system. This way of fault handling helps to reduce the negative impact of cyber system failure. Therefore, the CPDS reliability analysis methods based on the principle of differential analysis for fault location, which is adopted by most existing CPDS reliability analysis methods, may make the calculation results expand the adverse effects of cyber systems on physical systems.

3) It is difficult to adapt to the complexity of the actual distribution network. First, the grid structure is complex: due to the late development of China's distribution network, the existing distribution system target grid is not clear and the connection mode is diversified. There are a large number of feeders with multi-layer branch lines and several tie switches. Second, the components are diverse: the physical system has a variety of switching elements such as circuit breakers(CB), section switches(SS), fuses, tie switches(TS), disconnectors, etc.; and the automation terminal units in the cyber system have different types such as local fault indicator(LFI) unit, remote fault indicator(RFI) unit, remote monitoring and control(RMC) unit. The above two points lead to the complexity of the actual distribution network. However, most of the existing CPDS reliability analysis methods are based on some simplified assumptions, such as assuming that intelligent electronic devices(IED) are advanced enough, in which all the automation terminal units have RMC function; or assuming that there is no multi-level branch line and so on. These assumptions have brought limitations and difficulties to the application of most methods in the actual distribution network.

In summary, how to model the cyber-physical interaction process in CPDS more elaborately, quantify the impact of cyber system failures on the physical system more accurately, and establish a CPDS reliability analysis method suitable for various complex scenarios in the actual distribution network, are the current challenges in this field of research. To solve the three problems, an elaborate reliability analysis method catering to the needs mentioned above is proposed in this paper. The contributions of the work are listed as follows:

1) Elaborate reliability models for IEDs, which are the coupling elements of the two systems, are established. The models consider multiple working states caused by one or more modules' faults of three types of IEDs: IEDs with local fault indicator (LFI-IED), IEDs with remote fault indicator (RFI-IED), IEDs with remote monitoring and control (RMC-IED).

2) By analyzing the cyber-physical interaction of CPDS during the FLISR process, the quantitative mapping relationship of the multiple fault states of IEDs, the locations of IEDs and the reliability of CPDS is proposed and summarized as some laws. The laws fully consider the topology of the actual CPDS and the human-computer joint participation in the actual fault management, which makes them suitable and accurate for various complex cases in engineering applications.

3) A CPDS reliability calculation procedure for distribution network with various IEDs, multi-layer branch lines and several tie points is proposed based on the framework of Monte Carlo method, which provides technical support for reliability assessment in the planning and operation of the actual distribution networks considering the physical and cyber system integration.

The rest of the paper is organized in the following sequence. Section II proposes elaborate reliability models of the components and the two systems in CPDS. Section III analyzes the FLISR process and establishes the relationship between IED faults and physical fault processing time calculation. Section IV proposes the procedure of the CPDS reliability evaluation method. Section V simulation experiment verifies the feasibility and practicality of the proposed method. Section VI concludes the paper.

II. STRUCTURE AND RELIABILITY MODEL OF CPDS

A. STRUCTURE OF CPDS

The common CPDS structure is shown in Fig. 1. The physical system consists of switching elements (CBs, SSs, fuses, TSs, etc.), transmission lines, loads, and distribution transformers. The cyber system is generally composed of IEDs, server and its application software platforms, communication links and communication protocols between IEDs and server. Hierarchical structure design is usually adopted in this system, which is divided into a backbone layer and an access layer. Through the IEDs configured in the switches and the distribution transformers, CPDS realizes the cyber-physical interaction, and completes the real-time monitoring and fault handling of the distribution network.

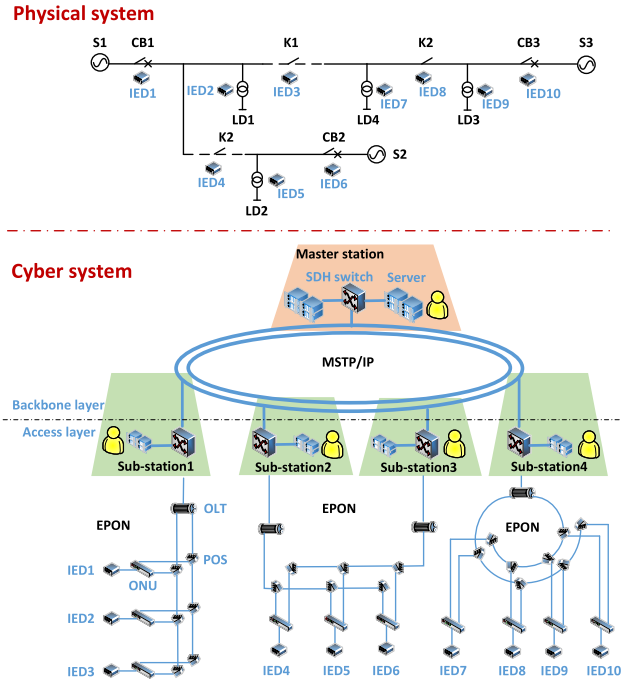


FIGURE 1. A common CPDS structure.

In this paper, a widely used communication mode is taken as an example to establish the reliability model of the cyber system. The backbone network adopts MSTP based integrated data optical terminals, and the optical ports of SDH to form the optical fiber self-healing ring network. The access network adopts ethernet passive optical network (EPON) to form one point to multi-point optical fiber network.

B. RELIABILITY MODEL OF CPDS ELEMENTS

In this paper, the "normal-fault" two-state model [19] is used to establish the reliability models of the CPDS elements except IEDs. It is considered that the normal operation time and fault outage time of these elements follow an exponential distribution, and the calculation formula of the state transition probability is referred to [20].

In particular, since the failure of one or more modules in the IEDs causes the IEDs to exhibit a variety of working states, a two-state reliability model is established for each module of the IEDs.

C. RELIABILITY MODEL AND WORKING STATE OF IED

CPDS realizes the cyber-physical interaction through IEDs. Establishing accurate reliability models for the coupling elements, IEDs, is one of the keys to study the reliability of CPDS.

In the physical system, IEDs which are installed at switches or distribution transformers, are the interface equipment to carry out the real-time monitoring and fault handling of the distribution network. The impact of their module faults or communication link faults on the reliability of power supply can be divided into direct impact and indirect impact. The direct impact can be incorporated into the reliability

parameters of the element [9]. It means that, the traditional reliability analysis methods and processes can be directly applied. The indirect effect is reflected in the IED failures of switching elements leading to errors in the FLISR process, which causes the unnecessary power outage events or the extension of the fault handling time. In the cyber system, IEDs are the evaluation objects of cyber system reliability, but the reliability of IEDs and their communication links with the server is generally not affected by the physical system failures, because the independent power modules of IEDs can support the IEDs to continue monitoring work for several hours after the power cut caused by the physical system failures. Based on the above reasons, this paper focuses on the reliability quantitative analysis when the cyber system fails at the same time with physical failures.

This article does not consider the failures of the IED independent power modules. In addition, microcomputer protection is used in the relay protection modules, and has high reliability, so this article assumes that these modules are completely reliable. The IEDs' models are shown in Fig. 2.

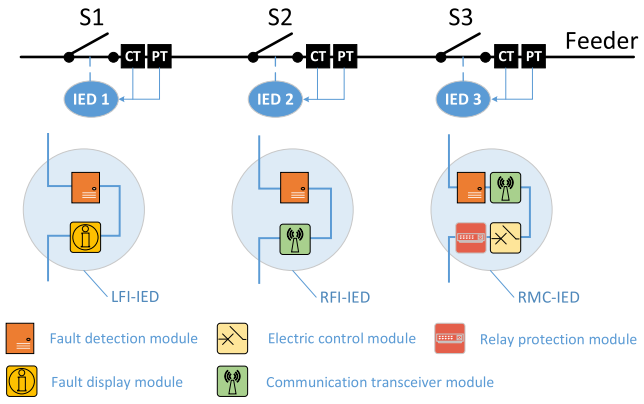


FIGURE 2. IEDs' models.

The function of LFI-IED is to indicate whether the fault current flows through the corresponding switch at the feeder site, which can help the maintenance personnel to find the fault quickly when inspecting the feeder. RFI-IED can identify whether the fault current has flowed through the switch and communicate this information to the master station, which can help the staff in the master station to determine where the fault may exist remotely. In addition to the function of RFI-IED, RMC-IED also enables the master station staff to remotely control the corresponding switch. Table 1 defines and summarizes the working states and characteristics of IEDs considering different the state combination of multiple modules, where 1 indicates normal and 0 indicates fault. The communication state is determined jointly by the state of the communication transceiver module of the IED and the state of the communication links between the IED and the server. Only when the module is normal and the link is reliable, the communication state of the IED is normal. The reliability analysis of the communication links is detailed in section I-D. The last column of Table 1 is the equivalent treatment of this kind of IEDs with this working state in the subsequent analysis of this article.

D. RELIABILITY MODEL OF COMMUNICATION LINK

The reliability evaluation of communication links generally covers three aspects of transmission performance: topological connectivity, timeliness of transmission, and accuracy of messages. The message transmission between the sender and the receiver can ensure the accuracy of the message with algorithm encryption, data retransmission or feedback after receiving successfully. Therefore, this paper does not consider the case of error code or packet loss.

1) TOPOLOGY RELIABILITY EVALUATION

Generally, redundancy protection is designed in the networking mode of the communication system. If any communication path between the IED and the server is reliably connected, the communication link of the IED meets the topology reliability requirement. The reliability of a single communication path is evaluated using the reliability model of the series system.

After abstracting the communication network based on graph theory, the topological reliability between all the IEDs and the server is obtained by calculating the reachability matrix [21] of the communication network with its adjacency matrix, instead of searching all the communication paths.

2) TIMELINESS RELIABILITY EVALUATION

If any of all connected communication paths can complete a single transmission with the server within the delay threshold of the IED, the IED is considered to meet the timeliness reliability requirement with the server. The delay of a single communication path in a single transmission is mainly related to the forwarding times of the node devices [22]. Moreover, considering the message flowing on the fiber line, especially the backbone layer line with a long length, which will also cause the delay [12], a linear model is used to calculate the delay of the communication path i between server A and IED B:

$$d_{A-B}(i) = \frac{L_i}{c} + \sum_{p=1}^{k} \tau_p \tag{1}$$

where, c is the speed of light, L_i is the fibers' lengths of the communication path, k is the number of node devices of the communication path, and τ_p is the message forwarding delay of the node device p. The value of τ_p adopts the Pareto distribution model with the parameters of 67.9ms and 20 [23].

III. ANALYSIS OF THE IMPACT OF CYBER SYSTEM ON FLISR

The cyber system influences the decision and realization of the FLISR process through the IEDs, thereby affecting the reliability of the physical system. The distribution automation (DA) system mainly realizes the FLISR process through three modes: local DA, distributed DA and centralized DA.

TABLE 1. Working states of three types of IEDs.

IED	Working state	Fault detection module state	Fault display module state	Commu-nication state	Electric control module state	Working characteristics	Equivalent treatment
LFI-IED	①	1	1	\	\	Normally indicate whether the fault current flows through the switch locally.	\
	②	0	1	\	\	The result of indicating whether the fault current flows through the switch locally is contrary to the fact.	\
	③	0 or 1	0	\	\	Indicates no fault current locally whether the fault current flows through the switch or not.	\
RFI-IED	①	1	\	1	\	Normally indicate whether the fault current flows through the switch remotely.	\
	②	0	\	1	\	The result of indicating whether the fault current flows through the switch remotely is contrary to the fact.	\
	③	0 or 1	\	0	\	The master station staff cannot know whether the fault current flows through the switch.	The switch has no IED configured
RMC-IED	①	1	\	1	1	The master station staff can monitor and control the switch normally.	\
	②	1	\	1	0	The master station staff can normally monitor the switch but cannot control it.	The switch is configured with RFI-IED in state ①.
	③	0	\	1	1	The result of indicating whether the fault current flows through the switch remotely is contrary to the fact, but the master station staff can control the switch normally.	\
	④	0	\	1	0	The result of indicating whether the fault current flows through the switch remotely is contrary to the fact, and the master station staff cannot control the switch normally.	The switch is configured with RFI-IED in state ②.
	⑤	0 or 1	\	0	0 or 1	The master station staff cannot monitor and control the switch.	The switch has no IED configured

The failures of cyber system has the greatest impact on the centralized FLISR process, and the functional differentiation of IEDs is also reflected in it. Therefore, this paper analyzes the impact of cyber system on the centralized FLISR process. The IEDs of the distribution transformers or loads have little effect on the FLISR process. Only the IEDs of the switching elements are considered below. At the critical positions of the feeder, the CBs and TSs are generally equipped with RMC-IEDs, following analysis complies with this principle. For the convenience of discussion, some definitions are as follows:

A. Manual switch(MS): SS without RMC-IED.

B. Associated IED(Ass-IED): IEDs that may affect fault handling time in case of misjudgment or missing judgment.

C. Area: Feeder range enclosed by operable switches (CB, SS, TS).

D. Incoming switch(InS): The switch at the boundary of the area where the direction of the current is from the outside to the inside of the area.

E. Outgoing switch(OutS): The switch at the boundary of the area where the direction of the current is from the inside to the outside of the area.

F. Remote area(RA): The area enclosed by the switches equipped with remote IEDs, without other switches equipped with remote IEDs inside.

G. Onsite area(OA): The area enclosed by the switches equipped with IEDs, without other switches equipped with IEDs inside.

H. Relay protection isolation area(RPIA): the downstream range of the upstream CB closest to the fault. This is the fault isolation area after relay protection action.

I. Actual remote fault location area(ARFLA): the minimum fault area that can be determined by the fault message transmitted remotely, consisting of the correct remote fault location area(CRFLA) and the error remote fault location area(ERFLA). CRFLA is the area enclosed by the switches of all the nearest remote IEDs of the fault. It is the minimum area where the master station staff judges the fault location when all the remote Ass-IEDs are not misjudged or missed. ERFLA is a remote fault location area except the area of CRFLA.

J. Preliminary fault isolation area(PFIA): the area outside the feeder area that can be restored relying on the remote switches and the message obtained by the remote IEDs. It is surrounded by the switches with RMC-IEDs and CBs, and contains the ARFLA.

K. Actual feeder inspection area(AFIA): the minimum fault area that can be determined by the onsite fault information and remote messages, including the correct feeder inspection area(CFIA) and the error feeder inspection area(EFIA). CFIA is the area enclosed by the switches of all the nearest IEDs of the fault. It is the minimum area where the fault is located after the maintenance personnel check the display of local IEDs onsite without misjudgment or missing judgment of all Ass-IEDs. EFIA is a feeder inspection area except the area of CFIA.

L. Final fault location area(FFLA): the area surrounded by all the nearest switches of the fault.

A. CENTRALIZED FLISR PROCESS OF ACTUAL DISTRIBUTION NETWORK

1) SPECIFIC STEPS OF FLISR PROCESS

As shown in Fig. 7 in Appendix A, the actual centralized FLISR process of CPDS includes the following steps:

Step 1: The upstream CB nearest to the fault trips due to the action of the relay protection module, forming a RPIA.

Step 2: The RFI-IEDs and RMC-IEDs in the RPIA send message about fault current to the master station. The analysis software of the master station and the staff jointly determine the ARFLA. If there is a switch with RMC-IED in RPIA and upstream of ARFLA, or there is a switch with RMC-IED or CB on the feeder that can recover power supply of downstream of ARFLA, the staff will remotely operate the above switches nearest to the fault to form PFIA, and remotely restore the loads with power transfer conditions downstream of PFIA. If there is no above-mentioned switch, the coverage of RPIA and PFIA are same.

Step 3: The maintenance personnel are dispatched to check the display of all LFI-IEDs in ARFLA, and then determine the AFIA.

Step 4: The maintenance personnel patrol the AFIA to find out the fault, and then determine the FFLA.

Step 5: If the upstream switch nearest to the fault is closed, open the switch and restore the loads upstream of FFLA. If part of the loads downstream of the FFLA has the condition of transfer, operate the related downstream switches nearest to the fault to restore their power supply.

Step 6: Repair the faulty element, and restore the power supply to all the loads in the FFLA and downstream the FFLA without power transfer conditions after repairment is finished.

2) TIME CALCULATION OF FLISR PROCESS

The fault handling time T can be divided into three parts: first, the remote isolation time t_1, which is the time for remote operation of switches with RMC-IEDs in step 2; second, the onsite isolation time t_2, which is the time for viewing LFI-IEDs, feeder patrol and operation of switches in steps 3-5; third, the fault repair time t_3, which is the time for repair of fault element in step 6

a: THE REMOTE ISOLATION TIME t_1

According to step 2, t_1 is calculated as follows:

$$t_1 = n_{3initial} \times t_{rmt} \tag{2}$$

where, t_{rmt} is the average time for remote operation of a switch with RMC-IED; $n_{3initial}$ is the number of switches with RMC-IEDs to be remotely operated in preliminary isolation operation (step 2), which can be expressed by the following formula:

$$n_{3initial} = n_{up-initial} + 2n_{down-initial} \tag{3}$$

where, $n_{up-initial}$ is the sign of whether the InS of the PFIA is configured with RMC-IED, if so, its value is 1, otherwise it is 0; $n_{down-initial}$ is the number of OutSs of the PFIA with remote power transfer conditions in the downstream feeder range, which is multiplied by 2 to consider that the downstream TSs also need to be remotely operated.

b: THE ONSITE ISOLATION TIME t_2

t_2 can be divided into four parts: the time for the maintenance personnel traveling to the fault feeder site t_{21}, the time for inspecting all the LFI-IEDs in the ARFLA t_{22}, the time for patrolling the feeder in the AFIA t_{23}, the time for operating the switches to restore all the loads outside the FFLA t_{24}:

$$t_2 = t_{21} + t_{22} + t_{23} + t_{24} \tag{4}$$

$$t_{22} = n_{IED1} \times t_{IED1} \tag{5}$$

$$t_{23} = l_{ptl} \times t_{ptl} \tag{6}$$

$$t_{24} = n_{3final} \times t_{rmt} + n_{mnl} \times t_{mnl} \tag{7}$$

where: n_{IED1} is the number of LFI-IEDs in the ARFLA; t_{IED1} is the average time to check the display of a LFI-IED; l_{ptl} is the feeder length of the AFIA; t_{ptl} is the average time for patrolling per kilometer of feeder; t_{mnl} is the average time for manually operating a switch; n_{3final} is the number of switches to be operated remotely in step 5; n_{mnl} is the number of switches to be operated manually in step 5.

n_{3final} can be calculated as follows:

$$n_{3final} = n_{up-final} + n_{down-final} + n_{tie} \tag{8}$$

where, $n_{up-final}$ is the sign of whether the InS with RMC-IED of the FFLA is also the InS of the PFIA, if so, its value is 0, otherwise it is 1; $n_{down-final}$ is the number of OutSs with RMC-IEDs of the FFLA (but not the OutSs of the PFIA), where the downstream feeder has transfer conditions. If the cyber system is normal, $n_{up-final}$ and $n_{down-final}$ are both 0. n_{tie} is the number of TSs that were closed in step 5 and not operated in step 2.

n_{mnl} can be calculated as follows:

$$n_{mnl} = n_{up-mnl} + n_{down-mnl} + n_{tie-mnl} \tag{9}$$

where, n_{up-mnl} is the number of manual InS of FFLA, this value is 0 or 1; $n_{down-mnl}$ is the number of manual OutSs of the FFLA with downstream feeder transfer conditions; $n_{tie-mnl}$ is the number of TSs that need to be manually closed in step 5. If the cyber system is normal, $n_{tie-mnl}$ is 0.

B. THE IMPACT OF CYBER SYSTEM FAILURE ON FAULT HANDLING TIME

According to the characteristics analysis and equivalent treatment of the various working states of the three types of IEDs in Sections II-C and II-D, as well as the states of all elements or modules of the cyber system, we can know the equivalent types and states of all IEDs in CPDS and whether there are misjudgments or missing judgments. If no misjudgment or missing judgment occurs in the IEDs, the normal fault handling time shall be calculated according to Section III-A.

Otherwise, the misjudged or missed IEDs shall be taken as breakthrough points to analyze the impact of cyber system failures on the FLISR process, and the actual fault handling time shall be calculated according to the mapping laws of IED failures and FLISR process abnormality established below.

In this paper, only one-order fault is considered for physical systems in the reliability analysis. However, due to the redundant design of the communication network, and the global fault information being considered in the centralized DA, not all IED faults affect the FLISR process. Therefore, the limit of one-order faults in cyber system may weaken the impact of cyber system failures on the physical system. In order to make it possible to obtain the laws of CPDS reliability analysis by enumerating all complex CPDS failure scenarios on the premise of ensuring the accuracy of the evaluation, all Ass-IEDs are given the limit that only one of them may be misjudged or missed.

By assuming that there is a remote or a local IED at the position possible for IEDs on the feeder and analyzing whether it affects the fault location and isolation process,, all the positions of Ass-IEDs are obtained. The remote Ass-IED is a remote IED with no more than 1 other remote IED on the minimum path between this IED and the fault. The local Ass-IED is a LFI-IED with no more than 1 other LFI-IED and no remote IEDs on the minimum path between this IED and the fault. In the case where all the above-mentioned positions and types of IEDs are normal, there are no less than two IEDs correctly indicating the location of the physical fault. Considering the role of human auxiliary judgment in the centralized FLISR process, missing judgments or misjudgments of remote IEDs or local IEDs at other positions are easy to be recognized by the main station staff or onsite maintenance personnel, and will not affect the failure location and isolation.

1) FAILURE IMPACT ANALYSIS OF REMOTE ASS-IED

a: IMPACT ON FAULT LOCATION

The misjudgments or missing judgments of the remote Ass-IEDs will result in the ERFLAs and EFIAs, thus affecting the calculation of t_{22} and t_{23}. According to the failure impact on FLISR process, remote Ass-IEDs can be divided into four types: 1) type I remote Ass-IED: the nearest remote Ass-IED upstream of the physical fault; 2) type II remote Ass-IED: the second nearest remote Ass-IED upstream of the physical fault; 3) type III remote Ass-IED: the nearest remote Ass-IED of the physical fault, but not on the minimum path between the physical fault and the power source; 4) type IV remote Ass-IED: the second nearest remote Ass-IED of the physical fault, but not on the minimum path between the physical fault and the power source.

Table 2 summarizes the laws about the impact of missing judgments or misjudgments of four types of remote Ass-IEDs on remote fault location and feeder inspection scope. Relevant analysis and explanation with drawings is in Appendix B.

b: IMPACT ON FAULT ISOLATION

The fault isolation process of CPDS can be divided into preliminary fault isolation (step 2) and final fault isolation (step 5). The failures of the remote Ass-IEDs may result in not carrying out the preliminary isolation that was originally required, or it may lead to the final isolation requiring remote operation of the switch that should be operated in the preliminary isolation, thereby causing changes in t_1 and t_{24} compared to normal conditions.

Table 3 summarizes the laws about the impact of missing judgments or misjudgments of four types of remote Ass-IEDs on fault isolation. Relevant analysis and explanation with drawings is in Appendix B.

2) FAILURE IMPACT ANALYSIS OF LOCAL ASS-IED

The misjudgments or missing judgments of the local Ass-IEDs will result in the EFIAs, thus affecting the calculation of t_{23}. According to the failure impact on FLISR process, local Ass-IEDs can be divided into four types: 1) type I local Ass-IED: the nearest local Ass-IED upstream of the physical fault; 2) type II local Ass-IED: the second nearest local Ass-IED upstream of the physical fault; 3) type III local Ass-IED: the nearest local Ass-IED of the physical fault, but not on the minimum path between the physical fault and the power source; 4) type IV local Ass-IED: the second nearest local Ass-IED of the physical fault, but not on the minimum path between the physical fault and the power source.

Table 4 summarizes the laws about the impact of missing judgments or misjudgments of four types of local Ass-IEDs on feeder inspection scope. Relevant analysis and explanation with drawings is in Appendix B.

C. THE IMPACT OF CYBER SYSTEM FAILURE ON FAULT EFFECT ANALYSIS

Fault effect analysis is the basis of calculating reliability indices of loads. Next, the laws of failure effect analysis in CPDS considering cyber failures is proposed and explained in combination with Fig. 3, where the judgment of the IED of switch S4 in the figure is missed.

1) The outage time of the loads outside RPIA is 0, such as LD1 in Fig. 3.

2) The outage time of the loads in RPIA and upstream of PFIA is t_1, such as LD2 in Fig. 3.

3) If the downstream area of an OutS of PFIA has the condition of power transfer, the outage time of the loads in downstream area of this OutS is t_1, such as LD7 and LD9 in Fig. 3.

4) The outage time of the loads in PFIA and upstream of FFLA is $t_1 + t_2$, such as LD3-LD5 in Fig. 3.

5) The outage time of the loads in FFLA is $t_1 + t_2 + t_3$, such as LD6 in Fig. 3.

6) If the downstream area of an OutS of FFLA does not meet the power transfer condition, the outage time of the loads in the downstream area of this OutS is $t_1 + t_2 + t_3$, such as LD10 and LD11 in Fig. 3.

TABLE 2. The impact of remote Ass-IED failures on fault location.

Law	Remote Ass-IED failure type	Resulting ERFLA	Resulting EFIA
A	Missing judgment of type I	The remote area that one of its OutSs is configured with this faulty IED	1) The onsite area that one of its OutSs is configured with this faulty IED 2) The onsite area that one of its OutSs is the InS of the first EFIA
B	Missing judgment of type II	The remote area that one of its OutSs is configured with this faulty IED	1) The onsite area that one of its OutSs is configured with this faulty IED
C	Misjudgment of type III	The remote area whose InS is configured with this faulty IED	1) The onsite area whose InS is configured with this faulty IED 2) All the onsite areas whose InS is one of the OutSs of the first EFIA
D	Misjudgment of type IV	The remote area whose InS is configured with this faulty IED	1) The onsite area whose InS is configured with this faulty IED

TABLE 3. The impact of remote Ass-IED failures on fault isolation.

Law	Remote Ass-IED failure type	Additional conditions	Impact on t_1 or t_{24}
E	Missing judgment of type I	1) This faulty IED is a RMC-IED. 2) In RPIA, there is a switch with a RMC-IED upstream of ERFLA. 3) There is a power transfer condition downstream of ERFLA.	Compared with the cyber normal situation, t_1 increases t_{rmt}.
F	Missing judgment of type I	1) This faulty IED is a RMC-IED. 2) In RPIA, there is no switch with a RMC-IED upstream of ERFLA. 3) There is no power transfer condition downstream of ERFLA.	Compared with the cyber normal situation, t_1 reduces t_{rmt}.
G	Missing judgment of type II	1) The switch where the missing IED is located is not a feeder head-end switch. 2) The type I or type II remote Ass-IED is a RMC-IED. 3) In RPIA, there is no switch with a RMC-IED upstream of ERFLA.	Compared with the cyber normal situation, t_1 reduces t_{rmt}.
H	Misjudgment of type III	1) This faulty IED is a RMC-IED. 2) In RPIA, there is a switch with a RMC-IED downstream of ERFLA. 3) There is a power transfer condition downstream of ERFLA.	Compared with the cyber normal situation, t_1 increases t_{rmt}.
I	Misjudgment of type III	1) This faulty IED is a RMC-IED. 2) There is no power transfer condition downstream of ERFLA.	Compared with the cyber normal situation, t_1 increases t_{rmt}.
J	Misjudgment of type IV	1) This faulty IED or its upstream type III remote Ass-IED is a RMC-IED. 2) There is a power transfer condition downstream of ERFLA. 3) In RPIA, there is no switch with a RMC-IED downstream of ERFLA.	Compared with the cyber normal situation, t_1 reduces $2t_{rmt}$.
K	Missing judgment of type II	1) The upstream switch nearest to the physical fault is a SS with RMC-IED. 2) The switch where the missing IED is located is not a feeder head-end switch.	Compared with the cyber normal situation, t_{24} increases t_{rmt}.
L	Missing judgment of type I	1) This faulty IED is a RMC-IED. 2) The switch where this faulty IED is located is the upstream switch nearest to the physical fault. 3) There is no power transfer condition downstream of this faulty IED.	Compared with the cyber normal situation, t_{24} increases t_{rmt}.
M	Misjudgment of type IV	1) The switch with the type III remote Ass-IED upstream of the faulty IED is a SS with RMC-IED, and it is the downstream switch nearest to the physical fault. 2) There is a power transfer condition downstream of ERFLA. 3) There is no switch with RMC-IED downstream of ERFLA.	If conditions 1) and 2) are satisfied, t_{24} increases t_{rmt} compared with the cyber normal situation. If conditions 1)-3) are satisfied, t_{24} increases $2t_{rmt}$ compared with the cyber normal situation.

TABLE 4. The impact of remote Ass-IED failures on fault location.

Law	Local Ass-IED failure type	Resulting EFIA
N	Missing judgment of type I	1) The onsite area that one of its OutSs is configured with this faulty IED 2) The onsite area that one of its OutSs is the InS of the first EFIA
O	Missing judgment of type II	1) The onsite area that one of its OutSs is configured with this faulty IED
P	Misjudgment of type III	1) The onsite area whose InS is configured with this faulty IED 2) All the onsite areas whose InS is one of the OutSs of the first EFIA
Q	Misjudgment of type IV	1) The onsite area whose InS is configured with this faulty IED

7) If the downstream area of an OutS of FFLA has the condition of power transfer, the outage time of the loads belonging to the PFIA in the downstream area of this OutS is $t_1 + t_2$, such as LD8 in Fig. 3.

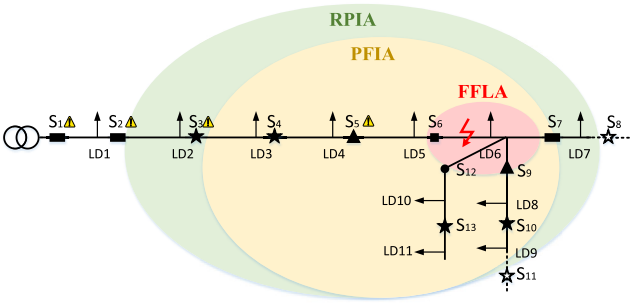
IV. ELABORATE RELIABILITY EVALUATION PROCEDURE OF CPDS

A. RELIABILITY INDICES

In this paper, the average annual outage rate λ (f/yr) and average annual outage time U (hr/yr) of loads are taken as load reliability indices. System reliability indices include system average duration frequency index(SAIDI), system average interruption frequency index(SAIFI), customer average interruption duration index(CAIDI), average service availability index(ASAI) and expected energy not supplied(EENS).

B. RELIABILITY EVALUATION PROCEDURE BASED ON MONTE CARLO METHOD

There are many complex scenes caused by the variability of IED equivalent types or working states, multi-layer branch



⚠ : Characterize the switch where the fault current flows

Note:
1)The rectangle, star, triangle, circle represents the CB, switch with RMC-IED, switch with RFI-IED, switch with LFI-IED respectively.
2)The black dotted line indicates the opposite line, and the switch on this line indicates the tie switch.

FIGURE 3. Fault effect analysis for CPDS.

lines and several tie points in actual CPDSs, which makes it difficult to evaluate the reliability by the analytical method. In addition, the FLISR process is a sequential process, which fits better with the Monte Carlo simulation process. Therefore, this paper uses the Monte Carlo method to evaluate the reliability of CPDS, as shown in Fig. 4, where S5 and S8 can be respectively divided into 5 sub steps:

S5.1 According to the description of the preliminary isolation operation in the FLISR process step 2 and definition J, combined with the description of CRFLA in definition I, t_{10} is calculated by using (2-3).

S5.2 According to the description of CRFLA in definition I, the time t_{220} for checking the display of all LFI-IEDs in CRFLA when the cyber system is normal is calculated by using (5).

S5.3 According to the description of CFIA in definition K, the time t_{230} for patrolling the feeder when the cyber system is normal is calculated by using (6).

S5.4 According to the description of the final isolation operation in the FLISR process step 5, combined with the description of FFLA in definition L, the time t_{240} for restoring all the loads outside the FFLA when the cyber system is normal is calculated by using (7-9).

S5.5 the time t_{20} is calculated by using (4).

S8.1 t_1 is obtained by modifying t_{10} according to the laws E-J.

S8.2 According to the laws A-D, ERFLA is obtained. Combining (5) and t_{220}, the time t_{22} in this simulation for checking the display of all LFI-IEDs in ARFLA is calculated.

S8.3 According to the laws A-D, N-Q, the EFIA is obtained. Combining (6) and t_{220}, the time t_{23} for patrolling AFIA in this simulation is calculated.

S8.4 According to the laws K-M, t_{240} is modified to obtain the time t_{24} for operating switches and restoring the loads outside FFLA in this simulation.

S8.5 the time t_2 is calculated by using (4).

V. SIMULATION ANALYSIS

This article takes an actual medium voltage distribution network system in a city as an example to build a CPDS, and

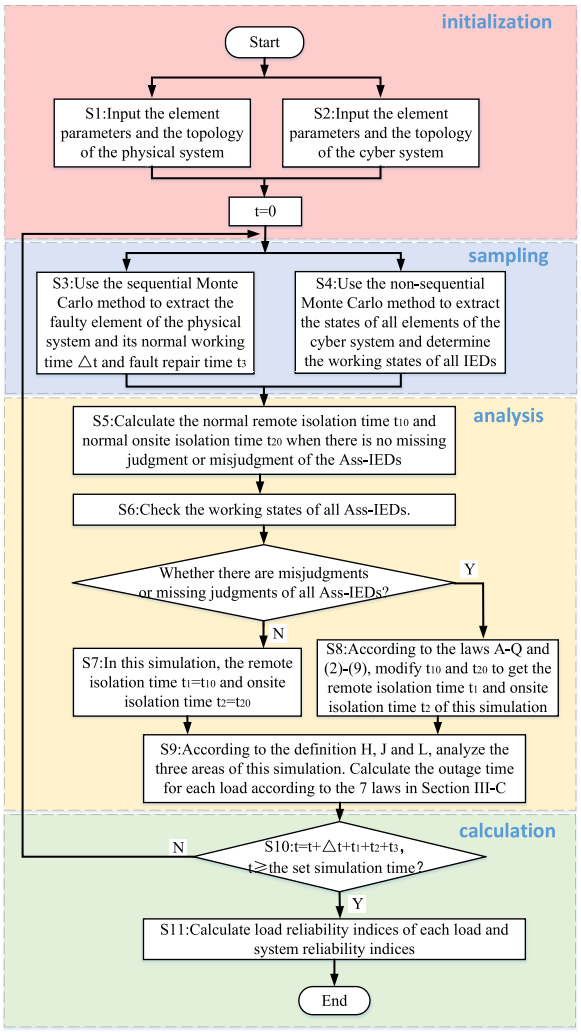


FIGURE 4. Fault effect analysis for CPDS. Reliability analysis procedure for complex CPDS.

uses the algorithm proposed above to perform reliability calculations.

A. SIMULATION SYSTEM AND PARAMETERS

After abstraction based on graph theory, the test CPDS structure is shown in Fig. 5. The physical system is a single power source and multi-feeders system. The tie points, switch types and IED configurations of each switch are marked as shown in the figure, where the thick line indicates the main line and branch line, the thin line represents the user branch line consisting of four elements: fuse, line, distribution transformer, and load. The technical characteristics of the backbone layer and the access layer of the cyber system are consistent with those described in Section II-A. The access layer adopts a chain topology.

The reliability parameters of the physical system elements [24], [25] and the cyber system elements [12], [18] are respectively shown in Appendix C, Table 8, Table 9. The delay threshold of IEDs is set by referring to [26]. Refer to [27],

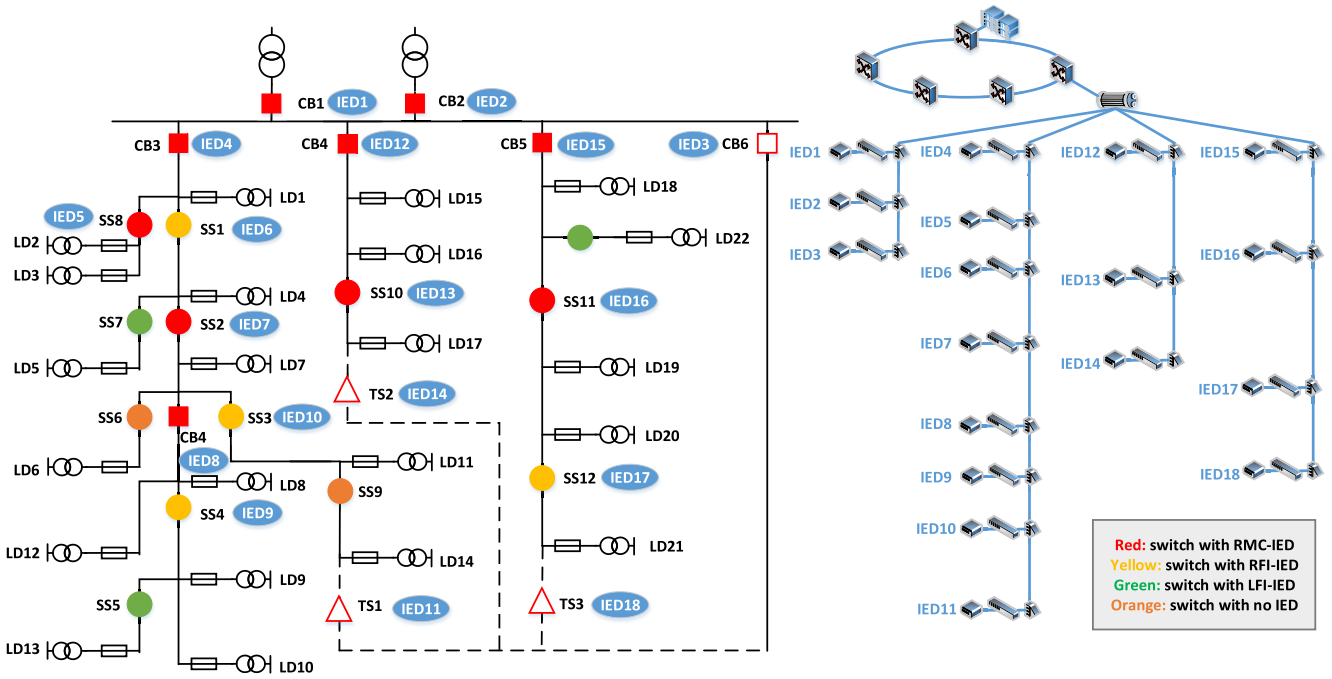


FIGURE 5. Structure of the test CPDS.

several time parameters related to the fault handling level of grid companies are set as shown in Appendix C, Table 10.

B. SIMULATION RESULT ANALYSIS

1) CASES SETTING AND RESULTS

In order to study the positive and negative effects of the cyber system on the physical system in the actual CPDS, and to test the reliability evaluation method proposed in this paper, four cases are designed in this section:

- Case 1: regardless of the cyber system, the physical fault handling process only relies on relay protection and manual feeder inspection.
- Case 2: considering that the cyber system is completely reliable, fault handling process depends on relay protection, realize error-free remote monitoring of the master station and manual feeder inspection.
- Case 3: considering that the cyber system is not completely reliable, fault handling process depends on relay protection, remote monitoring of the master station that may be wrong, and manual feeder inspection.
- Case 4: Refer to [12], it is assumed that the cyber system is not completely reliable, and the CPDS is advanced enough so that all switches are configured with RMC-IEDs.

The simulation duration is set to 15000a (the calculation result of this simulation duration has become stable). The system reliability indices for four cases, the load reliability indices of each load in case3, and the times of various cyber failures in case3 are respectively shown in Table 5–7.

TABLE 5. The system reliability indices for four cases.

Case	SAIDI (hr/cust·yr)	SAIFI (f/cust·yr)	CAIDI (hr/cust·yr)	ASAI (%)	EENS (MWh)
1	9.2296	1.2913	7.1475	99.8946	16.5704
2	5.8511	1.2900	4.5356	99.9332	10.7501
3	6.8917	1.2910	5.3384	99.9213	12.5263
4	6.6002	1.2906	5.1141	99.9247	11.9833

TABLE 6. The load reliability indices of each load in case3.

NO.	λ (f/yr)	U (hr/yr)	NO.	λ (f/yr)	U (hr/yr)
LD1	1.4024	6.2254	LD12	1.8413	8.1196
LD2	1.4015	7.4630	LD13	1.8403	9.5759
LD3	1.3986	7.4945	LD14	1.3988	7.6896
LD4	1.4013	6.8348	LD15	0.7743	7.1057
LD5	1.3975	7.2788	LD16	0.7738	6.7065
LD6	1.4000	7.0677	LD17	0.7733	4.8119
LD7	1.3985	5.8549	LD18	0.8547	4.6221
LD8	1.8409	7.9034	LD19	0.8512	5.6190
LD9	1.8381	8.4189	LD20	0.8574	5.9545
LD10	1.8365	8.0599	LD21	0.8532	5.3770
LD11	1.4027	6.7070	LD22	0.8549	6.1441

2) RELIABILITY RESULT ANALYSIS OF FOUR CASES

Table 5 is analyzed from the following aspects:

1) The SAIFI in the four cases is basically the same. The main reason that affects SAIFI is the reliability parameters of the component in physical system, and the CPDS reliability algorithm proposed in this paper focuses on the quantitative modeling and analysis of the indirect effect of cyber system on the physical system. Therefore, SAIFI will not vary much

TABLE 7. The times of various cyber failures in case3.

Statistics	Times	Statistics	Times
Total simulation times	67181	Times of the cyber system with complete reliability	3850
Simulation times of cyber system failures affecting FLISR	25634	Times of the server failure	717
Times of misjudgments or missing judgments of Ass-IEDs	2912	Times of communication link failures affecting FLISR	29582
Times of LFI-IEDs' fault detection module failures affecting FLISR	543	Times of communication link topological failures affecting FLISR	25923
Times of LFI-IEDs' fault display module failures affecting FLISR	207	Times of communication link delayed failures affecting FLISR	3659
Times of RFI-IEDs' fault detection module failures affecting FLISR	1039	Times of RFI-IEDs' communication transceiver module failures affecting FLISR	1741
Times of RMC-IEDs' fault detection module failures affecting FLISR	1132	Times of RMC-IEDs' communication transceiver module failures affecting FLISR	1536
Times of RMC-IEDs' electric control module failures affecting FLISR	40		

in these four cases in which different ways are taken to consider the cyber systems.

2) Compared with case 1, SAIDI, CAIDI and EENS decreased by 36.61%, 36.54% and 35.12% respectively, and ASAI increased by 0.0386% in case 2. This is because the cyber system improves the automation level of fault handling, which shortens the time of fault handling and greatly improves the reliability. Therefore, the construction and application of the cyber system are of great significance to a better guarantee of the reliability of the distribution network.

3) Compared with case 2, SAIDI, CAIDI and EENS increased by 17.78%, 17.70% and 16.52% respectively, and ASAI decreased by 0.0119% in case 3. Case 3 takes into account the misleading, missing assistance and other adverse effects of the cyber system failures on the FLISR process, which makes the fault handling time longer and the system reliability decrease to a certain extent. This shows that though the cyber system has positive effect on the reliability of the physical system, its negative effects cannot be ignored. Reliability calculations that consider the negative effects of cyber systems are more accurate and can more fully reflect the true reliability of the physical system under the coupling relationship between the two systems. In addition, this also shows that the maintenance of the cyber system and the improvement of the reliability of the cyber system itself also have a certain significance to the reliability of the physical system.

4) Compared with case 4, SAIDI, CAIDI and EENS increased by 4.42% (17.5 minutes), 4.39% (13.5 minutes) and 4.53% respectively, and ASAI decreased by 0.0034% in case 3. This shows that the lack of careful consideration of IED reliability model will lead to errors that cannot be ignored in the final reliability calculation results of complex CPDS. In particular, when evaluating and verifying the expected reliability of urban distribution network planning or reconstruction projects, the error may result that the planning or reconstruction schemes failing the reliability requirements of the corresponding power supply district pass the reliability verification, or lead to the wrong choice of the planning or transformation schemes. Therefore, the simulation results validate the accuracy and effectiveness of the reliability algorithm proposed in this paper for the CPDSs with more diverse components and more complex structures, whereas the reliability algorithm of case 4 is more suitable for the new park distribution networks which adopt the automatic construction scheme of all switches configuring with RMC-IEDs, such as the new parks belonging to A+ power supply district with high reliability requirement.

3) ANALYSIS OF VARIOUS CYBER FAILURES IN CASE 3

Table 7 is analyzed from the following aspects:

1) The failure probability of cyber system components cannot be ignored, especially the IEDs. The proportion of simulation times with cyber system failures in simulation process is as high as 94.27%. However, not all cyber system failures will affect the FLISR process and lead to the decline of CPDS reliability. For example, the IEDs that are missed or misjudged are not the Ass-IEDs of the physical fault, or the IEDs that lose connection with the server are not the IEDs that the fault location or isolation depends on, etc. In this case, 38.16% of physical system faults are affected by cyber system failures, which is far less than 94.27%. The above data once again confirms the importance of considering the cyber failure effects on the reliability calculation of CPDSs, and also showed that it is necessary to build an elaborate CPDS reliability analysis model and procedure by combing and analyzing all kinds of cyber failure conditions that really affect the FLISR process.

2) There are many times when a communication link interruption affects the fault handling process. Several remote IEDs may be disconnected simultaneously in a single physical system fault simulation, and the main reason causes the communication link to fail is that the failure to meet the topology reliability. After analysis, the following reasons are considered possible:

First, the process of remote fault location and preliminary fault isolation relies on the information provided by many remote IEDs at the same time. Any communication interruption of the IEDS will affect this process, which is quite different from the impact mechanism of IED missing judgments or misjudgments on FLISR process (only the missing judgments or misjudgments of Ass-IEDs will affect the fault handling). Especially when there is misjudgment or missing

judgment in the Ass-IED, the normal communication of other remote IEDs may narrow the scope of remote fault location, or eliminate the misdirection of misjudgment or missing judgment of the IED to fault location and isolation. Because the result of the communication transceiver module failure of the remote IED is similar to that of the communication link failure, the above is also the reason why the communication transceiver module failures of the remote IEDs affect the FLISR process more than the failure detection module does.

Secondly, the access layer of the cyber system in the test system adopts the chain network mode without alternative route. When any element of the access layer fails, the IED downstream will not be able to communicate with the server. Therefore, the influence of topology reliability on the reliability of communication link is particularly prominent, which may also cause some remote IEDs to be disconnected synchronously in a single physical system fault simulation. In addition, the condition that the delay reliability is not satisfied usually occurs in the case of route conversion. The route conversion of the test CPDS can only occur in the backbone layer of the cyber system, with a small range and fewer components. Therefore, compared with the topology reliability, the impact of delay reliability on the reliability of the communication link is relatively small.

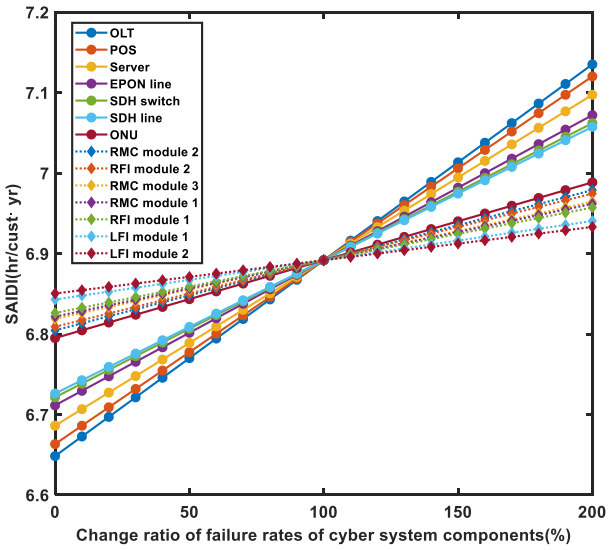


FIGURE 6. Sensitivity analysis of SAIDI to failure rates of cyber system components. Note: module 1 represents fault detection module; module 2 represents fault display module for LFI-IED; module 2 represents communication transceiver module for RFI-IED and RMC-IED; module 3 represents electric control module.

4) SENSITIVITY ANALYSIS IN CASE 3

In order to further study the influence of cyber system on the reliability of CPDS, the sensitivity analysis between SAIDI and the failure rates of cyber system components is carried out. Specifically, for each type of elements of the cyber system, its failure rate is increased from 0% to 200% in units of 1%, and the failure rates of other types of elements remains unchanged. In the case of the same failure rates, reliability calculations are performed for several times and the average of the results is taken as the reliability calculation result of this case. Finally, the reliability results corresponding to different failure rates of the same type of elements are linearly fitted, so that the relationship between the failure rates of various cyber system components and the SAIDI can be obtained, as shown in Fig. 6.

As can be seen from Fig. 6, due to the feature of no backup protection in the chain EPON network, the faults of OLTs and POSs may cause several IEDs on the feeder to lose contact at the same time, which has a greater impact on the reliability of the entire system. The server also has a greater impact on reliability. Once the server fails, all remote IEDs cannot assist in fault location and isolation, and the FLISR process can rely on LFI-IEDs. However, due to the low failure probability of the server, under the same failure rate change ratio, the server has less influence on reliability than OLTs and POSs. The impact of SDH network elements on reliability is at a moderate level, because SDH network is generally a ring structure, and the fault of a single element rarely causes multiple IEDs to lose contact at the same time. But if multiple SDH network elements fail, it is likely to affect all IEDs within a certain range, causing a significant impact on reliability. The failure rates of OUNs and IED modules have little effect on reliability, because the failure of such elements generally only affects a single IED, and not all IEDs' missing judgments or misjudgments will affect the FLISR process. In conclusion, in order to ensure the supporting role of cyber system on the reliability of physical system, power supply companies should pay more attention to the regular inspection and maintenance of components on the communication links.

VI. CONCLUSION

By establishing elaborate CPDS components and system reliability models, and analyzing the FLISR process with human-computer participation in actual CPDSs, this paper proposes a reliability evaluation method that adapts to the complex structures and various components of CPDSs, and considers the interaction between the physical system and the cyber system. It aims to provide some inspiration and ideas for the modeling and application of CPDS reliability assessment theory in the actual distribution network. By testing the proposed method, its feasibility and effectiveness are verified, and the following conclusions are drawn:

1) The reliability of cyber system components is one of the factors that cannot be ignored to affect the power supply reliability of physical system. In addition to attaching importance to the improvement of the power supply reliability by constructing the cyber system, we should also pay attention to the negative impact of the cyber failures and manage the reliability of cyber system by taking measures like regular maintenance.

2) The actual FLISR process includes not only the interaction between the cyber system and the physical system, but also the human-computer interaction. Therefore, not all cyber system failures will lead to the decline of the physical system reliability. In addition, the types of IEDs in the actual CPDs are diverse, so the elaborate reliability modeling and analysis of the CPDS is of great significance for more accurate evaluation of the actual distribution network reliability.

3) In order to ensure the supporting effect of cyber system on the reliability of physical system, power supply companies should pay more attention to the regular inspection and maintenance of elements on communication links than IEDs.

The existing DA system has a variety of fault handling modes, communication system technical characteristics and networking modes. Various power grid companies are accustomed to adopt different configuration schemes for DA systems. In order to facilitate the analysis, without prejudice to the application of the proposed method in most cases, this article makes certain assumptions about the fault handling mode, the technical characteristic and the networking mode of the communication system, but the method is still applicable to communication system with other networking modes with the same technical characteristics. In the follow-up research, the CPDS reliability evaluation theory with other automation modes and other communication modes will be studied more comprehensively, and the application and guidance of the CPDS reliability analysis in the prosumer energy management system of the existing distribution network will be further explored.

APPENDIX A

Fig. 7 here.

APPENDIX B

As shown in Fig. 8, the laws A-D about the impact of misjudgments or missing judgments of four types of remote Ass-IEDs on remote fault location and feeder inspection scope is explained following.

A) For example, if the RFI-IED of S5 in Fig. 8 are missed and other IEDs are normal, the master station staff will judge that the fault point is in area D. After checking the LFI-IED of S4 in area D and patrolling the feeder of area F, it can be concluded that there is no fault in area F. Then it can be judged that there is a misjudgment of S4's IED or a missing judgment of S5's IED. Through the feeder inspection of area E, it is known that area E has no fault, so S4's IED is normal, and it is S5's IED that has missing judgment. It can be re-known that the CRFLA is area G. To sum up, the ERFLA is area D, and the EFIA is e and F.

B) For example, if the RMC-IED of S3 in Fig. 8 are missed and other IEDs are normal, the master station staff judges that the fault point is in area A or G, and suspects that the S3's IED are missed or the S5's IED are misjudged. After checking the LFI-IED of S2 in area A and patrolling the feeder of area C, it is found that there is no fault in area C, then it can be judged that there is misjudgment of S2's IED or missing judgment of S3's IED. Based on the above judgment, it can be seen that the IED of S3 is missed, and the CRFLA is area G. To sum up, the ERFLA is area A, and the EFIA is C.

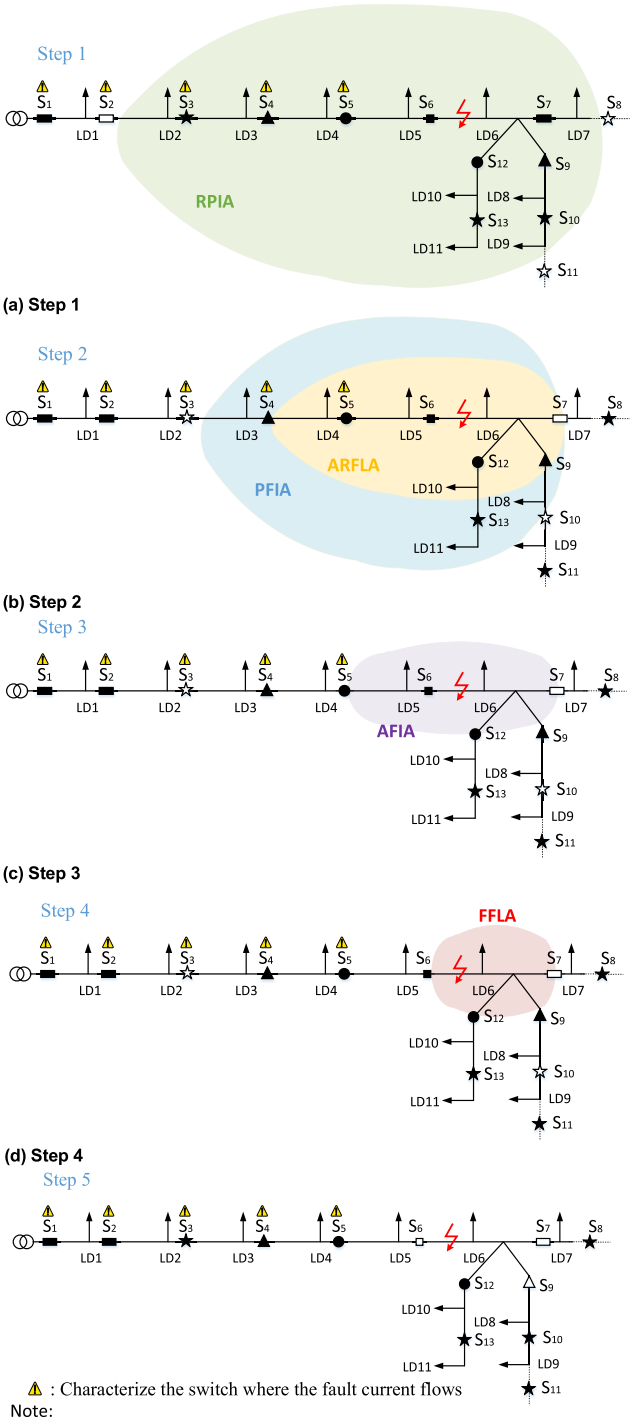
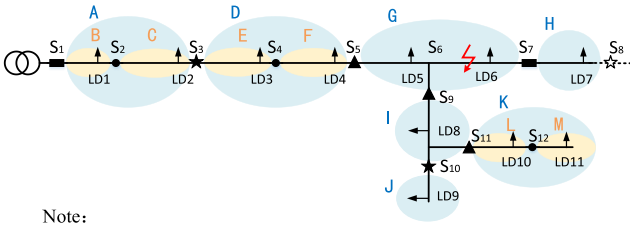


FIGURE 7. FLISR process of complex CPDS.

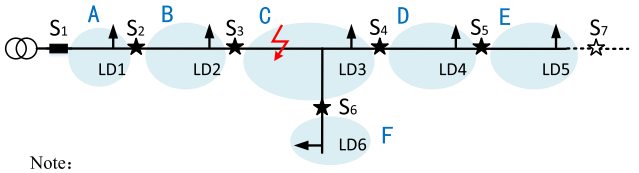


Note:
1)The rectangle, star, triangle, circle represents the CB, switch with RMC-IED, switch with RFI-IED, switch with LFI-IED respectively.
2)The black dotted line indicates the opposite line, and the switch on this line indicates the tie switch.

FIGURE 8. An example CPDS.

C) For example, if the RFI-IED of S9 in Fig. 8 is misjudged and other IEDs are normal, the master station staff will judge that the fault point is in area I. After the feeder inspection of area I, it is known that there is no fault in area I, then it can be judged as the IED misjudgment of S9 or the IED missing judgments of S10 and S11. Through the feeder inspection of area J and L, it is known that there is no fault in area J and L, so the IED of S10 and S11 is normal, and the IED of S9 is missed. It can be re-known that the CRFLA is area G. To sum up, the ERFLA is area I, and the EFIA is J and L.

D) For example, if the RFI-IED of S11 in Fig. 8 are misjudged and other IEDs are normal, the master station staff judges that the fault point is in area G or K, and suspects that S9's IED is missed or S11's IED is misjudged. After checking the LFI-IED of S12 in area K and inspecting the feeder of area L, it is known that there is no fault in area L, then it can be judged that there is misjudgment of S11's IED or missing judgment of S12's IED. Based on the above judgment, it can be seen that the IED of S11 is misjudged, and the CRFLA is area G. To sum up, the ERFLA is area K, and the EFIA is L.

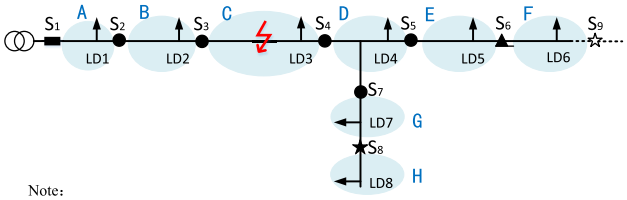


Note:
1)The rectangle, star represent the CB, switch with RMC-IED respectively.
2)The black filled and white filled switch indicates the closed and open state.

FIGURE 9. An example CPDS.

As shown in Fig. 9, the laws E-M about the impact of misjudgments or missing judgments of four types of remote Ass-IEDs on fault isolation is explained following.

E) For example, if the RMC-IED of S3 in Fig. 9 are missed and other IEDs are normal, the master station staff judges that the fault is in area B, so they control switches S2, S3 to open and S7 to closed remotely. But because the real fault area is area C, the relay protection of the opposite line acts in the process of transferring power supply. Through the remote signal of the IEDs of S4 and S5, it is known that area C has fault, so the staff control S4 to open remotely. In the above process, the switches S2-S4 and S7 are remotely controlled. Compared with the normal situation, the control of S2 is unnecessary, so t_1 increases t_{rmt}.



Note:
1)The rectangle, star, triangle, circle represent the CB, switch with RMC-IED, switch with RFI-IED, switch with LFI-IED respectively.
2)The black filled and white filled switch indicates the closed and open state.

FIGURE 10. An example CPDS.

F) In this cyber failure case, the master station staff judges that the fault is in the upstream area of the missed IED, and no switch can recover the loads upstream of the ERFLA, so the remote control action is not required. Compared with the normal situation that the staff control the switch with the missed IED remotely to restore upstream loads, t_1 reduces t_{rmt}.

G) For example, if the IED of S2 in Fig. 9 is missed and other IEDs are normal, the master station staff judges that the fault is in area A or C. When they are not sure which area the fault is in, they can only restore power to the area downstream of S4. Therefore, the S4 and S7 are controlled to be open and closed severally. Compared with the normal situation that the staff remotely control S3, S4 to open and control S7 to closed, t_1 decreases t_{rmt}.

TABLE 8. The reliability parameters of elements in the physical system.

Element	Failure rate (f/ yr)	Average repair time (hr)	Element	Failure rate (f/ yr)	Average repair time (hr)
Line	0.06	5	TS	0.002	2
Transformer	0.015	200	Fuse	0.002	3
CB	0.006	4	Load	0.007	11
SS	0.006	4			

H) For example, if the RMC-IED of S4 in Fig. 9 is misjudged and other IEDs are normal, the master station staff judges that the fault is in area D, so they remotely control switches S4, S5 to open and S7 to closed. However, since the real fault area is area C, the relay protection of this feeder acts again during the process of restoring the power supply upstream of the area D. Through the remote signal of the IEDs of S1-S3, it is known that the fault is in area C, so S3 is controlled to open remotely. In the above process, the switches S3-S5 and S7 are remotely controlled. Compared with the normal situation, the control of S5 is unnecessary, so t_1 increases t_{rmt}.

I) For example, if the RMC-IED of S6 in Fig. 9 is misjudged and other IEDs are normal, the master station staff judges that the fault is in area F, so they remotely control switch S6 to open in order to restore the loads upstream of

TABLE 9. The reliability parameters of elements in the cyber system.

Element	Module	Failure rate (f/ yr)	Average repair time (hr)
LFI-IED	Fault detection module	0.01	4
	Fault display module	0.01	4
RFI-IED	Fault detection module	0.01	4
	Communication transceiver module	0.01	4
RMC-IED	Fault detection module	0.01	4
	Communication transceiver module	0.01	4
	Electric control module	0.01	4
OLT	\	0.005	4
POS	\	0.005	4
ONU	\	0.005	4
SDH optical fiber	\	0.0008	12
EPON optical fiber	\	0.0008	12
SDH switch	\	0.006	12
Server	\	0.0013	8

TABLE 10. The parameters of fault handling time.

Time parameters	Value (hr)
The average time for remote operation of a switch with RMC-IED t_{rmt}	0.08333
The average time for the maintenance personnel traveling to the fault feeder site t_{21}	0.5
The average time to inspect the display of a LFI-IED t_{IED1}	0.1
The average time for patrolling per kilometer of feeder t_{ptl}	0.15
The average time for manually operating a switch t_{mnl}	0.25

S6. But since the real fault area is area C, the relay protection of this feeder acts again in the process of restoring the loads. Through the remote signal of S1-S5, it is known that area C is faulty, so S3, S4 are controlled to open and S7 is controlled to closed remotely. In the above process, the switches S3, S4, S6 and S7 are remotely controlled. Compared with the normal situation, the control of S6 is unnecessary, so t_1 increases t_{rmt}.

J) For example, if the IED of S5 in Fig. 9 is misjudged and other IEDs are normal, the master station staff judges that the fault is in area C or E. When the staff are not sure which area the fault is in, they can only restore power to the area upstream of S3, so S3 is controlled to open remotely. Compared with the normal situation that the staff remotely control S3, S4 to open and control S7 to closed, t_1 decreases $2t_{rmt}$.

K) In this cyber failure case, the main station staff judges that the fault is in two discontinuous areas, one of that is the remote area whose OutS is the switch with the missed IED. Therefore, the remote control of the upstream switch closest to the fault which should be operated in step 2 will be postponed to step 5, and t_{24} will increase t_{rmt} compared with the normal situation.

L) In this cyber failure case, the master station staff judges the fault in the remote area whose OutS is the switch with the missed IED. This area is the nearest upstream remote area of the fault. When there is no power transfer condition downstream of the switch with the missed IED, only the load recovery operation upstream of the ARFLA is considered in step 2. Therefore, the remote control of the upstream switch closest to the fault point that should be operated in step 2 is postponed to step 5. Compared with the normal situation, t_{24} increase t_{rmt}.

M) For example, if the RMC-IED of S5 in Fig. 9 is misjudged, and other IEDs are normal, the master station staff judges that the fault is in area C or E. S5 is sandwiched between area C and E, and when the staff is not sure which area the fault is in, step 2 will not remotely operate S5. There is transfer condition downstream of the fault area, and finally S5 will be operated to open remotely in order to restore the loads downstream of the fault, so t_{24} increase t_{rmt} compared with normal situation. Moreover, if there is no switch with RMC-IED belonging to this feeder at the downstream of area E, one power transfer operation is missing in step 2 compared with the normal situation, which will not be realized until step 5. Therefore, t_{24} increase $2t_{rmt}$ totally.

As shown in Fig. 10, the laws N-Q about the impact of misjudgments or missing judgments of four types of local Ass-IEDs on feeder inspection scope is explained following.

N) For example, if the LFI-IED of S3 in Fig. 10 is missed and other IEDs are normal, the onsite maintenance personnel judge that the fault is in area B. There is no fault point found after feeder inspection for area B, so it is judged that the IED of S2 is misjudged or the IED of S3 is missed. There is no fault point found after feeder inspection for area A upstream of area B, so it can be judged that the IED of S2 is normal, missing judgment occurs in the IED of S3. Then it can be known that the fault is in area C. To sum up, the EFIA is area A and B.

O) For example, if the LFI-IED of S2 in Fig. 10 is missed and other IEDs are normal, the onsite maintenance personnel judge that the fault is in area A or area C. The two areas need to be patrolled. After the feeder inspection, it is known that the fault is in area C. To sum up, the EFIA is area A.

P) For example, if the LFI-IED of S4 in Fig. 10 is misjudged and other IEDs are normal, the onsite maintenance personnel judge that the fault is in area D. There is no fault point found after feeder inspection for area D, so it is judged that the IED of S4 is misjudged or one of the IEDs of S5 and S7 is missed. After inspecting the areas E and G downstream of area D, no fault point was found, so the IEDs of S5 and S7 are normal. It can be judged that misjudgment occurs in the IED of S4, and the fault is in area C. To sum up, the EFIA is area D, E and G.

Q) For example, if the LFI-IED of S5 in Fig. 10 is misjudged and other IEDs are normal, the onsite maintenance personnel judge that the fault is in area C or area E. The two areas need to be patrolled. After the feeder inspection, it is known that the fault is in area C. To sum up, the EFIA is area E.

APPENDIX C

Tables 8, 9 and 10 here.

REFERENCES

[1] D. Xu, B. Zhou, Q. Wu, C. Y. Chung, C. Li, S. Huang, and S. Chen, "Integrated modelling and enhanced utilization of power-to-ammonia for high renewable penetrated multi-energy systems," *IEEE Trans. Power Syst.*, early access, Apr. 22, 2020, doi: 10.1109/TPWRS.2020.2989533.

[2] H. Wang, Z. Lei, X. Zhang, B. Zhou, and J. Peng, "A review of deep learning for renewable energy forecasting," *Energy Convers. Manage.*, vol. 198, Oct. 2019, Art. no. 111799.

[3] D. Xu, Q. Wu, B. Zhou, C. Li, L. Bai, and S. Huang, "Distributed multi-energy operation of coupled electricity, heating and natural gas networks," *IEEE Trans. Sustain. Energy*, early access, Dec. 23, 2019, doi: 10.1109/TSTE.2019.2961432.

[4] H. Wang, Y. Liu, B. Zhou, C. Li, G. Cao, N. Voropai, and E. Barakhtenko, "Taxonomy research of artificial intelligence for deterministic solar power forecasting," *Energy Convers. Manage.*, vol. 214, Jun. 2020, Art. no. 112909.

[5] B. Jimada-Ojuolape and J. Teh, "Impact of the integration of information and communication technology on power system reliability: A review," *IEEE Access*, vol. 8, pp. 24600–24615, 2020, doi: 10.1109/ACCESS.2020.2970598.

[6] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour, and A. Safdarian, "Impact of WAMS malfunction on power system reliability assessment," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1302–1309, Sep. 2012, doi: 10.1109/TSG.2012.2183397.

[7] M. Panteli and D. S. Kirschen, "Assessing the effect of failures in the information and communication infrastructure on power system reliability," in *Proc. IEEE/PES Power Syst. Conf. Exposit.*, Phoenix, AZ, USA, Mar. 2011, pp. 1–7, doi: 10.1109/PSCE.2011.5772565.

[8] B. Falahati and Y. Fu, "A study on interdependencies of cyber-power networks in smart grid applications," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–8, doi: 10.1109/ISGT.2012.6175593.

[9] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, Sep. 2012, doi: 10.1109/TSG.2012.2194520.

[10] B. Falahati and Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1677–1685, Jul. 2014, doi: 10.1109/TSG.2014.2310742.

[11] M. Heidari Kapourchali, M. Sepehry, and V. Aravinthan, "Fault detector and switch placement in cyber-enabled power distribution network," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 980–992, Mar. 2018, doi: 10.1109/TSG.2016.2573261.

[12] 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, doi: 10.1109/TPWRS.2018.2854642.

[13] J. Guo, W. Liu, F. R. Syed, and J. Zhang, "Reliability assessment of a cyber physical microgrid system in island mode," *CSEE J. Power Energy Syst.*, vol. 5, pp. 46–55, Mar. 2019, doi: 10.17775/CSEEJPES.2017.00770.

[14] C. Wang, T. Zhang, F. Luo, F. Li, and Y. Liu, "Impacts of cyber system on microgrid operational reliability," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 105–115, Jan. 2019, doi: 10.1109/TSG.2017.2732484.

[15] B. Chen, Z. Lu, and H. Zhou, "Reliability assessment of distribution network considering cyber attacks," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, Oct. 2018, pp. 1–6.

[16] Y. Zhang, Y. Xiang, and L. Wang, "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2343–2357, Sep. 2017.

[17] Z. Ding, Y. Xiang, and L. Wang, "Incorporating unidentifiable cyber-attacks into power system reliability assessment," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Aug. 2018, pp. 1–5.

[18] R. Guo, C. Qu, V. Vankayala, E. Crozier, S. Allen, and K. Adeleye, "Implementing self-healing distribution systems via fault location, isolation and service restoration," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, Vancouver, BC, Canada, May 2016, pp. 1–4, doi: 10.1109/CCECE.2016.7726671.

[19] G. Celli, E. Ghiani, F. Pilo, and G. G. Soma, "Reliability assessment in smart distribution networks," *Electric Power Syst. Res.*, vol. 104, pp. 164–175, Nov. 2013.

[20] M. R. Bhuiyan and R. N. Allan, "Modelling multistate problems in sequential simulation of power system reliability studies," *IEE Proc.-Gener., Transmiss. Distrib.*, vol. 142, no. 4, pp. 343–349, Jul. 1995, doi: 10.1049/ip-gtd:19951871.

[21] A. Ohuchi, M. Kurihara, and I. Kaji, "Implication theory and algorithm for reachability matrix model," *IEEE Trans. Syst., Man, Cybern.*, vol. 16, no. 4, pp. 610–616, Jul. 1986, doi: 10.1109/TSMC.1986.289267.

[22] Y. Wan, J. Cao, S. Zhang, G. Tu, C. Lu, X. Xu, and K. Li, "An integrated cyber-physical simulation environment for smart grid applications," *Tsinghua Sci. Technol.*, vol. 19, no. 2, pp. 133–143, Apr. 2014, doi: 10.1109/TST.2014.6787366.

[23] W. Zhang and J. He, "Statistical modeling and correlation analysis of end-to-end delay in wide area networks," in *Proc. 8th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw., Parallel/Distrib. Comput. (SNPD)*, Qingdao, China, Jul. 2007, pp. 968–973, doi: 10.1109/SNPD.2007.490.

[24] R. Billinton and S. Jonnavithula, "A test system for teaching overall power system reliability assessment," *IEEE Trans. Power Syst.*, vol. 11, no. 4, pp. 1670–1676, Nov. 1996, doi: 10.1109/59.544626.

[25] R. N. Allan, R. Billinton, I. Sjarief, L. Goel, and K. S. So, "A reliability test system for educational purposes-basic distribution system data and results," *IEEE Trans. Power Syst.*, vol. 6, no. 2, pp. 813–820, May 1991, doi: 10.1109/59.76730.

[26] D. Roberts, *Network Management Systems for Active Distribution Networks: A Feasibility Study*. London, U.K.: DTI, 2004.

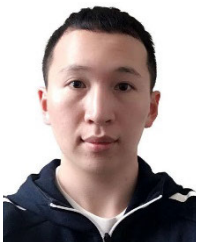
[27] L. Fengzhang, Y. Wentao, and Z. Tianyu, "Influence of distribution automation data transmission errors on power supply reliability of distribution system," *Autom. Electr. Power Syst.*, vol. 42, no. 19, pp. 10–17, 2018, doi: 10.7500/AEPS20170619006.

DAN LIN received the B.Eng. degree in electrical engineering from the South China University of Technology, Guangzhou, China, in 2018, where she is currently pursuing the M.S. degree with the School of Electric Power Engineering. Her research interests include distribution network planning and reliability assessment.

QIANJIN LIU (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in power plant engineering from the Huazhong University of Science and Technology, Wuhan, China, in 1989 and 1995, respectively. He is currently an Associate Professor with the College of Electric Power, South China University of Technology, Guangzhou, China. His research interests include distribution network operation control and its advanced application analysis and distribution network data fusion model and its information applications.

ZHUOHUAN LI received the B.S. degree in electrical engineering from the South China University of Technology, Guangzhou, China, in 2018, where he is currently pursuing the M.S. degree in electrical engineering with the School of Electric Power Engineering. His research interest includes optimal operation of power systems.

GUANGXUAN ZENG received the B.Eng. degree in electrical engineering from the South China University of Technology, Guangzhou, China, in 2017, where she is currently pursuing the M.S. degree with the School of Electric Power Engineering. Her research interest includes cyber-physical system reliability assessment.



ZIYAO WANG received the B.Eng. degree in electrical engineering from the South China University of Technology, Guangzhou, China, in 2019, where he is currently pursuing the M.S. degree with the School of Electric Power Engineering. His research interests include distribution planning and reliability assessment.

TAO YU (Member, IEEE) received the B.Eng. degree in electrical power system from Zhejiang University, Hangzhou, China, in 1996, the M.Eng. degree in hydroelectric engineering from Yunnan Polytechnic University, Kunming, China, in 1999, and the Ph.D. degree in electrical engineering from Tsinghua University, Beijing, China, in 2003. He is currently a Professor with the College of Electric Power, South China University of Technology, Guangzhou, China. His research interests include nonlinear and coordinated control theory, artificial intelligence techniques, and operation of power systems.

JUNXIAO ZHANG received the B.S. and M.S. degrees in electrical power system and automation from Wuhan University, Wuhan, China, in 2005. She is currently a Senior Engineer with the Grid Planning & Research Center, Guangdong Power Grid Company Ltd., CSG, Guangzhou, China. Her research interest includes distribution network planning.