Analytical Reliability Evaluation of Active Distribution Systems Considering Information Link Failures

Wenxia Liu, *Member, IEEE*, Zijian Lin, *Student Member, IEEE*, Lingfeng Wang, *Senior Member, IEEE*, Zhiqiang Wang, *Member, IEEE*, Hanyu Wang, *Student Member, IEEE*, and Qi Gong

***Abstract*—With the growing study on the active distribution network, an objective and efficient reliability evaluation method for such cyber-physical systems (CPS) is urgently needed. In this paper, first considering the cyber transmission performance, a new method is proposed for efficient evaluation of cyber link validity based on frequency-time domain transformation. In order to quantify the indirect interdependencies of cyber failures, an unresponsiveness probability model for switches is established. Then, an innovative method is proposed by combining the equivalent method and the minimal path method. Finally, a test system is established to verify the effectiveness of the proposed method. This study is instrumental in informing the efficient planning of contemporary CPS-based distribution networks.**

***Index Terms*—Active distribution networks, cyber physical systems, frequency-time domain transformation, reliability evaluation, transmission performance.**

NOMENCLATURE

a_i	The available rate of node *i*;
λ_i	The failure rate of node *i*;
μ_i	The repair rate of node *i*;
$a_{i,j}$	The available rate of line *i-j*;
$\lambda_{i,j}$	The failure rate of line *i-j*;
$\mu_{i,j}$	The repair rate of line *i-j*;
$P_{i,j}$	The validity probability of line *i-j*;
$A_{i,j}$	The available rate of the channel *i-j*;
$C_{i,j}$	The information error probability of the channel *i-j*;
$D_{i,j}$	The timely transmission probability of the channel *i-j*;
$\bar{C}_{i,j}$	The probability that the channel *i-j* transmits messages accurately;
$f_i^L(t)$	The delay probability density function of the node *i* in the time domain;
$f_{i,j}^L(t)$	The delay probability density function of the channel *i-j* in the time domain;
$F_i^L(s)$	The delay probability density function of the node *i* in the frequency domain;
$F_{i,j}^L(s)$	The delay probability density function of the channel *i-j* in the frequency domain;
$t_i(s)$	The validity of the cyber component *i* in the frequency domain;
$t_{i,j}(s)$	The validity of the line *i-j* in the frequency domain;
A	The cyber link validity;
T	The tolerance time for all message delays;
p_c	The probability of responsiveness;
$A_{sw,i}^M$,	The validity probability of monitoring message of sectionalizing switch *i*;
$A_{sw,i}^C$	The validity probability of control message of sectionalizing switch *i*;
$A_{sw,i}^F$	The validity probability of feedback message of sectionalizing switch *i*;
$p_{sw,i}^{ICT}$	The probability of fault isolation by the sectionalizing switch *i* upstream the fault;
p_{sw}^e	The probability that the sectionalizing switch can properly act;
$p_{sw,i}^C$	The probability that the sectionalizing switch would operate successfully;
$A_{t,i}^C$	The validity probability of the control message of the tie switch *i*;
p_t^e	The probability that the tie switch can correctly act;
$A_{q,PCC}^C$	The validity probabilities of PCC control message;
$A_{q,PCC}^F$	The validity probabilities of PCC feedback message;
p_{PCC}^e	The probability that the PCC switch can properly act;
p_{br}	The probability that the branch can be disconnected in time;
λ_f^{eq}	The equivalent failure rate of the branch *f*;
N	The number of divided areas according to the sectionalizing switches;
M	The number of sectionalizing switches on the branch;
r_j	The equivalent repair time in the downstream area of switch *j*;

Manuscript received May 11, 2019; revised October 12, 2019 and February 11, 2020; accepted April 28, 2020. Date of publication May 19, 2020; date of current version November 4, 2020. This work was supported by the National Key Research and Development Program of China under Award 2017YFB0903100. Paper no. TPWRS-00650-2019. *(Corresponding author: Wenxia Liu.)*

Wenxia Liu, Zijian Lin, Zhiqiang Wang, and Hanyu Wang are with the School of Electrical and Electronic Engineering, and also with the State Key Laboratory for Alternate Electrical Power System with Renewable Energy Sources, North China Electric Power University, Beijing, China (e-mail: liuwenxia001@163.com; 9128743@qq.com; wwwgode@163.com; wanghanyu0802@163.com).

Lingfeng Wang is with the Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211 USA (e-mail: l.f.wang@ieee.org).

Qi Gong is with the State Grid Wuxi Electric Power Company, Wuxi, China (e-mail: gongqihen@163.com).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRS.2020.2995180

t_{sw} The switching time;
λ_n^L The failure rate of the customer n;
r_n^L The repair time of the customer n;
λ_i^{eq} The equivalent failure rate of the non-minimal path j;
r_i^{eq} The repair time of the non-minimal path j;
λ_j The failure rate of the minimal path j;
r_j The repair time of the minimal path j;
$A_{q,DG}^M$ The validity probabilities of monitoring message of DG in the island q;
$A_{q,DG}^C$ The validity probabilities of control message of DG in the island q;
$A_{q,DG}^F$ The validity probabilities of feedback message of DG in the island q;
$A_{q,ES}^M$ The validity probabilities of monitoring message of batteries;
$A_{q,ES}^C$ The validity probabilities of control message of batteries;
$A_{q,ES}^F$ The validity probabilities of feedback message of batteries;
p_q^p The validity probabilities depending on the operating strategy and the capacity of DG;
$t_{is,q}$ The switching time of the intentionally formed island;
M_{up} The sum of the component or equivalent branch of the minimum path;
$p_{t,i}^c$ The probabilities that the tie switches are in a normal state;
$p_{t,sw}^c$ The probabilities that the sectionalizing switches are in a normal state;
p_t The probabilities that the load transfer could be successfully performed;
p_t^p The validity probabilities depending on the operating strategy of the transferable range;
N_{up} The sum of the minimal-path component and the non-minimal-path branch.

I. Introduction

THE development of active distribution systems is to enable the coordinated control of a variety of distributed energy resources by integrating advanced intelligent measurement, information, communication and control technologies. It aims to achieve higher penetration of renewable energy resources, improve the asset utilization, and boost the power system reliability. The major functions of the active distribution system dealt with in this study include: 1) optimizing distributed generations (DGs) under normal circumstances; and 2) realizing the fault location, isolation and recovery under the failure circumstances [1]. The typical structure of an active distribution system is shown in Fig. 1.

In the process of fault handling, the difference between the active distribution system and the traditional distribution system is listed as follows:

1) Monitoring and control information is used to realize the automation of fault location, isolation and load transfer, which improves the efficiency of fault handling and reduces the time of power failure.
2) In the process of fault recovery, DGs and energy storage system are allowed to form an island to supply power to the faulted area in order to reduce the number of customers being affected.
3) The automation of the whole process relies on the cyber system. Once the cyber system fails, the fault location and the control scheme will be inaccurate.

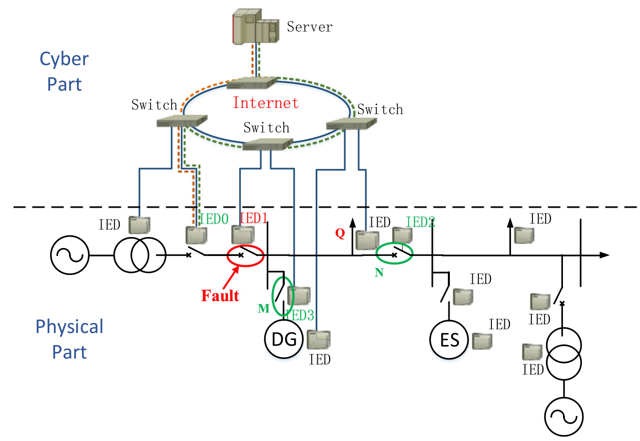

Fig. 1. The Typical Structure of an Active Distribution System.

Here is an illustrative example. If IED1 detects a circuit breaker fault of distribution network, to isolate the faulted area, IED0 and IED2 send out a control signal to open the circuit breaker, which results in the power outage of customers Q. Later, IED3 sends out a switch control command to close the switch to restore the power supply to customers Q.

After the concept of the Cyber Physical System (CPS) was proposed in 2006, the research of CPS reliability has gone through three research stages. In the first stage, a typical cyber system structure was established, and the coupling relationship was explored between the cyber system and the physical system [2], [3]. Then the direct and indirect relationships between cyber failures and physical systems were studied in [4]–[6]. In the second stage, the study on the interdependencies between cyber and physical systems was conducted under various situations. Specifically, the impact of cyber component faults and the change of the network topology on physical components was analyzed based on the direct interdependency, and the reliability model considering cyber failures was developed [5]–[11]. With the deepened research, the cyber system configuration is evolving from simple [12], [13] to more complex topologies [5], [14].

The recent research can be regarded as the third stage for the research on this topic, which mainly focuses on more detailed cyber modeling and deeper analysis. First, the influence of information transmission performance, especially the data transmission delay on the CPS reliability, is considered [15]–[18]. Reference [19] points out that the transmission performance is closely related to the nodal processing capability and the study establishes a cyber node transmission delay model that is related to the network load rate. However, due to the huge computational cost of the Monte Carlo simulation method, its application to the fine-grained CPS reliability evaluation is limited. Second, the coupling relationship analysis of CPS has gradually evolved from direct to indirect interdependency studies in recent years. It is obvious that the control function plays a pivotal role in these interactions, so the distribution system self-healing capability demanding diverse control functions has become an emergent topic more recently [18]–[21]. For example, automation with a centralized telecontrol system is researched in [18]. Indeed, fault recovery in active distribution networks should consider the contribution of micro sources and the load transfer mechanism. However, with the grid-connection of distributed generators, the low efficiency of simulation methods becomes more serious, because the intentional island should be considered when the fault occurs and the fault state analysis is more complicated than the traditional power network. Therefore, it is urgent to explore an efficient method to meet the actual computing requirements of power grid planning and operations in the CPS reliability evaluation. So far, some research has been performed using analytical methods to evaluate the distribution automation fault handling processes. In [20], the availability of the signal transmission path is used as the probability of fault isolation. However, its modeling process is somewhat simplified, in which only the random failure of cyber components is considered, ignoring the contribution of micro sources to fault recovery.

Therefore, this paper proposes a reliability analysis method that considers a detailed model of cyber systems to improve the efficiency of the algorithm. First, based on consideration of the cyber transmission performance, a new method for the rapid evaluation of cyber link validity is proposed using frequency-time domain transformation. Then, based on the indirect impact of cyber failure on the distribution network [4], [5], a reliability model is established for the distribution network with various switches. In order to quantify the impact of cyber failure on fault self-healing, intentional islanding and load transferring, an analytical method for the reliability analysis is proposed with the combination of the network equivalent equalization and the minimal path method. The method this paper proposed can provide a technical foundation for the planning and design of cyber systems in modern power distribution grids.

The procedure of the proposed reliability evaluation method is illustrated by Fig. 2. In Section II, the validity of information link is modeled, and an analytical method is proposed to solve the validity of information link by frequency/time domain conversion. In Section III, the reliability of the switching components is modeled and the validity of the information link is equivalent to the switching component. In Section IV, the reliability calculation method of distribution network combined with the upward equivalence and the minimal path is proposed, and the case studies are performed in Section V.

The key technical contributions made in this study can be summarized as follows. Firstly, in the existing research on the cyber physical systems, the component modeling of cyber physical systems usually only considers the equipment failure. However, component failure, transmission delay and information error are considered comprehensively in this paper, and then the information link validity model is formed. Besides, the Laplace transform and inverse transform are used in the calculation of transmission delay, which improves the calculation efficiency greatly. Secondly, in studying the cyber physical interactions in CPSs, the influence of cyber faults on the physical system performance can be divided into direct and indirect types. The direct influence means the physical components are unavailable caused by cyber faults directly, and it is modeled by superimposing cyber failures on the failure rates of physical components. While the indirect influence refers to the functions of physical components influenced by the cyber performance. The indirect influence is usually modeled qualitatively in the existing research, but it is modeled quantitatively in this study. Thirdly, based on the switch model and the information link model affected by cyber failures, the network equivalent method is combined with the shortest path method. In addition, considering the island-forming probability, the paper establishes an analytical model for reliability calculation of ordinary customers, and customers with the intentional island and load transfer. An analytical method for distribution network reliability evaluation is developed considering the indirect impact of cyber system failures. Lastly, compared with [19], the calculation time is saved by 86% in the proposed method, and the calculation results are approximately the same under the same case and computer configuration. Due to the large scale of practical distribution networks (e.g., a distribution entity usually manages hundreds of medium-voltage feeders), the corresponding reliability indices calculation demands tremendous computing burden. Therefore, the proposed analytical method can be used to enable efficient calculations of reliability indices for real-world applications.

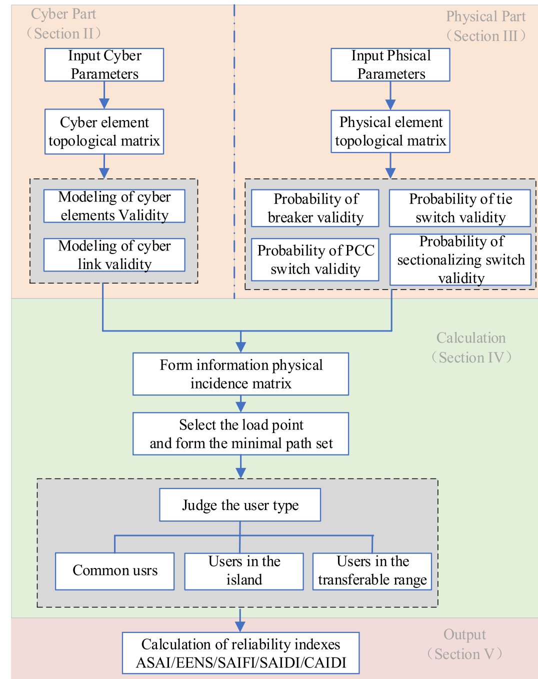

Fig. 2. The Procedure of the Proposed Reliability Evaluation Method.

II. Modeling and Evaluation of Cyber Link Validity

A. Modeling of Cyber Components

The communication interruption caused by cyber component failures, the communication delay caused by the excessive network load, and the information error caused by information transmission errors can invalidate the information for monitoring

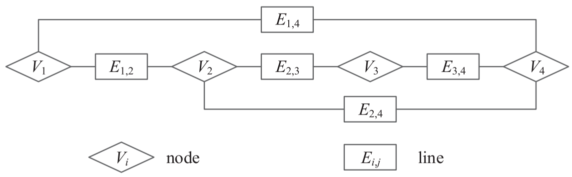

Fig. 3. Undigraph of Cyber System.

and control transmitted through the cyber link [23], [24]. Therefore, this paper copes with the cyber link validity issue from three major aspects: fault characteristics, delay characteristics, and error characteristics.

Cyber systems mainly include communication nodes (e.g., intelligent electronic devices (IEDs), switches, and servers) and communication lines. Thus, the cyber network can be abstracted into an undirected graph $G(V_i,\ E_{i,j})$ as shown in Fig. 1, and the communication node model $V_i = \{a_i, f_i(t), c_i\}$ can be represented by a set of node availabilities, delay probability density functions, and error probabilities. Similarly, the communication line model $E_{i,j} = \{a_{i,j}, f_{i,j}(t), c_{i,j}\}$ can also be represented by a set of line availabilities, delay probability density functions, and information error probabilities. The availability can be expressed as follows:

$$\begin{cases} a_i = \frac{\mu_i}{\lambda_i+\mu_i} \\ a_{i,j} = \frac{\mu_{i,j}}{\lambda_{i,j}+\mu_{i,j}} \end{cases} \tag{1}$$

where a_i and $a_{i,j}$ represent the available rate of node *i* and the line *i-j*, *i, j*∈N, respectively.

In a cyber network, the cyber link refers to a transmission circuit between two nodes, while the cyber transmission channel refers to a specific transmission path during information transmission, which consists of multiple nodal devices and transmission lines. In other words, there are several transmission channels to ensure the reliable information transmission in an end-to-end link communication. As shown in Fig. 3, the cyber link between V_1 and V_4 is composed of three cyber transmission channels that mutually back up each other, such as $\{V_1, E_{1,4}, V_4\}$, $\{V_1, E_{1,2}, V_2, E_{2,3}, V_3, E_{3,4}, V_4\}$ and $\{V_1, E_{1,2}, V_2, E_{2,4}, V_4\}$. Generally, the cyber link validity comprehensively reflects the device reliability and the backup mechanism of multiple transmission channels.

B. Modeling of Transmission Channel

For a certain transmission channel *i-j*, if one component is out of service, or the transmission delay exceeds the system threshold, or an information error occurs, the transmission channel will become invalid. Notably, the term of "validity" means not only the physical equipment of CPS should be "available" but also the transmission delay and error probability need to meet the system requirements. In other words, any event of information loss, delay and error is considered "invalid." Therefore, the channel validity can be expressed as the product of the availability, the probability of timely message transmission and the probability of accurate messaging:

$$P_{i,j} = A_{i,j} \cdot (1 - C_{i,j}) \cdot D_{i,j} \tag{2}$$

where $A_{i,j}$ is the available rate of the channel *i-j*, $C_{i,j}$ is the information error probability of the channel *i-j*, and $D_{i,j}$ is the timely transmission probability of the channel *i-j*, which can be expressed as the integral of the channel delay probability density function *fL i, j*(*t*):

$$D_{i,j}(x) = \int_{-\infty}^{x} f_{i,j}^{L}(t)dt \tag{3}$$

where *x* is the default delay threshold. Once the transmission delay exceeds *x*, the message is invalid.

It is assumed that for a certain channel, the whole channel would fail to transmit messages if one component is out of service, and the message will be transmitted by the standby channel unless all channels in the information link fail. The availability of the channel can be treated as a typical series reliability model, and the availability can be expressed as follows:

$$A_{i,j} = a_j \cdot \prod_{k=i}^{j-1} a_k \cdot a_{k,k+1} \tag{4}$$

Besides, the communication error of components is independent of each other. Once a component has a communication error, the message transmission will go wrong. For convenience of illustration, let$\bar{C}_{i,j}$ indicate the probability that the channel *i-j* transmits messages inaccurately. The probability that the message transmission is not erroneous can be represented by a series model as follows:

$$\bar{C}_{i,j} = \bar{c}_j \cdot \prod_{k=i}^{j-1} \bar{c}_k \cdot \bar{c}_{k,k+1} \tag{5}$$

where $\bar{c}_k$ and $\bar{c}_{k,k+1}$ are the probabilities that no communication error occurs in node *k* and line *k*-*k*+1, respectively.

In addition, the delay of the transmission channel is closely related to the delay characteristics of each component through which the message passes. However, discussions about the failure of protocols and their fault tolerant capabilities are out of the scope of this paper. The delay probability density function should be the convolution of the respective delay probability density functions of the components; that is,

$$f_{i,j}^{L}(t) = f_i(t) * f_{i,i+1}(t) * \cdots * f_j(t) \tag{6}$$

However, the calculation of a multiplication convolution is very complicated and time-consuming. If the frequency domain function is used to describe the delay density function, the end-to-end link delay distribution would be the product of the frequency domain functions of the components [25], which can achieve fast calculation of the cyber link delay distribution function, as shown in (7).

$$\mathscr{L}[f_i(t) * \cdots * f_j(t)] = F_j \cdot \prod_{k=i}^{j-1} F_k \cdot F_{k,k+1} = F_{i,j}^{L}(s) \tag{7}$$

Therefore, the delay distribution time domain expression can be transformed into a frequency domain expression by Laplace Transform at first in the cyber delay calculation. Expression (2) can be rewritten as follows:

$$P_{i,j}(x) = \int_{-\infty}^{x} \mathscr{L}^{-1}[A_{i,j} \cdot \bar{C}_{i,j} \cdot F_{i,j}^{L}(s)]dt \tag{8}$$

The concept of validity is defined to characterize the fault, error and delay characteristics of a cyber link or channel, and it can be mathematically expressed as follows:

$$T_{i,j}(s) = A_{i,j} \cdot \bar{C}_{i,j} \cdot F_{i,j}^{L}(s) \tag{9}$$

If the concept of validity is extended to each component, we have:

$$\begin{cases} t_i(s) = a_i \cdot \bar{c}_i \cdot F_i(s) \\ t_{i,j}(s) = a_{i,j} \cdot \bar{c}_{i,j} \cdot F_{i,j}(s) \end{cases} \tag{10}$$

where $t_i(s)$ and $t_{i,j}(s)$ represent the validity of the cyber component *i* and cyber line *i-j*, respectively.

According to (4)–(7), the validity of the cyber channel can be expressed as the product of the validity of all components that constitute the channel.

$$T_{i,j}(s) = t_j(s) \cdot \prod_{k=i}^{j-1} t_k(s) \cdot t_{k,k+1}(s) \tag{11}$$

C. The Solution Method of Cyber Link Validity

In an actual network, there are multiple cyber channels between two nodes, the components in the same channel are connected in series, and different cyber channels back up each other. Therefore, the following method can be used to analyze the validity characteristics of the cyber link from *m* to *n*:

1) Transforming the time-domain distribution function to the frequency domain using Laplace Transform;
2) Solving all cyber channels between *m* and *n* using a depth-first or breadth-first search algorithm;
3) Generally, validity features a typical series structure for a certain cyber channel, which can be calculated by (11);
4) For the *k*-th cyber channels of the link from *m* to *n*, the validity of the link between *m* to *n* can be calculated by

$$T_{m,n}(s) = \min\{T_{m,n,1}(s), \ldots, T_{m,n,k}(s)\} \tag{12}$$

where min $\{T_{m,n,1}(s), \ldots, T_{m,n,i}(s), \ldots, T_{m,n,k}(s)\}$ can be obtained by comparing with the expected value of $T_{m,n,i(s)}$.

5) The probability density function of validity can be obtained by performing the Laplace Inverse Transformation on the frequency domain characteristics.
6) In order to ensure the timeliness of message transmission, CPS has an upper bound of tolerance (denoted as *T*) for all message delays. Therefore, the validity probability of the current cyber link can be obtained by

$$A = P(x < T) = \int_{-\infty}^{T} \mathscr{L}^{-1}[T_{m,n}(s)]dt \tag{13}$$

Theoretically, the message validity can be regarded as the cyber link validity, and the validity probability of the cyber link can be regarded as the validity probability of the message transmitted by the cyber link. For a certain physical component, end-to-end cyber links can be divided into uplink and downlink, and the uplink and downlink are in the same information link and the cyber components are the same. During a failure event, the transmission interval of monitoring (uplink), control (downlink) and control feedback message (uplink) is short, and the successful transmission of messages for these three actions depends on the validity of the cyber link. Thus, the validity probability of these three types of message transmission could be considered identical which is equal to the validity probability of the cyber link.

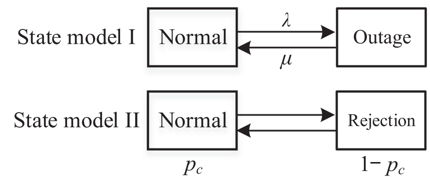

Fig. 4. Simplified Switch State Space.

III. Modeling of Probability of Switch Unresponsiveness

During the fault clearing process in the active distribution network, the sectionalizing switch, the tie switch, and the Point of Common Coupling (PCC) of the intentional island all need to communicate with the control center to update the monitoring message, receive instructions, and report the execution of the instructions. Thus, the self-healing sequence from the control center can be accomplished only when the physical components operate normally and the associated cyber link is in service. What's more, all the control messages cannot be transmitted properly if the server fails – in this case, the whole cyber-physical system could be considered to be invalid.

Generally, the cyber component is equipped with an Uninterruptible Power System (UPS), so the physical fault has little impact on the cyber system. Thus, the interaction of CPS is mainly related to the influence of cyber faults on the self-healing process.

If the monitoring message of the sectionalizing switch fails, it will affect the judgment of the control center on the current system state. Therefore, the sectionalizing switch without being monitored cannot participate in the self-healing process. Besides, if the control message of any switch fails to be transmitted, the switch will not operate successfully. If the feedback message fails to be transmitted for the switch that has successfully isolated the fault, the control center cannot confirm whether the switch has successfully completed fault isolation. As long as the sectionalizing switch fails to act due to the cyber invalidity, it can be regarded as a switch "unresponsiveness" event caused by message transmission failures. For this reason, there should be a "unresponsive state" besides the "normal state" and "outage state," which is used to indicate that the switch is in a normal state but cannot respond properly. Neglecting the situation of very low probability where "unresponsive state" and "outage state" occur simultaneously, the state space of the switch statuses can be described by the two-state models as shown in Fig. 4.

State transition probability can be used to characterize the "unresponsive state," that is, the probability of unresponsiveness is $1 - p_c$. The reason a switch becomes unresponsive is not only due to the invalidity of the switch's functional commands, but also the defect of the switch itself. Actually, different types of switches require different types of messages to perform their functions. For example, the PCC switch only requires the control message, while the sectionalizing switch also requires the monitoring message. Therefore, a detailed analysis of each type of switch needs to be performed.

A. Probability of Unresponsive Breaker

As a typical switch of the distribution network, the breaker must disconnect the branch in time when a fault occurs. Being consistent with the traditional power grid, the breaker can be operated without the communication. However, the drive module between the breaker detection, calculation and action may also malfunction, which could cause the failure of the switch. This type of failure should be classified as a secondary system failure, so the probability of the unresponsive breaker p_{br} is due to its own design and structural defects.

B. Probability of Unresponsive Sectionalizing Switch

The message uploaded by sectionalizing switches is an important basis for fault localization. If the monitoring message of one sectionalizing switch fails, the control center can only use the monitoring message of its upstream sectionalizing switch to determine the fault location. This sectionalizing switch would not be adopted during the self-healing process, which can cause the range of fault isolation to expand. After completing the fault location task, the control center will assign a control command to the switch whose monitoring message is valid, which is the closest to the fault point. In this way, the fault can be isolated, and the control center can be informed by the feedback of the switch about whether the fault can be successfully isolated. Therefore, if the control or the control feedback message fails to be properly transmitted, the control center will mistakenly believe that the fault has not been successfully isolated, and then issue the control commands to the upstream switch one by one sequentially until the fault is isolated successfully. During a failure event, the uploading of monitoring messages, the issuing of control commands, or the uploading of control feedback messages could be invalid due to the cyber random faults (e.g., delay and error code) caused by packet loss. Only when all three actions are successful in this process, the fault handling can be performed correctly. Therefore, these three activities are considered independent. As a consequence, the probability of fault isolation by the fault upstream switch *i* and the confirmation of the control center is the product of the validity probability of monitoring message $A^M_{sw,i}$, control message $A^C_{sw,i}$, and control feedback message $A^F_{sw,i}$.

$$p^{ICT}_{sw,i} = A^M_{sw,i} \cdot A^C_{sw,i} \cdot A^F_{sw,i} \tag{14}$$

Similar to the breaker, there is still a probability of unresponsiveness after a sectionalizing switch receives the control command due to the design defect of the component itself. So the probability that the sectionalizing switch would operate successfully can be expressed as follows:

$$p^c_{sw,i} = p^e_{sw} \cdot p^{ICT}_{sw,i} = p^e_{sw} \cdot A^M_{sw,i} \cdot A^C_{sw,i} \cdot A^F_{sw,i} \tag{15}$$

where p^e_{sw} is the probability that the sectionalizing switch can properly act when receiving control commands.

C. Probability of Unresponsive Tie Switch

For a load transferring range with constant users after the control center finds the position of the fault range through the monitoring message, if the upstream sectionalizing switch of the transferring range is successfully switched, the control center will send a control message to the tie switch to accomplish load transferring. Once the tie switch properly acts, the load can be successfully restored by the tie line. Therefore, the probability that the tie switch *i* would operate successfully can be expressed as follows:

$$p^c_{t,i} = p^e_t \cdot A^C_{t,i} \tag{16}$$

where $A^C_{t,i}$ is the validity probability of the control message of the tie switch *i* in the transferring range *t*, and p^e_t is the probability that the tie switch can correctly act when receiving control commands.

D. Probability of Unresponsive PCC Switch

Generally, the PCC can work as a switch to disconnect the intentional islanding from the distribution network. Before switching to the islanded operation mode, the control center needs to send a control message to the PCC at first to form an island. After receiving the control feedback message confirming that the intentional island is already in operation, the command of the islanding operation mode can be sent to the micro source. Therefore, the probability that the PCC can successfully disconnect the island from the distribution network is expressed as follows:

$$p^c_{q,PCC} = A^C_{q,PCC} \cdot A^F_{q,PCC} \cdot p^e_{PCC} \tag{17}$$

where $A^C_{q,PCC}$ and $A^F_{q,PCC}$ are the validity probabilities of PCC control and the control feedback message respectively, and p^e_{PCC} is the probability that the PCC switch can properly act when receiving the control commands.

IV. An Improved Minimal Path Method of Distribution Network Validity

A. Method Introduction

Based on the characteristics of the active distribution network, an improved minimal path method is proposed in this study. First, the reliability parameter of the branch is upward equivalent to the head node of the branch by means of the network equivalent method. Next, the minimal path method is adopted to calculate the reliability of customers, as shown in Fig. 5.

The network upward equivalence method uses the equivalent node connected in series at the head of the branch to reflect the influence of the upstream branch. It is convenient to quantify the fault pervasion resulting from the switch unresponsiveness by using the upward equivalence, which can reflect the impact of the fault isolation function of branch switches to the trunk line layer by layer. However, the differences between the method proposed by this paper and the traditional network equivalent approach mainly lie in the two aspects. On the one hand, the cyber fault is

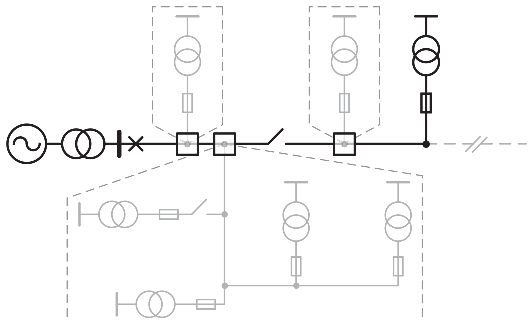

Fig. 5. Improved Minimal Path Method

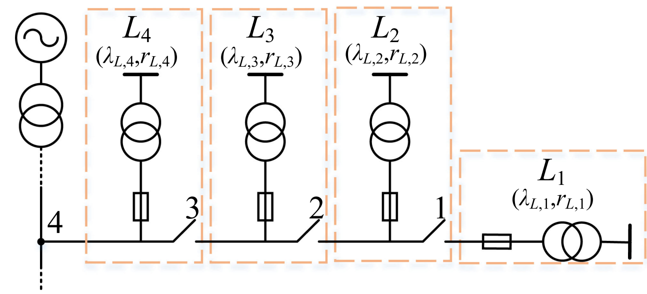

Fig. 6. Branch Division of Distribution Network.

considered by using unresponsiveness probability. On the other hand, the equivalent mean repair time of the switch component during the upward equivalent process is corrected by this paper, and it is regarded as the expectation of the equivalent repair time in the normal and outage state of the switch operation, rather than the switching time of the traditional distribution network [26]. In addition, a calculation method of the equivalent repair time considering multi-switch participation in fault isolation is proposed. Meanwhile, the contribution of the tie line and the intentionally formed island is considered when using the minimal path method for reliability calculation. Finally, the probability of the load transfer and the islanded operation is calculated according to the validity probability of the micro source and the probability of the unresponsive switch.

B. The Upward Equivalence of the Branch

Although any failure on the branch may spread to the upstream area, the branch can be disconnected in time with a certain probability p_{br} after detecting the fault current, since the breaker does not require the information of the control center. So the equivalent failure rate for the feeder *f* with the breaker at the head can be expressed as follows:

$$\lambda_f^{eq} = (1 - p_{br}) \sum_{i=1}^{N_f} \lambda_i \tag{18}$$

where λ_f^{eq} is the equivalent failure rate of the branch *f*, and λ_i is the failure rate of the component on the branch or on the downstream branch.

Only considering physical faults, it is assumed that the switches could be restored manually. In other words, the equivalent repair time of the failure switch in the downstream is the switching time, or the sum of the switching time and the manual operation time. This kind of handling method cannot reflect the actual self-healing process of the distribution network. Therefore, this paper proposes the concept termed switch equivalent repair time:

$$\begin{aligned} \mathrm{r}_f^{\mathrm{eq}} &= p_{br} \cdot t_{br} + \frac{U_f^{eq}}{\lambda_f^{eq}} \\ &= p_{br} \cdot t_{br} + \frac{\sum_{i=1}^{N_f} \lambda_i r_i}{(1 - p_{br}) \sum_{i=1}^{N_f} \lambda_i} \end{aligned} \tag{19}$$

where r_i is the repair time of the component on the branch or the downstream branch. It means that the equivalent repair time of the switch is the expectation of the switching time t_{br} and the equivalent repair time of the downstream switches.

In addition, all the upstream switches are likely to isolate the fault. In a branch with sectionalizing switches, as shown in Fig. 6, the branch can be divided into *N* areas according to the sectionalizing switches. Once a fault occurs, the upstream sectionalizing switches will try to isolate the fault under the remote command. Only when the upstream segment switches can operate reliably can the downstream segment be normally isolated from faults. Based on (18), the failure rate of the downstream switch is:

$$\lambda_{down} = \lambda_{L,i-1} \cdot \prod_{j=i}^{M} (1 - p_{sw,j}^{c}) \tag{20}$$

Therefore, the equivalent failure rate of the branch can be expressed as follows:

$$\lambda_f^{\mathrm{eq}} = \sum \lambda_{down} = \sum_{i=2}^{N} \left[\lambda_{L,i-1} \prod_{j=i-1}^{M} (1 - p_{\mathrm{sw},j}^{\mathrm{c}}) \right] \tag{21}$$

where *M* is the number of sectionalizing switches on the branch.

For the fault in the downstream range of the switch *j*, the repair time of the upstream component is the switching time t_{sw} when the switch successfully isolates the fault. Otherwise, it will isolate the area until the branch breaker or branch node. Therefore, the equivalent repair time of the downstream area of switch *j* is expressed below:

$$r_{L,j}^{eq} = \sum_{i=j}^{M} \left[p_{sw,i}^{c} \prod_{k=j}^{i-1} (1 - p_{sw,k}^{c}) \right] \cdot t_{sw} + \prod_{i=0}^{M-j} (1 - p_{sw,j+i}^{c}) r_j \tag{22}$$

$$r_j = \frac{1}{\sum_{i=1}^{j} \lambda_{L,i}} \left(\lambda_{L,j} r_{L,j} + \sum_{k=1}^{j-1} \lambda_{L,k} \cdot r_{L,j-1}^{eq} \right) \tag{23}$$

where r_j is the equivalent repair time in the downstream area of switch *j*.

C. Evaluation Method of Reliability Based on Minimal Path

According to the relationship of the customers and the power source, the customers can be divided into three types in the distribution network: common customers, customers within the transferable range, and customers in the intentionally islanded area.

1) Reliability Evaluation of Common Customers: Common customers constitute the majority in the distribution network, and the minimal path between customers and the main power source can be obtained directly. Therefore, the failure rate and the average repair time of common user *n* can be expressed as follows:

$$\lambda_n^L = \sum_{i=1}^{N_e} \lambda_i^{eq} + \sum_{j=1}^{M_d} \lambda_j \tag{24}$$

$$r_n^L = \frac{1}{\lambda_n^L} \left(\sum_{i=1}^{N_e} \lambda_i^{eq} r_i^{eq} + \sum_{j=1}^{M_d} \lambda_j r_j \right) \tag{25}$$

where λ_n^L and r_n^L are the failure rate and the repair time of the customer *n*; λ_i^{eq} and r_i^{eq} are the equivalent failure rate and the repair time of the non-minimal path; λ_j is the failure rate of the component; and r_j is the repair time of the minimal path.

2) Reliability Evaluation Of Customers in The Intentionally Formed Island: The micro source requires the information of the control center so as to be operated properly, so it is necessary that the monitoring, control, and the control feedback messages of the micro source should remain valid. Therefore, the probability that the DG and the batteries work properly can be expressed as follows:

$$\begin{cases} p_{q,DG}^c = A_{q,DG}^M \cdot A_{q,DG}^C \cdot A_{q,DG}^F \\ p_{q,ES}^c = A_{q,ES}^M \cdot A_{q,ES}^C \cdot A_{q,ES}^F \end{cases} \tag{26}$$

where $A_{q,DG}^M$, $A_{q,DG}^C$ and $A_{q,DG}^F$ are the validity probabilities of monitoring, control, and control feedback messages of DG in the island *q,* respectively; and $A_{q,ES}^M$, $A_{q,ES}^C$ and $A_{q,ES}^F$ are the validity probabilities of monitoring, control, and control feedback messages of batteries, respectively.

In addition, the probability that the island can be intentionally formed and operated stably is not only related to the probability that the PCC could disconnect the distribution network successfully, but also related to the probability that the customers can be supplied by the intentionally formed island. Therefore, this probability can be expressed as follows:

$$p_q = p_{q,ES}^c \cdot p_{q,DG}^c \cdot p_{q,PCC}^c \cdot p_q^p \tag{27}$$

where p_q^p depends on the operating strategy and the capacity of DG [22].

The failure rate of customer *n* in the intentionally formed island can be expressed as follows:

$$\lambda_n^L = (1 - p_q) \sum_{i=1}^{M_{up}} \lambda_i + \lambda_{q,n}^{eq} \tag{28}$$

When a fault occurs outside the intentionally formed island, the average repair time of customers in the intentionally formed island is the switching time $t_{is,q}$ if the intentionally formed island *q* can be successfully converted to the islanded mode. Otherwise, the repair time is equivalent to that of the outside intentionally formed island, which can be expressed as follows:

$$r_{n,up}^L = (1 - p_q) \cdot \frac{1}{\sum_{i=1}^{M_{up}} \lambda_i} \cdot \sum_{i=1}^{M_{up}} \lambda_i r_i + p_q \cdot t_{is,q} \tag{29}$$

Consequently, the average repair time of customer *n* is as follows:

$$\begin{aligned} r_n^L &= \frac{1}{\lambda_n^L} \left(\sum_{i=1}^{M_{up}} \lambda_i \cdot r_{n,up}^L + \lambda_{q,n}^{eq} r_{q,n}^{eq} \right) \\ &= \frac{1}{\lambda_n^L} \left[(1 - p_q) \cdot \sum_{i=1}^{M_{up}} \lambda_i r_i + \sum_{i=1}^{M_{up}} \lambda_i \cdot p_q \cdot t_{is,q} + \lambda_{q,n}^{eq} r_{q,n}^{eq} \right] \end{aligned} \tag{30}$$

where λ_n^L and r_n^L are the failure rate and repair time of customer *n*; λ_i and r_i are the equivalent failure rate and the repair time of the component or branch located in the minimum path between the island *q* and the main power source; M_{up} is the sum of the component or equivalent branch of the minimum path; and $\lambda_{q,n}^{eq}$ and $r_{q,n}^{eq}$ are the equivalent failure rate and repair time from customer *n* to PCC.

3) Reliability Evaluation of User in Transferable Range: Since the tie line can be used as the second power source of the distribution network, the customers in the transferring area can be supplied when there is a fault in the minimum path outside the transferring area. The premise of the load transferring is that the tie switch and the sectionalizing switch of the transferring area could operate properly. Therefore, the probability that the load transfer could be successfully performed is:

$$p_t = p_{t,i}^c \cdot p_{t,sw}^c \cdot p_t^p \tag{31}$$

where $p_{t,i}^c$ and $p_{t,sw}^c$ are the probabilities that the tie switch and the sectionalizing switch are in a normal state, respectively; and p_t^p is the same as p_q^p.

For the transferable customer *n*, when a fault occurs outside the transferring area, the customer has p_t chance to restore power supply through the tie line, so the failure rate and the average repair time for this kind of customer can be expressed as follows:

$$\lambda_n^L = (1 - p_t) \sum_{i=1}^{N_{ti}} \lambda_i + \lambda_{t,n}^{eq} \tag{32}$$

$$r_n^L = \frac{1}{\lambda_n^L} \left[(1 - p_t) \cdot \sum_{i=1}^{N_{up}} \lambda_i r_i + \sum_{i=1}^{N_{up}} \lambda_i \cdot p_t \cdot t_{ti,t} + \lambda_{t,n}^{eq} r_{t,n}^{eq} \right] \tag{33}$$

where λ_i and r_i are the failure rate and repair time of components located in the minimal path between the transferring area *t* and the main source or the branch of the non-minimal path; N_{up} is the sum of the minimal-path component and the non-minimal-path branch; and $\lambda_{t,n}^{eq}$ and $r_{t,n}^{eq}$ are the equivalent failure rate and repair time from customer *n* to the sectionalizing switch, respectively.

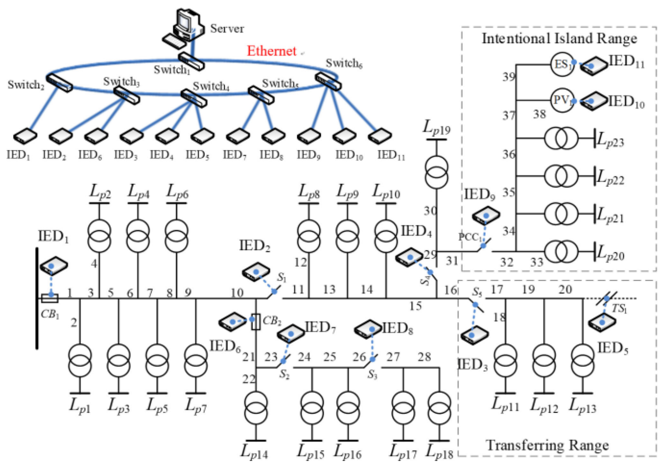

Fig. 7. Distribution Network Structure.

TABLE I
LOAD DATA

	Load Point Number	User Type	Number of Users	Mean Power /MW
1	2	Residential	126	1.81
2	1, 6	Residential	147	1.90
1	5	Residential	132	1.12
4	8, 11, 14, 19	Residential	79	1.63
4	10, 12, 16, 22	Residential	76	1.09
2	15, 20	Agricultural	1	1.27
3	3, 13, 17	Agricultural	1	1.54
2	4, 18	Agricultural	1	1.15
2	7, 23	Agricultural	1	1.48
2	9, 21	Agricultural	1	1.80
Total	23		1183	33.63

V. CASE STUDIES

A. *Test System and Parameters*

The test system is the feeder 4 of IEEE RBTS BUS 6 as shown in Fig. 7. The feeder contains 23 load points, 1183 users of total power 33.63 MW, a generation unit of 7 MW and an energy storage system of 6 MW/12 MWh [12], as shown in Table I. What's more, the probability that the circuit breaker reliably switches is 80%, and the probability of the sectionalizing switch and the tie switch is 90% [27]. The failure rate of the power line is 0.05 f/a·km, and the repair time is 4 h; The failure rate of the breaker is 0.002 f/a, and the repair time is 4 h; the failure rate of the transformer is 0.015 f/a, and the repair time is 200 h. Due to the fault self-healing process, the switching time of the sectionalizing switch is 1 min; the switching time of the tie switch is 2 min, and the transmission limit power of the tie line is 6 MW.

In addition, the cyber system adopts a ring structure and Ethernet. The switches are "manageable" in order to ensure fault tolerance against the failure of a switch or the disconnection of a media. The server failure rate is 0.01 f/a and the repair time is 8 h; the switch failure rate is 0.05 f/a and the repair time is 12 h; the fiber line failure rate is 0.004 f/a·km and the repair time is 24 h; the IED failure rate is 0.06 times/year and the repair time is 12 h. What's more, the communication node adopts the Pareto distribution model with the compliance parameter of 67.9 ms and 20 [28], [29]; the IED forwarding delay follows the normal distribution model $N(68.35,11)$ [30]. The cyber line delay follows the exponential distribution model [31]. Meanwhile, considering that the cyber system studied in this paper is small, the system delay threshold takes 600 ms [32], [33]. Furthermore, the error probability of the cyber node and IED is 10^{-4} [34], and the fiber error is 10^{-9}.

TABLE II
CYBER LINK VALIDITY PROBABILITY

IED	Physical Component	Validity Probability	IED	Physical Component	Validity Probability
IED 1	CB1	98.77%	IED 7	S2	96.65%
IED 2	S1	96.83%	IED 8	S3	96.86%
IED 3	S5	91.94%	IED 9	PCC1	98.81%
IED 4	S4	92.67%	IED 10	PV1	98.65%
IED 5	TS1	92.81%	IED 11	ES1	98.68%
IED 6	CB2	96.80%			

TABLE III
SYSTEM RELIABILITY RESULTS

	Only Physical Failures Considered	Both Cyber and Physical Failures Considered
ASAI	99.82	99.81
EENS	558.08	602.59
SAIFI	1.52	1.64
SAIDI	15.35	16.62
CAIDI	10.12	10.10

B. *Results and Analysis*

In order to study the impact of cyber failures on physical systems, the validity probability of all cyber links is calculated at first, as shown in Table II. Then reliability indices are calculated, such as the Average Service Availability Index (ASAI), the Expected Energy Not Supplied (EENS), the System Average Interruption Frequency Index (SAIFI), the System Average Interruption Duration Index (SAIDI) and the Customer Average Interruption Duration Index (CAIDI).

It can be seen that the validity probability of the cyber link is generally above 90%. As shown in Table II, the validity probability of the cyber link can be divided into three groups: {IED1, IED9, IED10, IED11} and {IED2, IED6, IED7, IED8} and {IED3, IED4, IED5}. Specially, the validity probability of each group is very similar, and the tendency of the cumulative function is very similar. Since the primary and backup routes of each group have the same sum of cyber nodes, it can be concluded that the transmission performance and the message forwarding hops are important factors affecting the validity of cyber links. Obviously, improving the cyber node performance and reducing the hops of messages forwarding can improve the validity effectively.

As shown in Table III, cyber system failures indeed have an impact on the system reliability. Especially, the system reliability indices of EENS, SAIFI, and SAIDI increase by 7.97%, 8.48% and 8.24%, respectively, caused by the cyber system fault, while CAIDI increases by less than 1%. Although the impact of cyber system faults on the reliability of active distribution network is not highly significant, they cannot be ignored in power system planning in the cyber-physical context.

TABLE IV
COMPARISION OF RESULTS CALCULATED

		Analytical Method	Convolution Analytical Method	Hybrid Simulation Method
Results	ASAI	99.81	99.81	99.81
	EENS	602.59	602.55	601.41
	SAIFI	1.64	1.64	1.91
	SAIDI	16.62	16.61	16.42
	CAIDI	10.10	10.10	8.59
Efficiency	Total	10.14s	22.72s	72.53s
	Cyber Process	9.52s	22.12s	9.18s
	Physic Process	0.62s	0.60s	63.35s

TABLE V
COMPARISION OF DIFFERENT METHODS

	λ (f/a)		U (h/a)		r (h/f)	
	Analytical Method	Simulation Method	Analytical Method	Simulation Method	Analytical Method	Simulation Method
L_{P9}	2.06	2.44	20.61	19.87	10.00	8.14
L_{P14}	1.67	1.97	16.10	16.20	9.66	8.21
L_{P18}	2.29	2.66	24.61	22.56	10.76	8.80
L_{P12}	1.47	1.55	13.37	12.08	9.11	7.76
L_{P22}	2.54	1.79	28.42	23.87	11.18	11.72

TABLE VI
THE DEPENDENCE OF EACH COMPONENT AND THE VALIDITY PROBABILITY OF CYBER LINK

	ω_i	Validity		ω_i	Validity
CB1	0	92.67%	S5	47.21	96.83%
CB2	0	91.94%	PCC1	330.91	98.81%
S1	122.16	96.86%	TS1	140.39	98.68%
S2	38.66	96.65%	PV1	199.82	98.77%
S3	20.81	92.81%	ES1	135.98	98.65%
S4	38.80	96.80%			

1) Comparison of Calculation Correctness and Efficiency: In order to validate the correctness and efficiency of the proposed algorithm, the obtained results are compared with the analytical method using convolution to solve the cyber transmission delay, and with the hybrid simulation method proposed by [19], as shown in Table IV. It should be noted that the convergence condition of the hybrid simulation method is that the EENS' variance coefficient should be less than 0.02 during the 8 continuous iterations.

It can be found that there is little difference between the results of the analytical method proposed in this paper and the simulation method, which verifies the correctness of the proposed algorithm. At the same time, it can be found that the efficiency of the proposed algorithm is 86.02%, which is higher than the simulation method. The time to handle cyber systems by the analytical method is 9.52 s; the reason it is much longer than the physical system processing time is that Laplace transform for the cyber system takes more time. However, the processing time of the cyber system using the convolution method is 22.12 s, which is about 2.32 times of the frequency-time conversion method. Besides, as the scale of the system increases, the cost of a convolution calculation will increase drastically, which is even more unsuitable for CPS reliability evaluation demanding fast calculations.

In addition, the difference of the results during the fault self-healing process between the analytical method proposed in this paper and the hybrid simulation method is compared. Common customers L_{P9}, L_{P14} and L_{P18}, transferring customers L_{P12}, and islanded customers L_{P22} are selected to analyze the changes in customers' reliability.

TABLE VII
BEFORE AND AFTER OPTIMIZED MATCHING

	System Reliability Before Optimized Matching	System Reliability After Optimized Matching
ASAI	99.81	99.81
EENS	602.59	593.57
SAIFI	1.64	1.61
SAIDI	16.62	16.34
CAIDI	10.10	10.15

Compared with the results calculated by the analytical method in this paper, the user's failure rate calculated by the simulation method is a little higher, while the average power repair time is slightly lower, but they are consistent in terms of the tendency of reliability changes. Particularly, the failure rate of L_{P18} is obviously higher than L_{P14}, proving that the branch equivalent method considering a multi-switch proposed in this paper can clearly describe the isolation effect of a multi-switch on downstream faults.

2) Dependence Degree of Physical Components: Through the analysis of the cyber link validity probability and the cumulative function, it can be assumed that if a cyber link with high validity is assigned to the component that has a strong influence on the self-healing process, the reliability of the active distribution network could be improved. Therefore, the dependence degree ω_i of the component is defined to describe how much the component depends on the cyber system, according to the working characteristics of the switch, the micro source and the tie switch.

$$\omega_i = \begin{cases} 0, & \text{breaker} \\ \frac{|S_n - S_0|}{p_i^e(1-p_i^n)}, & \text{other components} \end{cases}, \tag{34}$$

where S_n is EENS of the current state; S_0 is the EENS that the cyber system is valid; p_i^e is the probability that the component is reliable; p_i^n is the validity probability of component i in the current state.

It can be seen that PCC, PV generators and batteries are of high ω_i, indicating that there are significant constraints on the formation and operation of an intentional island caused by the cyber failure. Particularly, ω_i of PCC node is the highest, which indicates that the intentional island could not be formed mainly because of the invalidity of the PCC node. In addition, the ω_i value of the switch S1 is the highest, because most components are in the downstream area, and the timely action of S1 can effectively prevent the spread of faults. Therefore, improving the performance of the micro source, the PCC, and the sectionalizing switch in the head of the trunk line can effectively improve the reliability of the active distribution system. Then, a system after optimized matching is proposed, and the reliability of the system is calculated as shown in Table VII.

Comparing the system reliability indices before and after the optimized matching, it can be seen that the reliability of the active distribution system is somehow improved. Specifically, EENS, SAIFI, and SAIDI decrease by 1.50%, 2.15% and 1.67%,

TABLE VIII
SYSTEM RELIABILITY UNDER DIFFERENT CASES

	ASAI	EENS	SAIFI	SAIDI	CAIDI
Case 1	99.80	685.18	1.73	17.59	10.15
Case 2	99.81	602.59	1.65	16.62	10.10
Case 3	99.82	549.03	1.59	15.98	10.07

TABLE IX
SYSTEM RELIABILITY UNDER DIFFERENT CASES

	ASAI	EENS	SAIFI	SAIDI	CAIDI
Case 1	99.79	665.79	1.82	18.58	10.20
Case 2	99.81	602.59	1.65	16.62	10.10
Case 3	99.82	572.90	1.56	15.69	10.05

respectively. Due to the small scale and the limited number of devices in the established test system, the optimized result is not very significant. However, for a large-scale system, matching the effective validity of the cyber link with the importance of physical components is a useful method that can effectively improve the reliability without significantly changing the structure of the communication network.

3) The Impact Analysis of Cyber Failure on the Intentionally Formed Island: The micro source plays a vital role in the active distribution network, which can effectively reduce the load loss and improve the system reliability. However, the micro source needs to be properly controlled to ensure its stable operation. Here three cases are established to analyze the impact of the micro source on the reliability of an active distribution network.

Case 1: Active distribution network without the micro source, considering both systems' components may fail.

Case 2: Active distribution network with the micro source, considering both systems' components may fail.

Case 3: Active distribution network with the micro source, only considering the physical system components may fail.

It can be seen from Table VIII that the existence of the micro source can improve the reliability of the active distribution system. For example, the ASAI in Case 2 is about 0.01% higher than that of Case 1, but is slightly lower than 99.82% in Case 3, indicating that the cyber system failure has some influence on the intentionally formed island. However, the improvement of the active distribution network by the micro source cannot be ignored.

4) The Impact Analysis Of Cyber Failure on Load Transferring: Similar to the micro source, the tie line can also improve the reliability. Three cases are established to analyze the impact of the load transferring on the active distribution network.

Case 1: Active distribution network without a tie line, considering the components in both systems might fail.

Case 2: Active distribution network with a tie line, considering components in both systems might fail.

Case 3: Active distribution network with a tie line, only considering physical system components might fail.

It can be seen from Table IX that compared with Case 1, the ASAI of Case 2 increases from 99.79% to 99.81%, and there are different degrees of improvement for other indices. By comparing Case 2 and Case 3, it can be found that the cyber failure has an appreciable influence on the load transfer.

VI. CONCLUSION

First, considering the cyber transmission performance, this paper proposes an efficient solution method using a frequency-time domain conversion. Then, based on the switch model, a method combining the upward equivalence and the minimal path method is proposed, which greatly improves the calculation efficiency. Finally, a test system is established to analyze the impact of the cyber transmission performance on the reliability of an active distribution network, and the correctness and efficiency of the proposed method are verified. There are two main observations based on the simulation results. On the one hand, the performance of the cyber components themselves as well as the times that the information is forwarded through the cyber components are important factors affecting the invalidity of the cyber system. Improving the performance of the cyber components and reducing the number of times the information is forwarded through the components can improve the reliability of cyber-physical systems. It is worth noting that due to the high invalidity of the information link in the actual distribution network, the impact of cyber system failures on the reliability of active distribution networks is not particularly significant, but still some attention needs to be paid to it. On the other hand, cyber failures have a great impact on the forming and operation of intentional islands, so PCC, photovoltaic cells and energy storage batteries are of high importance in the active distribution network. As a result, improving the corresponding cyber link performance of the abovementioned components can effectively improve the overall system reliability. Finally, this study shows that the failure of information will affect the micro sources and the use of tie lines for load transfer to improve the customers' reliability. At the same time, in case of cyber failures, micro sources can effectively improve the reliability of active distribution networks as the automatic transfer from the centralized control mode to the local control mode is performed.

In the further research, the impact of a cyber system backup and protection methods on cyber validity will be explored. What's more, the accuracy of a cyber validity model and the efficiency of a CPS reliability assessment need to be further improved.

REFERENCES

[1] N. Kashyap, C. Yang, S. Sierla, and P. G. Flikkema, "Automated fault location and isolation in distribution grids with distributed control and unreliable communication," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2612–2619, Apr. 2016.

[2] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour, and A. Safdari, "Impact of WAMS malfunction on power system reliability assessment," *IEEE Trans. on Smart Grid*, vol. 3, no. 3, pp. 1302–1309, Sep. 2012.

[3] 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. Expo.*, 2011, pp. 1–7.

[4] 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.*, Washington, DC, USA, 2012, pp. 1–8.

[5] 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.

[6] 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.

[7] F Aminifar, M Fotuhi-Firuzabad and A. Safdarian, "Optimal PMU placement based on probabilistic cost/benefit analysis," *IEEE Trans. Power Syst.*, vol. 28, no. 1, pp. 566–567, Feb. 2013.

[8] T. Chaudonneret, and H. Decroix, "Representation of the influence of telecommunications on electrical distribution network reliability," in *Proc. IEEE Smart Grid Commun. Int. Conf.*, 2013, pp. 258–263.

[9] S. Babu, P. Hilber, and J. H. Jürgensen, "On the status of reliability studies involving primary and secondary equipment applied to power system," in *Proc. IEEE Probabilistic Methods Appl. Power Syst. Int. Conf.*, 2014, pp. 1–6.

[10] B. Yunus, A. Musa, H. S. Ong, A. R. Khalid, and H. Hashim, "Reliability and availability study on substation automation system based on IEC 61850," in *Proc. IEEE Power Energy Int. Conf.*, 2009, pp. 148–152.

[11] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie, "Cyber-physical system risk assessment." in *Proc. IEEE Intell. Inf. Hiding Multimedia Sign. Proces. Int. Conf.*, 2014, pp. 442–447.

[12] T. Zhao *et al.*, "A risk assessment method for cascading failure caused by electric cyber-physical system (ECPS)," in *Proc. 5th Int. Conf. Electr. Utility Deregulation Restructuring Power Technol.*, 2015, pp. 787–791.

[13] G. Celli *et al.*, "Impact of ICT on the reliability of active distribution networks," in *Proc. CIRED 2012 Workshop: Integration Renewables Distribution Grid*, 2012, pp. 1–4.

[14] Y. Han *et al.*, "Incorporating cyber layer failures in composite power system reliability evaluations," *Energies*, vol. 8, no. 9, pp. 9064–9086, 2015.

[15] S. F. Bush, "Network theory and smart grid distribution automation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1451–1459, Jul. 2014.

[16] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[17] 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.

[18] Y. Guo, S. Liu, Y. Liang, and Li Huang, "Research on reliability of distribution network based on grid cyber-physical system and telecontrol system," in *Proc. IEEE Int. Conf. Energy Int.*, 2017, pp. 256–261.

[19] 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.

[20] M. H. 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.

[21] S. Kazemi, R. J. Millar, and M. Lehtonen, "Criticality analysis of failure to communicate in automated fault-management schemes," *IEEE Trans. Power Del.*, vol. 29, no. 3, pp. 1083–1091, Jun. 2014.

[22] W. Liu *et al.*, "Collaborative planning of DERs and intentional islands in distribution network considering loss-of-load risk," in *IEEE Access*, vol. 6, pp. 45961–45973, 2018.

[23] B. Falahati, Y. Fu, and M. J. Mousavi, "Reliability modeling and evaluation of power systems with smart monitoring," in *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 1087–1095, Jun. 2013.

[24] B. Falahati and Y. Fu, "Faults and failures in cyber-power interdependent networks," in *Proc. IEEE PES T&D Conf. Expo.*, 2014, pp. 1–5.

[25] W. He, X. Liu, L. Zheng, and H. Yang, "Reliability calculus: A theoretical framework to analyze communication reliability," in *Proc. IEEE Distribution Comput. Sys. Int. Conf.*, 2010, pp. 159–168.

[26] H. Wang, *et al.*, "Dynamic equivalent-based reliability evaluation of distribution systems with DGs," *IET Gener., Transmiss. Distribution*, vol. 10, no. 10, pp. 2285–2294, 2016.

[27] R. Billinton, and P. Wang, "Reliability-network-equivalent approach to distribution-system-reliability evaluation," *IEE Proc. - Gener., Transmiss. Distributop*, vol. 145, no. 2, pp. 149–153, Mar. 1998.

[28] W. Zhang and J. He, "Modeling end-to-end delay using pareto distribution." in *Proc. IEEE Int. Monit. Prot. Int. Conf.*, 2007, pp. 21–21.

[29] W. Zhang and J. He, "Statistical modeling and correlation analysis of end-to-end delay in wide area networks," in *Proc. Conf. Softw. Eng., Artif. Intell., Netw., Parallel/Distribution Comput. (SNPD)*, 2007, pp. 968–973.

[30] Y. Wan, "An integrated cyber-physical simulation environment for smart grid applications," *Tsinghua Sci. Technol.*, vol. 19, no. 2, pp. 133–143, 2014.

[31] W. P. Jin, and J. M. Lee, "Transmission modeling and simulation for Internet-based control," in *Proc. IEEE Ind. Electron, Soc. Conf.*, 2001, pp. 165–169 vol. 1.

[32] D. Roberts, *Network Management Systems for Active Distribution Networks–A Feasibility Study*, Scotland, U.K.: SP Power Systems Ltd, Scottish Power Plc., 2004.

[33] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 42–49, Jan. 2013.

[34] L. Zheng *et al.*, "Energy efficient communication networks design for demand response in smart grid," in *Proc. Int. Conf. Wireless Commun. Sign. Proces.*, 2011, pp. 1–6.

Wenxia Liu (Member, IEEE) received the B.S. degree in radio engineering from the Nanjing University of Science and Technology in 1990,and the M.S. degree in power system & automation from Northeast Electric Power University in 1995, and the Ph.D. degree in the same field from North China Electric Power University (NCEPU) in 2009. Currently, she is a Professor in the School of Electrical and Electronic Engineering at NCEPU. Her research interests are intelligent planning of power systems, power system risk assessment, power communication system, and reliability and planning of Cyber-Physical System (CPS).

Zijian Lin (Student Member, IEEE) received the B.S. degree in electrical engineering from the Zhejiang University of Technology, Hangzhou, China in 2018. Currently, he is a M.S. Student in electrical engineering of North China Electric Power University (NCEPU). His research interests are CPS reliability, CPS operations, and distribution systems.

Lingfeng Wang (Senior Member, IEEE) received the B.E. degree in measurement and instrumentation from Zhejiang University, Hangzhou, China, in 1997, and the M.S. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2002, and the Ph.D. degree from the Electrical and Computer Engineering Department, Texas A&M University, College Station, TX, USA, in 2008. He is currently a Professor with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee, Milwaukee (UWM), WI, USA. His major research interests include power system reliability, security and resiliency.

Dr. Wang is an Editor of the IEEE TRANSACTIONS ON SMART GRID, IEEE TRANSACTIONS ON POWER SYSTEMS, and IEEE POWER ENGINEERING LETTERS, and served on the Steering Committee of the IEEE TRANSACTIONS ON CLOUD COMPUTING. He is a recipient of the Outstanding Faculty Research Award of College of Engineering and Applied Science at UWM in 2018.

Zhiqiang Wang (Member, IEEE) received the B.S. degree in electrical engineering from the Nanjing University of Science and Technology, in 1990, and the M.S. degree in power system & automation from Northeast Electric Power University in 1995. Currently, he is an Associate Professor in the School of Electrical and Electronic Engineering at North China Electric Power University (NCEPU). His research interests are power system planning and communication system.

Hanyu Wang (Student Member, IEEE) received the B.S. degree in electrical engineering from Northeast Electric Power University, Jilin, China in 2018. Currently, she is a M.S. Student in electrical engineering of North China Electric Power University (NCEPU). Her research interests are CPS reliability and distribution system operations.

Qi Gong received the B.S. degree in smart grid engineering from North China Electric Power University (NCEPU), Beijing, China in 2016, and the M.S. degree in power system & automation from the same university in 2019. Currently, he works in State Grid Wuxi Electric Power Company. His research interests are CPS operations and power distribution systems.