Reliability Modeling and Evaluation of Active Cyber Physical Distribution System

Wenxia Liu, *Member, IEEE,* Qi Gong, *Student Member, IEEE,* Hui Han, *Student Member, IEEE,* Zhiqiang Wang, *Member, IEEE,* and Lingfeng Wang, *Senior Member, IEEE*

***Abstract*—To enable an in-depth study of active cyber-physical distribution network, a cyber subsystem model is urgently needed to describe the performance in distribution communication. The methods for quantifying the interactions between subsystems, especially indirect interactions, have not been adequately studied in the existing research. In this paper, a novel model is developed to evaluate the validity of cyber link considering dynamic routing, delay, and communication error, particularly the cyber traffic. Then, an analytical method is presented to quantify the impact of cyber faults considering the functionality validity during distribution automation. And the reliability of cyber and physical subsystems is evaluated based on Non-Sequential and Sequential Monte Carlo methods respectively. Finally, a test system for reliability evaluation is established to analyze the influences of cyber faults. Also sensitivity analyses on the impact of cyber network traffic, element failure rate, and network topology and access communication technology are carried out. The obtained results could provide useful insights into planning and operation of active cyber-physical distribution networks.**

***Index Terms*—Active distribution network, cyber-physical system, reliability evaluation, transmission validity, distribution automation.**

I. Intruduction

Large amounts of distributed renewable sources being grid-connected are changing the operational characteristics of distribution systems and degrading the power quality. To address the challenges, the concept of Active Distribution Network (ADN) was proposed [1]. The future distribution systems are becoming more computerized and connected, and massive measurement signals and control instructions are transmitted through communication networks [2]. ADN adopts a variety of control methods to avoid status deterioration, further enhance network performance, and improve sources efficiency. However, the active management cannot be achieved without Information and Communications Technology (ICT). On the one hand, timely and accurate transmission and decision-making are the basis for enabling a variety of active control functions; on the other hand, ICT system's random failures may lead to adverse consequences such as operational condition deterioration and widespread blackouts. Thus, the control characteristics of ADN make it highly dependent on ICT, which is essentially similar to the Cyber Physical System (CPS) - so ADN can be regarded as a typical Cyber Physical Distribution System (CPDS).

Structurally, CPS can be divided into two major parts: cyber subsystem and physical subsystem, which interact with and interdepend on each other. Generally, the existing research was focused on the interaction analysis, model establishment, and evaluation method. The interactions between cyber and physical subsystems can be classified into four kinds of interdependencies [3], which are elaborated in [4] and [5]. These interdependencies are determined by different direct or indirect relationships between the cyber faults and the physical faults.

The direct interdependencies mean that the cyber fault can directly result in the failure of the corresponding physical elements [6, 7]. For example, a line protection malfunction would lead to misoperation of this line's adjacent breaker [8]. Communication interruption could result in malfunctions of Automatic Generation Control (AGC), causing bulk system outages [9]. And Distributed Generation (DG) cannot be properly integrated into the grid without valid communications with the station [4]. Generally, the direct interdependencies can be mathematically represented by series reliability models with cyber failures being superimposed on the physical subsystem.

The indirect interdependencies refer to that the cyber failure can lead to the degradation of physical performance, such as the potential impact of monitoring failure on physical subsystem during its normal operation [10], and the impact of cyber failure on physical control when physical faults occur, which will affect the fault processing and worsen the operational status [7, 11]. The status of physical operation is influenced by not only indirect interdependencies, but also a number of other complex factors. Consequently, it is rather difficult to quantify the indirect effect. Simply, physical element with monitoring fault can be regarded as the same one with higher failure rate [5, 8, 12]. New approaches are also proposed to describe the interdependencies between subsystems based on Markov model and stochastic Petri Nets [13-15]. However, there are

This work was supported by the National Key Research & Development Program of China under Award 2017YFB0903100; and Lingfeng Wang was supported by the National Science Foundation (NSF) under Award ECCS1739485. (*Corresponding authors: Wenxia Liu and Lingfeng Wang*).

W. Liu, Q. Gong, H. Han, and Z. Wang are with the School of Electrical and Electronic Engineering, and are also with the State Key Laboratory for Alternate Electrical Power System with Renewable Energy Sources, North China Electric Power University, Beijing, China (e-mails: liuwenxia001@163.com; gongqihen@163.com; ncepuhh@126.com; and wwwgode@163.com)

L. 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).

few studies focusing on indirect interdependencies between distribution automation and cyber fault in distribution networks.

Recently, the cyber modeling in CPS reliability is greatly different in different research scenarios. Literature [7, 16-18] establishes a simple communication system, in which messages are transmitted through an end-to-end path - once interrupted, message transmission would immediately fail. Several equivalent methods, such as the theory of complex network [19, 20], network mapping [21], and reliability block diagram [5, 22], are adopted to describe the transmission communication system while ignoring routing protocols, actual structures and self-protection mechanisms. The distribution communication network composed of passive optical networks, industrial Ethernet, power line carrier, wireless network, and so on [23] which can be regarded as a typical heterogeneous network. However, it has not been adequately studied, especially for the factors influencing the reliability, such as the line length, external environment, and traffic conditions [24, 25]. Though an information transmission model considering transmission errors and delays has been proposed in [26], the associated parameters (especially the transmission error threshold) need to be more comprehensively defined and studied.

There are three major reliability evaluation methods for CPS: 1) analytical method is used in both subsystems; 2) analytical method is used in cyber subsystem and simulation method is used in physical subsystem; 3) simulation method is used in both subsystems. The analytical method is usually used in simple scenarios [4, 5]. While the physical subsystem usually adopts the simulation method, simulation and analytical methods can both be used in the cyber subsystem according to system complexity [8, 14, 16, 27].

In this paper, considering the dynamic routing, delay, and communication error, a new model which focuses particularly on validity evaluation of the cyber link is developed to determine whether a link is able to transmit messages effectively. In particular, the traffic of the cyber network is considered as well. Then, the paper presents an analytical method to quantify the impact of cyber fault on the reliability of physical subsystem during distribution automation. Thirdly, considering the contribution of distributed generator in fault restoration, the reliability of the cyber and physical subsystem is derived based on Non-Sequential and Sequential Monte Carlo simulation methods respectively. Finally, a test system is established, and the influence of cyber validity on CPDS reliability is examined. The sensitivity analyses on the impact of cyber network traffic, element failure rate, network topology, and access communication technology are carried out. The research results could provide useful technical support for active distribution network planning and operation.

The overall paper is divided into the following sections. In Section II, the structure and function of CPDS is described. In Section III, factors which may impact the cyber subsystem are analyzed, meanwhile the validity model of cyber link is presented in this section. In Section IV, the model of quantifying the impact of cyber fault on physical distribution automation is described. In Section V, reliability evaluation of CPDS is presented. In Section VI, a typical CPDS is used as a test system to validate the proposed model and method. The conclusions are drawn in section VII.

II. Structure and Function of CPDS

CPDS can be divided into cyber and physical subsystem. The cyber subsystem usually includes interface layer, communication layer and application layer, shown in Fig. 1.

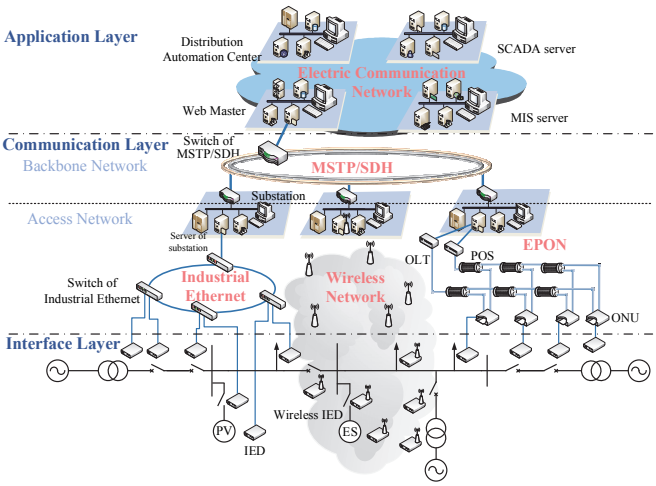


Fig. 1 The CPDS main structure

The application layer can achieve many functions such as human interaction, information analysis, and decision-making. The communication layer is in charge of transmitting monitored data, control instructions, and other messages. In actual power systems, the substation does not perform decision making, instead, it only conducts data collection and pre-processing tasks. Therefore, distribution automation process needs the main station (i.e., the control center) to make decisions. However, the structure, the communication technology, and the function of the communication network between the substation and the main station are totally different from that between the substation and the terminal. Thus, the communication layer can be divided into two parts [28]: backbone network and access network. Backbone network is the communication network between the control center and substation, in which message is transmitted through synchronous network with ring topology. Access network is the communication network between substation and distribution terminal, which can adopt many communication technologies, such as Ethernet, power line carrier, wireless, and so on. The interface layer includes the feeder protection equipment, feeder terminal units (FTU), distribution terminal units (DTU), inverters, and other intelligent distribution terminals. The cyber equipment of CPDS is generally operated with Uninterruptible Power System (UPS), while the physical fault has little impact on the cyber subsystem. Thus, this paper is mainly focused on the influence of potential cyber faults on the reliability of physical subsystem during ADN's distribution automation process.

Local feeder automation is mostly used in the traditional distribution. However, feeder automation based on centralized monitoring (simplified as centralized automation) is widely used in CPDS with large numbers of DGs, and it has high dependence on the cyber subsystem. Therefore, centralized automation is used as the research scenario. Through the status monitoring and control function, the centralized automation, which includes failure elimination, location, isolation, and restoration [29], is enabled by proper communications with the

control center for controlling circuit breakers, sectionalizing switches, and switching micro-sources [30]. In centralized automation, feeder protection faults as well as switch controller malfunctions would cause line outages, switch false tripping and refusal. The interactions of these failures fall into direct interdependencies, which can be modeled by analyzing the historical data of outages. The monitoring and control function failures in the fault handling process resulted from the IED, communication network and server faults fall into indirect interdependencies, which could greatly compromise the reliability of CPDS. Therefore, this paper will be focused on the indirect interdependencies.

III. Validity Analysis and Modeling of Cyber Subsystem

A. Analysis of Fault Factors in Cyber Subsystem

In this paper, the transmission circuit between interface layer and the application layer is defined as the cyber link (application server is not included). The validity of cyber link refers to its ability to meet the requirements of three types of reliability: topology reliability, delay reliability, and error reliability, which are similar to those in [31]. That is to say, a cyber link is valid only if the message can be transmitted through it uninterruptedly, timely, and accurately [32, 33].

1) Fault Factors of Interface Layer

The interface layer can measure and upload the messages of voltage, current, power and switch status through the interface equipment, and it can also receive and execute control instructions [34]. The interface layer fault usually contains the failure of status collection and uploading, as well as the failure of instruction execution. Interface layer fault will lead to the interruption of cyber link, while the error of the data measurement will decrease the accuracy. In addition, the algorithm or parameter errors will cause malfunctions. Among them, the interruption caused by an element fault is the most significant factor affecting the communication performance, because the interface layer equipment operates without redundancy in a complicated environment.

2) Fault Factors of Communication Layer

The communication link is the transmission circuit between the source and the sink (not including the source and sink elements), which mostly consists of multiple communication paths. Usually, the transmission performance can be described by the connectivity affected by network element failures, the timeliness affected by message transmission delay, and the accuracy affected by the communication error. Varying with specific communication technologies, the above three properties can be enhanced quite differently.

The partial communication link in the backbone network, mostly with ring topology, has at least two paths to guarantee connectivity by switching to alternate channel in the event of a fault. The transmission time generally grows with the number of nodes that the path traverses, so the delay reliability would be compromised after alternate switching due to more nodes.

In the access network, the validity of communication link is closely related to the communication technology. When Industrial Ethernet (Ethernet based on TCP/IP), mostly with the ring topology, is used in access network, the communication link would still be connected by means of failover after a random fault occurs. The transmission delay is closely related to the traffic and the number of nodes [35], and the communication error. The accuracy of transmission is very high because of the low BER of fiber lines and the error control of TCP.

When GPRS is used, connectivity can be easily guaranteed because the GPRS system is usually configured in star topology with different degrees of overlapping between radio cells. The probabilistic characteristic of the delay reflects the service of mobile net. Generally, the delay is related to the network traffic, while the BER is associated with weather conditions and channel quality.

When the passive optical network is used, the network will be constructed based on the double chain topology for ensuring high reliability. Usually, to ensure a good performance, multiple access technologies are used in uploading data, while broadcast is used in downloading data. The main factors influencing the delay are the hop routing and network flow which fluctuates within a narrow range and can actually satisfy the demands in reality [36]. The packet loss caused by the remote transmission distance and poor installation accounts for a significant proportion.

3) Fault Factors of Application Layer

CPDS application server can implement such functionalities as distribution automation and status optimization through information analysis. The server outage will directly lead to uninformed or wrong decisions accordingly causing the failure of distribution automation. Therefore, the server, usually equipped with backup equipment for higher reliability, plays a pivotal role in the distribution automation process. The server faults due to the delay or the algorithm are extremely rare events, so they are not considered in this paper.

Considering the differences of validity under different communication technologies, this paper establishes a specified cyber subsystem, where the backbone network adopts SDH while access network adopts industrial Ethernet. Moreover, industrial Ethernet with a large capacity is generally used in distribution communication systems [37], in which the transmission is assumed to be lossless.

B. Cyber Link Validity Modeling

Cyber link is the basic unit in message transmission, and the cyber faults could lead to communication interruptions, delays or errors exceeding the threshold, causing unsuccessful transmission. Based on the analysis of part *A*, the influence of application layer delays and errors can be ignored, so is the communication error of interface layer. In this paper, the cyber link validity is denoted as $A(x)$. The cyber link mentioned above is the link between the interfacing equipment of physical element x and the server, which is responsible for transmitting data relating to monitoring, control or control feedback signals. Cyber link usually contains at least two paths to ensure successful transmission. If one path is invalid (e.g., the path is interrupted, delayed or has bit error), the communication system must allocate another path to transmit message based on the shortest distance protocol. Therefore, the cyber link is valid when there is at least one valid path. If there are n paths between the source (i.e., the IED of physical element x) and the sink (i.e., the server), the validity of the cyber link can be expressed as

$$A(x)=\bigcup_{i=1}^{n} A(x_i) \tag{1}$$

where x_i is the i-th path of multiple paths between the interface equipment and the server, $A(x_i)$ is the validity of path x_i, and can be represented as

$$A(x_i)=C(x_i)\cap T(x_i)\cap E(x_i) \tag{2}$$

where $C(x_i)$ is the topology reliability of path x_i, whose value of "1" indicates uninterrupted transmission, and "0" means interrupted transmission. $T(x_i)$ is the delay reliability, whose value of "1" indicates that the transmission satisfies the delay demands, and "0" means the opposite. $E(x_i)$ is the error reliability, whose value of "1" indicate the transmission satisfies BER demands; otherwise its value is "0".

When the above three kinds of reliability requirements are satisfied simultaneously, that is, $A(x_i)$ =1, the path x_i is valid. Meanwhile, only when there exists one valid path between the interface equipment of node x and the server, $A(x)$ =1, the cyber link is able to successfully transmit the message.

1) The Topology Reliability Modeling of Cyber Path Considering Routing

Connectivity fault of the path is embodied by its inability to transmit messages [38], which can be described by the topology reliability. The topology reliability of one cyber path is mainly determined by the availabilities of elements in this path. For a specific path i consisting of m elements, the path is uninterrupted only when the statuses of all associated elements are normal, that is, $C(x_i)$ = 1, which can be represented as:

$$C(x_i)=S(1)\cap\cdots\cap S(k)\cap\cdots\cap S(m) \tag{3}$$

where $S(k)$ is the availability state of element k.

Most faults of cyber elements are repairable without considering aging failures, and the element status can be described as the cycle of "running-outage-running". Therefore, the availability state of the cyber element k is

$$S(k)=\begin{cases}1 & \text{normal operation}\\ 0 & \text{outage}\end{cases}. \tag{4}$$

2) The Delay Reliability Modeling of Cyber Path

Delay reliability refers to the ability that the message could be transmitted within a specified time period through the path x_i. The delay reliability of path i can be expressed as:

$$T(x_i)=\begin{cases}1 & \tau(x_i)\le\tau_0\\ 0 & \tau(x_i)>\tau_0\end{cases} \tag{5}$$

where $\tau(x_i)$ is the transmission delay of x_i , τ_0 is the delay threshold based on the service requirement. The delay is mainly composed of interface layer delay and communication path delay:

$$\tau(x_i)=\tau_{ied}(x_i)+\tau_{path}(x_i) \tag{6}$$

where $\tau_{ied}(x_i)$ is the delay of interface layer and $\tau_{path}(x_i)$ is the delay of communication path.

The delay of interface layer is relatively stable and small, so the delay of the cyber path depends mainly on the communication path delay which changes with different communication protocols. For a specified communication path x_i, communication path delay is the sum of the backbone network path delay $\tau_1(x_i)$ and access network path delay $\tau_2(x_i)$:

$$\tau_{path}(x_i)=\tau_1(x_i)+\tau_2(x_i). \tag{7}$$

In the backbone network adopting SDH or other synchronous protocols, the path delay includes the node delay and the line transmission delay. The node delay τ_t is relatively stable, so for a SDH communication path consisting of N nodes, the network delay is:

$$\tau_1(x_i)=N\cdot\tau_t+\frac{L_1}{c} \tag{8}$$

where L_1 is the total length of the backbone optical link and c is the speed of light.

In the access network which adopts industrial Ethernet, TCP originally uses acknowledgement and retransmission to detect and repair losses, while the time of retransmission is affected by the channel BER and network traffic. However, in switched industrial Ethernet, collisions/retransmissions no longer occur, and the main communication delays occur inside the nodes [39]. Meanwhile, the delay is affected not only by the number of hops but also the processing time of nodes which is related to the network traffic [40]. Thus, when the traffic of industrial Ethernet is certain, the delay of the communication path between two points will comply with the probabilistic characteristics. According to [20, 41], the delay of transmission path can be described by the Pareto distribution in the event-driven application scenarios, and the probability distribution function is represented by:

$$P(\tau)=1-(\frac{t_m}{\tau})^{\beta} \tag{9}$$

where t_m is the minimum delay of path between two nodes that is the sum of transmission path delay and information processing time; β is a positive parameter whose value decreases as the mean load ratio ρ increases; and the value of β can respectively take 30, 20 or 10 under light, medium and heavy loads [42]. Generally, the actual network traffic has statistical self-similarity and heavy-tailed, therefore it is long-range dependent [43]. This paper assumes that the mean load ratio of cyber network obeys the Weibull distribution, and we can obtain the communication path delay of path x_i by calculating t_m and then sampling ρ and $P(\tau)$.

3) The Error Reliability Modeling of Cyber Path

Due to the long transmission lines, poor channel quality and environmental noise, errors will occur during the message transmission. For the communication path i with m' communication lines, the message carried by this path is reliable only when the error reliability of every line simultaneously satisfies the system demand, that is, $E(x_i)$=1.

$$E(x_i)=E_{xi}(1)\cap\cdots\cap E_{xi}(k')\cap\cdots\cap E_{xi}(m'). \tag{10}$$

The error reliability of the line k' between two adjacent nodes can be expressed as:

$$E_{xi}(k')=\begin{cases}1 & \gamma_{k'}\le\gamma_0\\ 0 & \gamma_{k'}>\gamma_0\end{cases} \tag{11}$$

where $\gamma_{k'}$ is the BER of communication path k', γ_0 is the error threshold allowed for the system, which usually changes with the error control mode.

When the message is being transmitted, SDH will check it at both ends of the transmission link and once the erroneous codes are identified, they can be corrected immediately. Consequently, the message transmitted in the backbone network could be totally reliable considering few errors are beyond the error

control capacity. In industrial Ethernet, TCP is also able to handle a small number of errors and delays at both ends through acknowledgements and cyclic redundancy check (CRC), delay characteristics hence can reflect the error feature to a certain extent. Therefore, if the transmission delay meets the requirements in industrial Ethernet, the message is definitely accurate.

IV. Status Analysis of CPS Based Invalidity

How to analyze and quantify the influence of cyber faults on distribution automation is a critical and challenging issue. The cyber fault does not affect the distribution automation when the physical subsystem is normally operating. But when the physical fault occurs, the cyber fault will affect switching actions and DG controls, thus worsening the system status. Therefore, this paper primarily analyzes the influence of cyber faults on the fault location, isolation and restoration during distribution automation, while considering the application layer failure and cyber link failure.

A. Failure Status Analysis under Application Layer Fault

If a fault occurs in the application layer when the physical subsystem fails, the whole distribution automation will be shut down, prolonging the outage time and disabling the intentional islanding. For a feeder with tie switch, $X=\{x_i \mid i = 1, 2, n\text{-}1\}$ indicates the upstream switch set of fault point, where x_n indicates a breaker. $L(x_i)$ is the load between switch x_i and x_{i-1}, while $L(x_1)$ indicates the total load downstream from x_1. $Y=\{y_i \mid i = 1,2,\ldots,m\text{-}1\}$ indicates the downstream switch set, where y_m is a tie switch, $L(y_i)$ indicates the load between y_i and y_{i+1}. A single feeder with tie switch is shown in Fig. 2, where x_4 is a breaker, y_3 is tie switch, the line fault f occurs between x_1 and y_1, and the repair time is t_{re}.

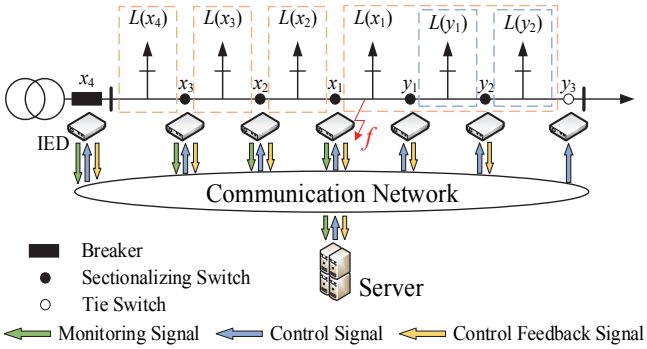


Fig. 2 Failure Status Analysis of CPDS System

When the fault f occurs, the feeder head circuit breaker can trip the fault with instantaneous response, then each sectionalizing switch uploads the fault information. Once the application layer fails, erroreous decisions might be made, leading to unsuccessful switch isolations. Here factitious inspection and isolation is needed, and x_1 and y_1 are manually closed to isolate the failure after t_{1man}, and then y_3 will be manually closed for resoration after t_{2man}.

In the above process, the load loss can be divided into three parts. The outage time and the loss of upstream load can be expressed as

$$\begin{cases} T_{all1} = t_{1man} \\ U_{all1} = \sum_{i=2}^{n} L(x_i) \cdot T_{all1} \end{cases}; \tag{12}$$

while the load manually handled can be expressed as

$$\begin{cases} T_{all2} = t_{1man} + t_{2man} \\ U_{all2} = \sum_{i=1}^{m-1} L(y_i) \cdot T_{all2} \end{cases}; \tag{13}$$

and the remaining can be expressed as

$$\begin{cases} T_{all3} = t_{re} + t_{1man} + t_{2man} \\ U_{all3} = (L(x_1) - \sum_{i=1}^{m-1} L(y_i)) \cdot T_{all3} \end{cases} \tag{14}$$

B. Failure Status Analysis under Cyber Link Fault

1) Fault Location and Isolation

In this process, the control center makes the location decision by collecting the fault information of each switch, and then sends control messages to the specific sectionalizing switch to isolate, and get information about successful isolation by control feedback messages. To accomplish the whole process preciously, the validity must be ensured, not only the validity of control link, but also the monitoring link and the control feedback link of sectionalizing switches at both fault ends. But actually, only the cyber links validity of the upstream switches has an effect on the location and isolation. So, this paper defines $S_{loss}(x_i)$ as the function validity of x_i in the fault location and isolation, which can be represented as

$$S_{loss}(x_i) = A_b(x_i) \cap A_c(x_i) \cap A_m(x_i) \tag{15}$$

where $A_m(x_i)$ is the monitoring validity of upstream switch x_i, $A_c(x_i)$ is the control validity and $A_b(x_i)$ is control feedback validity. The method of calculation is consistent with what has been described in part *B* of section III.

Thus, whether x_i can successfully isolate the fault mainly depends on its function validity $S_{loss}(x_i)$. Specially, the feeder breaker has been tripped, so $S_{loss}(x_n) \equiv 1$.

As mentioned, if the monitoring function of switch x_i fails, the center will get the failure information by switch x_{i+1} located in the upstream from x_i. If the control message is not transmitted to x_i or x_i does not execute it successfully, the center will send the control messages to x_{i+1} for fault isolation. If the control feedback fails after the successful isolation, the control center would also make a wrong judgement, thus sending control messages to x_{i+1} for closure. In sum, if any malfunction occurs in the monitoring, control or control feedback, the consequence would be the expanded outage region. However, as long as there is a valid switch x_i, the fault isolation can be successfully accomplished, while the control message is sent according to the distance from the fault point. Specially, the non-zero minimum among X can be denoted as $smal\{X\}$. If the switching time of sectionalizing switch is t_{sp}, the outage time and the loss of the upstream region of x_i are

$$\begin{cases} T_{loss1} = t_{sp} \\ U_{loss1} = \text{smal}\{S_{loss}(x_i) \cdot \sum_{j=i}^{n} L(x_{j+1}) \mid i = 1,\ldots,n\} \cdot T_{loss1} \end{cases}. \tag{16}$$

And the outage time and the loss of downstream region are

$$\begin{cases} T_{loss2} = t_{re} \\ U_{loss2} = \text{smal}\{S_{loss}(x_i) \cdot \sum_{j=1}^{i} L(x_j) | i = 1,\ldots,n\} \cdot T_{loss2} \end{cases} \quad (17)$$

Usually, the monitoring, control and feedback control link have the same path, and the time of distribution automation process is far less than the outage time of cyber element, so cyber status can be considered to be static in one automation process. The traffic is usually balanced in a certain time period. Thus, the validity statuses of cyber links should be constant in one automation process, and (15) can be simplified to

$$S_{loss}(x_i) = A(x_i) \quad (18)$$

where $A(x_i)$ is the validity of the cyber link between the interface equipment of x_i and server.

2) Fault Restoration by Tie switch

The restoration of active distribution includes restoration by tie switch and by the intentional islanding. After the successful action of the downstream switch of fault point, the main control center will control tie switch to transfer and recover power supply. So, in order to realize the restoration, the validity of the control cyber link of the tie switch y_n should is ensured, as well as the validity of control and the control feedback cyber link of sectionalizing switch y_i. The function validity of restoration by tie switch can be expressed as

$$S_{tran}(y_i) = A_c(y_i) \cap A_b(y_i) \cap A_c(y_n) . \quad (19)$$

Similarly, (19) can be simplified to

$$S_{tran}(y_i) = A(y_i) \cap A(y_n) . \quad (20)$$

If the cyber link of tie switch fails, this kind of restoration will fail. As shown in Fig. 2, when the cyber link of tie switch is valid, the restoration can be carried out if any switches y_i in the downstream from fault point can be successfully isolated. So, the load successfully recovered is expressed as

$$L_{tran} = \max\{S_{tran}(y_i) \cdot \sum_{j=i}^{n-1} L(y_j) | i = 1,\ldots,n\} . \quad (21)$$

Meanwhile, the outage time is the minimum between the fault isolation time and the switching time t_{tr} of the tie switch, so the outage time and the loss of load L_{tran} are as follows:

$$\begin{cases} T_{tran} = \min(t_{tr}, t_{sp}) \\ U_{tran} = \max\{S_{tran}(y_i) \cdot \sum_{j=i}^{n-1} L(y_j) | i = 1,\ldots,n\} \cdot T_{tran} \end{cases} \quad (22)$$

3) Fault Restoration by Intentional Islanding

For a microgrid with determined supply range, whether micro-sources can effectively supply the load inside microgrid, depends on not only their own availability, but also the validity of monitoring and control link because those sources are real-time controlled in ADN [44]. Consequently, the availability of sources can be expressed as

$$\begin{cases} A_{ES} = A_m(ES) \cap A_c(ES) \cap A^0_{ES} \\ A_{PV} = A_m(PV) \cap A_c(PV) \cap A^0_{PV} \end{cases} \quad (23)$$

where A^0_{ES} is the availability state of the energy storage, and A^0_{PV} is the availability state of PV.

Only when the control and control feedback link of the sectionalizing switch of the microgrid is valid, can the intentional islanding operation be carried out. Therefore, the function validity of intentional islanding can be expressed as

$$S_{island}(z) = A_{PV} \cap A_{ES} \cap A_c(z) \cap A_b(z) . \quad (24)$$

Expressions (23) and (24) are combined and simplified as

$$S_{island}(z) = A(ES) \cap A^0_{ES} \cap A(DG) \cap A^0_{DG} \cap A(z) . \quad (25)$$

Therefore, the outage time and loss are expressed as

$$\begin{cases} T_{island} = \min(t_{tr}, t_{sp}, t_{is}) \\ U_{island} = S_{island}(z) \cdot L(z) \cdot T_{island} \end{cases} \quad (26)$$

where t_{is} is the island switching time.

V. Evaluation Method of CPDS Reliability

Considering the temporal property of sources and load, the sequential Monte Carlo simulation method is used to evaluate the physical subsystem. And due to the discrete nature and complexity of cyber faults, sequential Monte Carlo used in both subsystems will seriously reduce the calculation efficiency. Considering that the distribution automation process is not very time-consuming and automation fault has no influence on the physical subsystem with normal operations, after sequential Monte Carlo sampling is completed, non-sequential Monte Carlo sampling is used to get the state of cyber subsystem in every time instant of physical fault. Also this study is conducted based on the assumption that the cyber fault duration is consistent with physical fault duration, which can simplify the state sampling process and increase the sampling efficiency. Besides, in the status analysis process, each link is seen as a unit in evaluating the cyber link validity, and the cyber routing tables are derived based on Depth-First-Search (DFS) according to the cyber topology.

After sampling the system states, we can evaluate the validity of the cyber link, which transmits messages from or to the switches and micro-sources that need to be controlled under the current fault. Then, the load loss and outage time can be calculated by the method proposed in section IV. The details are presented in the following, and the associated flow chart is shown in Fig. 3.

A. Reliability Evaluation Process

1) Initialization: Input the parameters of physical subsystem, establish the reliability model of physical elements and the topology of power grid. Input the parameters of cyber subsystem and calculate the routing information table.

2) Status Sampling: Sequential Monte Carlo is used to sample the status of physical elements. After obtaining the status set, fault elements can be found and then the non-sequential Monte Carlo is used to sample the statuses of cyber elements. At the same time, the cyber load ratio of the current section is sampled. A status scenario can be formed including a set of fault status of physical elements, a set of cyber elements statuses, and load ratio of the cyber subsystem.

3) Status Analysis: By analyzing the element fault status in the physical subsystem, this paper studies which cyber links are needed in the distribution automation. The reliability can be evaluated as follows:

①Input the CPDS status information, if application layer fails, use (12)-(13) to calculate outage time and losses, turn to

⑤. Otherwise, according to the physical fault location, the minimum path method is used to generate switch set X and Y;

② According to the switch set, the cyber link of each sectionalizing switch can be evaluated by (15), and then the outage time and losses of power are calculated by (16)-(17);

③Use (20)-(21) to define the load recovered by tie switch, and then use (22) to calculate the outage time and load loss;

④Islanding Operation: use (25) to evaluate the cyber link of the breaker, and sources of the island, and analyze whether the microgrid can be operated normally in islanded mode. Sample the output curve of PV and calculate the running time of island. There has been much research on islanded operations [45], which are not explained here.

⑤Calculate the outage time and losses.

4）Indices Calculation and Convergence Judgment: Calculate SAIDI and EENS. Determine whether the variance coefficient of EENS meets the convergence condition, if not, repeat step 2) – 4); if so, then output SAIDI and EENS.

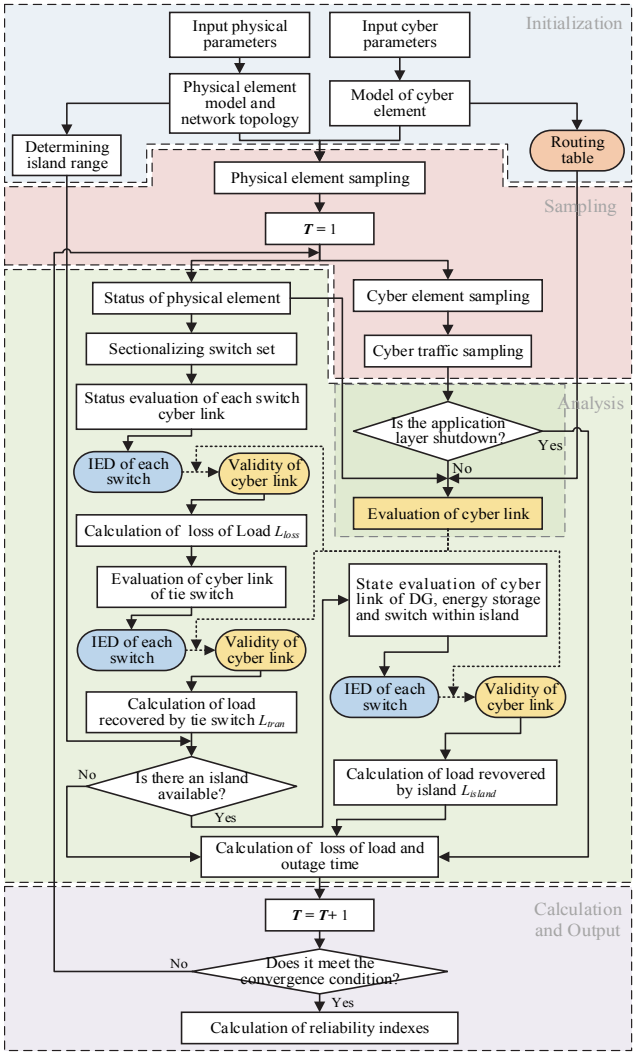


Fig. 3 CPDS system reliability evaluation process

B. *Validity Evaluation Process of Cyber Link*

Based on the status of cyber elements and load traffic of the access network, the validity evaluation of cyber link between the interface elememt and server can be carried out as follows:

1) Input the routing table and the cyber element status, take the IED of each physical element as the initial node, and search the cyber paths between itself and the server according to the routing table. Initialize i=1, and proceed to the next step.

2) For the i-th path, the topology reliability can be calculated by (3).

3) The backbone delay is calculated by (8) and the access delay is calculated by (9), respectively. The total delay of the link is calculated by (6), then the delay reliability is obtained by (5).

4) The path validity $A(x_i)$ is calculated according to (2). If i=n, proceed to next step; otherwise, i=i+1, return to step 2).

5) The validity $A(x)$ of cyber link is calculated by (1). If $A(x)$ =1, the cyber link is valid; otherwise, it is invalid.

6) Output the validity outcome of the link.

VI. CASE STUDIES

A. *Simulation System Setup*

The test system is established as shown in Fig .4. Black lines represent the physical subsystem structure, and blue ones are associated with the cyber subsystem. The control, monitoring and protection functions are all enabled by IED units which can communicate while the control center in the main station can send message through SDH and industrial Ethernet.

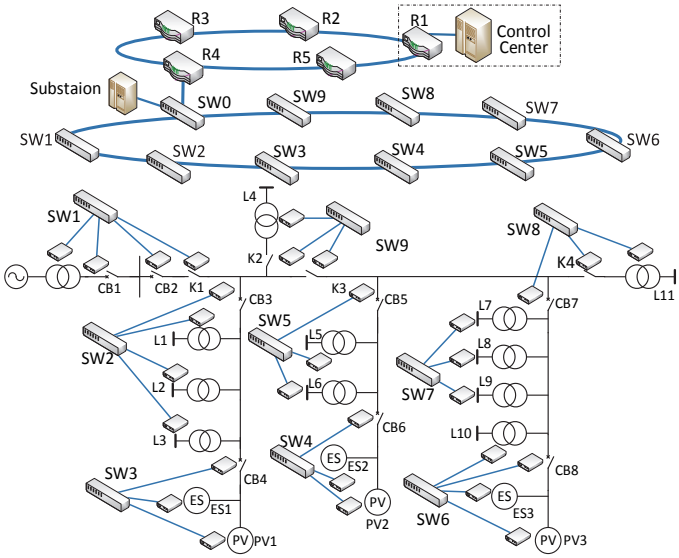


Fig.4 Test system structure

The distribution network consists of three PV units and three energy storage units, whose parameters are shown in TABLE I. There are eleven energy users in the network, and the load profile is shown in TABLE II. The reliability parameters, such as the failure rate and repair time of physical and cyber elements in the system, are shown in TABLE III and could refer to [8, 46, 47]. And the threshold setting of cyber subsystem delay may be obtained from [48].

TABLE I. PHOTOVOLTAIC POWER GENERATION AND ENERGY STORAGE PARAMETERS

PV	PV capacity (MW)	Energy storage	Maximum power (MW)	Capacity (MW·h)
1	1.2	1	0.9	4.5
2	0.5	2	0.4	2
3	1.2	3	0.9	4.5
PV total capacity	2.9 MW	Energy storages	2.2 MW	11 MW·h

TABLE II. LOAD DATA OF PHYSICAL SUBSYSTEM

User	Load (MW)	User	Load (MW)	User	Load (MW)
1	0.3764	5	0.2748	9	0.2382
2	0.2139	6	0.1094	10	0.2931
3	0.2431	7	0.1761	11	0.1072
4	0.1459	8	0.2098		
General load			2.3879 MW		

TABLE III. RELIABILITY DATA OF EQUIPMENT

Physical component	Failure rate	Repair time	Cyber component	Failure rate	Repair time
Distribution line	0.05f/(km·a)	5h	Optical fiber	0.004f/(km·a)	24h
Switches	0.005f/a	8h	Ethernet switch	0.05f/a	12h
Breaker	0.002f/a	4h	SDH switch	0.05f/a	12h
PV	3f/a	20h	IED	0.06f/a	12h
Storages	5f/a	10h	Server	0.01f/a	8h
Transformer	0.015f/a	200h			

B. Results Analysis

In order to analyze the influence of cyber subsystem on the CPDS reliability, four cases are mainly studied:

Case 1: Only the physical fault is considered, while the cyber subsystem is deemed totally reliable.

Case 2: The faults of both physical and cyber subsystems are considered, and the cyber access network operates under the light load (network load ratio ρ = 20%).

Case 3: The faults of both physical and cyber subsystems are considered, and the cyber access network operates under the medium load (network load ratio ρ = 50%).

Case 4: The faults of both physical and cyber subsystems are considered, and the cyber access network operates under the heavy load (network load ratio ρ = 80%).

In the four cases described above, the proposed method is used to calculate the reliability indices, and the results obtained are shown in TABLE IV.

TABLE IV. RELIABILITY RESULTS

	EENS (MWh/Year)	SAIDI (h/user·year)
Case 1	0.020409	0.044770
Case 2	0.063108	0.070663
Case 3	0.078640	0.082056
Case 4	0.117908	0.113147

As can be seen from the results, the reliability indices of Case 1 is rather lower than those of other cases, which indicates that the random fault in the cyber subsystem compromises the reliability of CPDS. In addition, the reliability indices of Case 2 are much higher than those of Case 1. Messages are not delayed in Case 2 because of the light traffic. Thus, communication interruption is the only factor affecting CPDS reliability under light traffic. However, the system reliability indices of Case 3 and Case 4 are significantly higher than those of Case 2, which indicates that the communication delay has vital influence on the CPDS reliability, especially under heavy traffic conditions. And the reliability indices obtained in Case 2, Case 3 and Case 4 are in ascending order, indicating that the message delay has an increasing impact on the reliability of CPDS with the growth of access network traffic.

In order to illustrate the interdependencies mechanism, a time instant is specified, a fault in $L11$ occurs while the $SW8$ fails under medium traffic. $K4$ cannot communicate with the control center such that $K4$ cannot effectively isolate the fault. The monitoring message from $K3$ is valid with 0.2579s delay. The control center decides that the fault occurs in the downstream from $K3$ and will send control signals to $K3$ for isolation. These faults result in a load loss ranging from 0.1072 MW to 1.4086 MW.

C. Influence Analysis of Different Cyber Element Faults on CPDS Reliability

In order to discuss the influence of each type of cyber element's fault on the CPDS reliability, in this study the reliability of CPDS is calculated under different settings by assuming the studied element is likely to fail while other elements are completely reliable. The obtained results are shown in TABLE V.

TABLE V. RELIABILITY INDICES UNDER DIFFERENT TRAFFIC CONDITIONS

Traffic condition	Unreliable element	EENS (MWh/Year)	SAIDI (h/user·year)
Light	None	0.019560	0.045460
	All	0.064183	0.070957
	Server	0.020912	0.047089
	SDH switch	0.034024	0.053402
	Ethernet switch	0.038433	0.055355
	IED	0.023367	0.048290
	Backbone optical fiber	0.021124	0.046157
	Access optical fiber	0.025785	0.049649
Medium	None	0.035379	0.057361
	All	0.075099	0.078735
	Server	0.036052	0.058089
	SDH switch	0.048096	0.060978
	Ethernet switch	0.052910	0.062587
	IED	0.040332	0.062035
	Backbone optical fiber	0.037665	0.060500
	Access optical fiber	0.042251	0.059752

As can be seen from the results, the calculated reliability indices can be listed in a descending order as follows: Ethernet Switch, SDH Switch, Ethernet Line, IED, SDH Line and Server. The reason why the Ethernet switch has the greatest impact on reliability is that the Ethernet switch is not only connected to other switches, but also connected to many IEDs. Once the Ethernet switch fails, the transmission of the connected IED will be interrupted, and the transmission from other switches will also be affected. Then, the impact of SDH switches on reliability is smaller than that of Ethernet switches. This is because only the fault of the SDH switch connected to the Ethernet or the server will result in invalid transmission. And if other SDH switches fail, the standby path can be established through route reconstruction, which can effectively mitigate the effects caused by the single fault. In addition, the server cannot significantly impact the CPDS reliability as expected, though the server fault would compromise the automation function. The main reason is the low failure rate because of the enhanced protection of the server, so the server outage has little impact on the reliability indices. Besides, the faults of IED and communication line do adversely impact on CPDS reliability to a certain extent. The IED fault can lead to the loss of messages which are transmitted from/to an element.

In order to investigate the impact of cyber element faults on load loss, statistics are derived on the frequency and the mean value of further load loss caused by cyber fault, as shown in Fig.5. Among those outages which cyber faults impose impact on slightly or heavily, the frequency of further outage caused by server fault is rather low, which is about 1%. But the load loss of further outage is rather high, and the proportion of further load loss due to server fault is 44.35%. Server fault can be regarded as a low-probability, high-impact event. In addition, the load loss caused by the Ethernet switch and line fault is indeed larger than that caused by the SDH switch and line fault – the underlying reason has been discussed previously. Also the frequency of further outage caused by IED fault is very high due to the high failure rate and the large amounts.

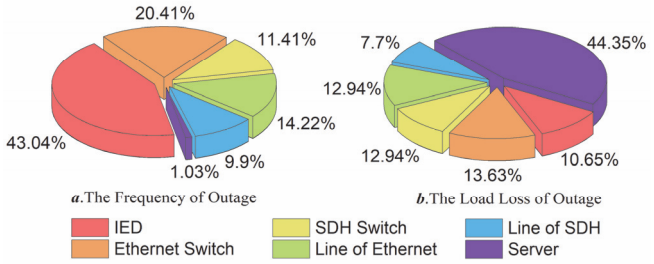


Fig. 5 The impact of cyber fault on load loss under medium traffic. (***a***) The frequency of further outage caused by cyber elements faults, (***b***) The load loss of further outage caused by cyber elements faults

D. Influence Analysis of Cyber Failure Rate on CPDS Reliability

In order to study the impact of cyber elements with different failure rates on the CPDS reliability, and to identify the element which is most significant in improving system reliability, the failure rate of each kind increases or decreases 90% by 1% step-size with other element failure rates being constant. Through linear fitting of the results, the trend of CPDS reliability changes over failure rate is obtained, as shown in Fig.6.

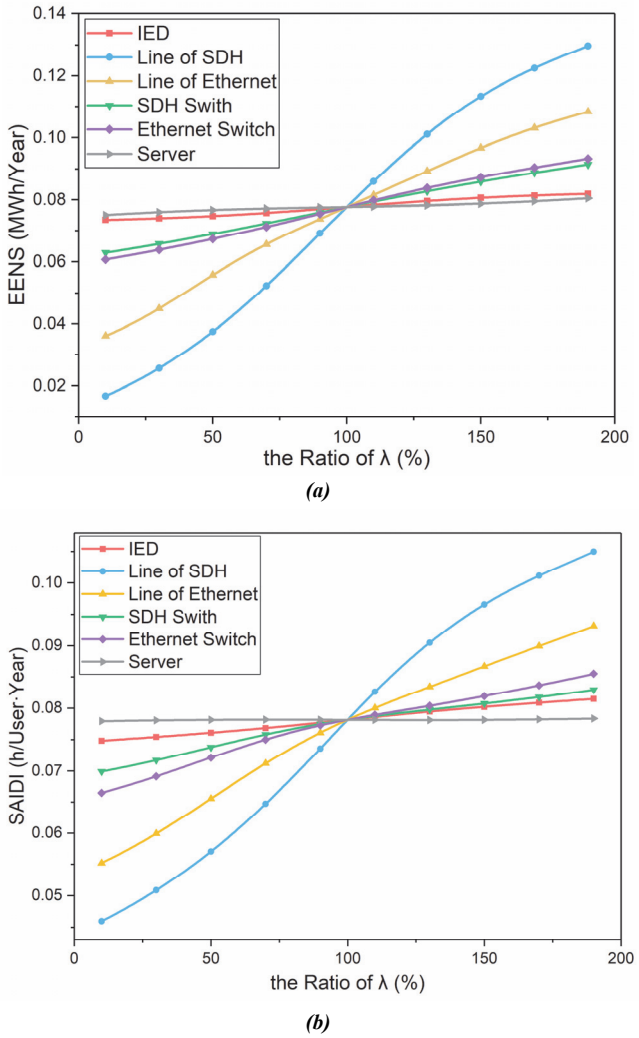
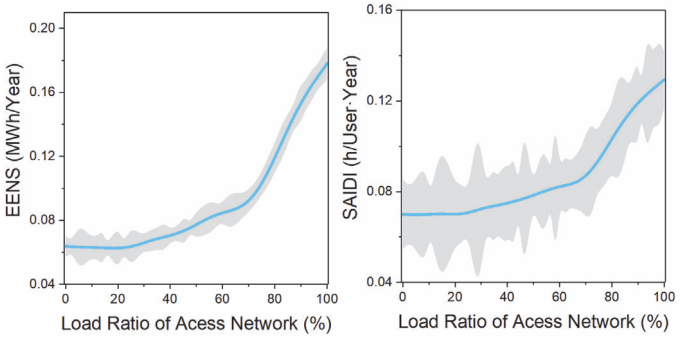


Fig. 6 The trend of reliability indices under different element failure rates. (***a***) The trend of EENS under different element failure rates, (***b***) The trend of SAIDI under different element failure rates

It can be seen that the failure rate of each element, particularly the optical line, has a significant influence on the reliability, which is more worthy of attention in the planning, construction and maintenance activities. Small improvements in line availiability can bring about significant gains. Generally, IED is mainly responsible for status acquisition and instruction execution. The IED fault only affects message execution (not the transmission), but Ethernet switch fault will affect it directly or indirectly. Once a switch fault occurs, IED directly connected to it will not be able to upload messages or execute instructions. However, the messages sent by other switches can still be transmitted with longer delay caused by reconfiguration. Hence, compared to IED, the change of switch failure rate has more significant impact on the reliability, and more attention should be paid to the improvement of switch reliability. However, because the server protection measures have been improved, improving reliability through the server cannot be achieved immediately.

E. Influence of Access Network Traffic on CPDS Reliability

In order to analyze the influence that the access network traffic has on the reliability, the mean load ratio of access network will increase from 0 to 100%, and step-size is 0.1%. The curves indicating the relationships between the reliability indices and different mean load ratios can be obtained.



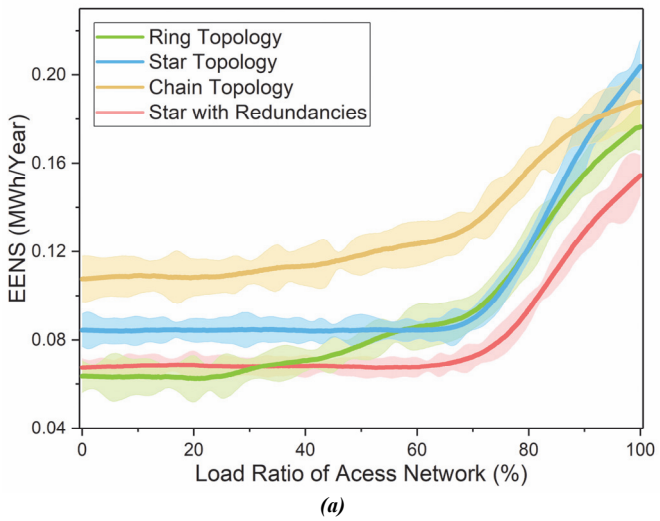
a ***b***

Fig. 7 Relationship curve between reliability indices and mean load ratio. (***a***) the curve of EENS under varying mean load ratios of access network, (***b***) The curve of SAIDI under varying mean load ratios of access network

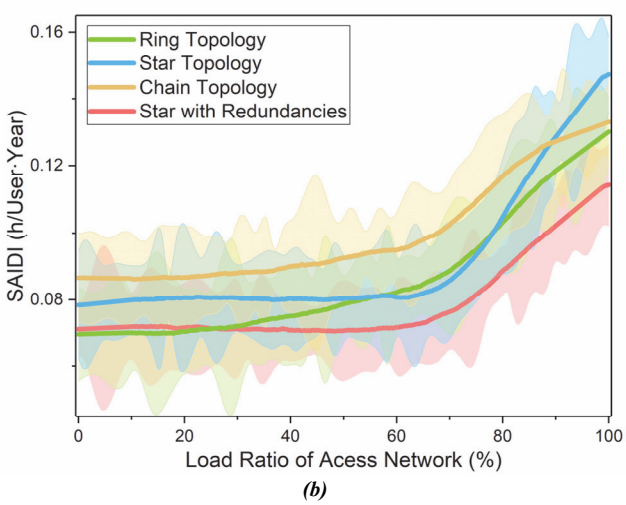
As shown in Fig.7, the reliability indices significantly increase with the access load ratios which are above 40%. The transmission average delay grows with the load ratio, resulting in the increased number of invalid links, impacting the distribution automation and finally worsening the reliability.

F. Influence of Access Topologies on CPDS Reliability

In addition to reducing the occurrences of element faults and managing the network traffic, CPDS reliability can also be enhanced by optimizing the framework of cyber network. Here the reliability indices under four typical network topologies are compared, as shown in Fig.8.



(a)



(b)

Fig. 8 Curves of reliability indices under different network topologies. (***a***) EENS Curves under different network topologies, (***b***) SAIDI Curves under different network topologies

It can be seen that the chaintopology without redundancies features the lowest reliability, and the reliability of star topology is lower than that of ring topology; while the reliability of star topology with redundancies is significantly higher than others. Because the transmission of this topology cannot be interrupted by other routing, the delay of the main routing is basically the same as that of the alternate routing. However, the complexity of the star topology with redundancies is rather high, so its corresponding construction cost could be excessively high.

G. Influence of Communication Technology on the CPDS Reliability

In the current active distribution systems, EPON (Ethernet Passive Optical Network) is widely used as an efficient access communication technology. Assuming that all the cyber links are valid, the test system with EPON is simulated based on the parameters in [49], and the results are shown in TABLE VI.

TABLE VI. RELIABILITY INDICE RESULTS IN DIFFERENT ACCESS COMMUNICATION TECHNOLOGIES

	Topology	EENS (MWh/year)	SAIDI (h/user·year)
Industrial Ethernet	Ring topology	0.048206	0.059508
	Chain topology	0.077223	0.075565
	Star topology	0.052336	0.060945
	Star with redundancies	0.033703	0.052148
EPON	Chain topology	0.200232	0.185781
	Double chain topology	0.198631	0.134608

Obviously, the CPDS reliability is relatively low when using EPON. Theoretically, the reliability of the chain topology is worse than the double chain. But the reinforced topology, namely the double chain EPON network, cannot significantly improve the CPDS reliability as expected. So it is necessary to improve the reliability through targeted enhancement of the weak but critical elements.

VII. CONCLUSION

This paper proposes a new model to evaluate link validity with the consideration of dynamic routing, delay and communication error. The influence of cyber fault on the physical reliability is quantified by taking distribution automation as a study case. Finally, the influence of cyber validity on CPDS reliability is verified based on Monte Carlo simulation. The results show that the traffic has a great impact on CPDS reliability, and more attention should be paid to optical line due to its adverse impact. Notably, the effect of double chain communication network on CPDS reliability is overestimated when cyber subsystem is built with EPON. In this paper, some assumptions and simplifications, especially in the cyber model, are made due to the large amount of equipment and the variety of communication technologies. The current research is focused on the interdependency issue of cyber fault in the traditional distribution automation system, but in the future systems with enhanced, more comprehensive active control, the interdependency issue will not only be related to distribution automation, but also be associated with distribution generation, microgrid, demand side response, etc. [50]. In particular, the emerging multi-energy systems demand more active controls, making the interdependency problem more complex. Besides, the simulation method used in this paper could be improved to become very efficient in calculating reliability indices in the future research.

REFERENCES

[1] C. D'Adamo, S. Jupe, C. Abbey, "Global survey on planning and operation of active distribution networks—Update of CIGRE C6.11 working group activities", *Proc. 20th Int. Conf. Exhibit. Elect. Distrib.*, pp. 1-4, 2009.

[2] N. Moreira, E. Molina, J. Lázaro, E. Jacob, and A. Astarloa, "Cyber-security in substation automation systems," *Renewable and Sustainable Energy Rev.*, vol. 54, pp. 1552-1562, 2016.

[3] B. Falahati and Y. Fu, "A study on interdependencies of cyber-power networks in smart grid applications," in *Proc. IEEE ISGT*, Washington D.C., DC, USA, 2012.

[4] B. Falahati, Y. Fu, and W. Lei, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, Sep. 2012.

[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, July 2014.

[6] H. Lei, and C. Singh, "Power system reliability evaluation considering cyber-malfunctions in substations," *Electr. Power Syst. Res.*, vol. 129, pp. 160-169, 2015.

[7] T. Zhao, D. Wang, D. Lu, Y. Zeng, and Y. Liu, "A risk assessment method for cascading failure caused by electric cyber-physical system (ECPS)," *2015 5th Int. Conf. on Electr. Utility Deregulation and Restructuring and Power Technol. (DRPT)*, Changsha, 2015, pp. 787-791.

[8] Y. Han, Y. Wen, C. Guo, and H. Huang, "Incorporating Cyber Layer Failures in Composite Power System Reliability Evaluations," Energies, vol. 8, no. 9, pp. 9064-9086, 2015.

[9] M. Parandehgheibi, E. Modiano, and D. Hay, "Mitigating cascading failures in interdependent power grids and communication networks," *2014 IEEE Int. Conf. on Smart Grid Commun*, Venice, pp. 242-247, 2014.

[10] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour, and A. Safdarian, "Impact of WAMS Malfunction on Power System Reliability Assessment," *IEEE Trans. on Smart Grid*, vol. 3, no. 3, pp. 1302-1309, 2012.

[11] F. Yang, A. P. S. Meliopoulos, G. J. Cokkinides and Q. B. Dam, "Effects of Protection System Hidden Failures on Bulk Power System Reliability," *2006 38th North Am. Power Symp.*, Carbondale, pp. 517-523, 2006.

[12] Y. Zhang, Y. Xiang, and L. Wang, "Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems," *IEEE Trans. on Smart Grid*, vol. PP, no. 99, pp. 1-15, 2016.

[13] X. Sun, N. Huang, B. Wang and J. Zhou, "Reliability of cyber physical systems assessment of the aircraft fuel management system," *Int. Conf. on Cyber Technol. in Automat., Contr. and Intell.*, Hong Kong, pp. 424-428, 2014.

[14] S. Nannapaneni, S. Mahadevan, S. Pradhan and A. Dubey, "Towards Reliability-Based Decision Making in Cyber-Physical Systems," *2016 IEEE Int. Conf. on Smart Comput. (SMARTCOMP)*, St. Louis, pp. 1-6, 2016.

[15] Y. Zhang, L. Wang, Y. Xiang, and C. W. Ten, "Power System Reliability Evaluation With SCADA Cybersecurity Considerations," *IEEE Trans. on Smart Grid,* vol. 6, no. 4, pp. 1707-1721, 2017.

[16] K. Marashi, S. S. Sarvestani, A. R. Hurson, K. Marashi, S. S. Sarvestani, and A. R. Hurson, "Consideration of Cyber-Physical Interdependencies in Reliability Modeling of Smart Grids," *IEEE Trans. Sustainable Comput.*, vol. PP, no. 99, pp. 1-1, 2017.

[17] G. Celli, E. Ghiani, F. Pilo and G. G. Soma, "Impact of ICT on the reliability of active distribution networks," *CIRED 2012 Workshop: Integration of Renewables into the Distrib. Grid*, Lisbon, pp. 1-4, 2012.

[18] D. Schacht, D. Lehmann, H. Vennegeerts, S. Krahl, and A. Moser, "Modelling of interactions between power system and communication systems for the evaluation of reliability," *2016 Power Syst. Comput. Conf. (PSCC)*, Genoa, pp. 1-7, 2016.

[19] Z. Huang, C. Wang, S. Ruj, M. Stojmenovic, and A. Nayak, "Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory," *Conf. on Ind. Electron. and Appl. (ICIEA)*, Melbourne, pp. 1023-1028, 2013.

[20] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Characterization of Cascading Failures in Interdependent Cyber-Physical Systems," *IEEE Trans. Comput.*, vol. 64, no. 8, pp. 2158-2168, Aug. 1 2015.

[21] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-Physical Modeling and Cyber-Contingency Assessment of Hierarchical Control Systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2375-2385, Sept. 2015.

[22] M. Panteli and D. S. Kirschen, "Assessing the effect of failures in the information and communication infrastructure on power system reliability," *IEEE PES Power Syst. Conf. and Exposition*, Phoenix, pp. 1-7, 2011.

[23] 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, January 2013.

[24] M. Bessani, R. Z. Fanucchi, A. C. C. Delbem, and C. D. Maciel, "Impact of operators' performance in the reliability of cyber-physical power distribution systems," *IET Gener., Transm. Distrib.*, vol. 10, no. 11, pp. 2640-2646, 8 4 2016.

[25] H. Hashemi-Dezaki, H. Askarian-Abyaneh and H. Haeri-Khiavi, "Impacts of direct cyber-power interdependencies on smart grid reliability under various penetration levels of microturbine/wind/solar distributed generations," *IET Gener., Transm. Distrib.*, vol. 10, no. 4, pp. 928-937, 2016.

[26] C. Wang, T. Zhang, F. Luo, F. Li, and Y. Liu, "Impacts of Cyber System on Microgrid Operational Reliability," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1-1.

[27] M. Heidari-Kapourchali, M. Sepehry, L. Zhao and V. Aravinthan, "Reliability analysis of cyber-enabled power distribution system using sequential Monte-Carlo," *2015 North Am. Power Symp. (NAPS)*, Charlotte, pp. 1-6, 2015.

[28] B. Feng, Q. Fan, Y. Li, and D. Ding, "Research on framework of the next generation power communication transmission network," *Int. Conf. on Comput. Sci. and Electron. Eng. (ICCSEE)*, vol. 3, pp. 414-417, 2012.

[29] C. Y. Ho, T. E. Lee and C. H. Lin, "Optimal Placement of Fault Indicators Using the Immune Algorithm," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 38-45, Feb. 2011.

[30] R. Das, V. Madani, F. Aminifar, J. McDonald, S. S. Venkata, D. Novosel, A. Bose, and M. Shahidehpour, "Distribution Automation Strategies: Evolution of Technologies and the Business Case," *IEEE Trans. on Smart Grid*, vol. 6, no. 4, pp. 2166-2175, 2015.

[31] T. Sanislav, S. Zeadally, G. Mois and H. Fouchal, "Multi-agent architecture for reliable Cyber-Physical Systems (CPS)," *2017 IEEE Symp. on Comput. and Commun. (ISCC)*, Heraklion, pp. 170-175, 2017.

[32] S. Lazarova-Molnar, N. Mohamed, and H. R. Shaker, "Reliability modeling of cyber-physical systems: A holistic overview and challenges," *Model. and Simul. of Cyber-Phys. Energy Syst. (MSCPES)*, Pittsburgh, pp. 1-6, 2017.

[33] D. Schacht, S. Patzack, H. Vennegeerts, S. Krahl, and A. Moser, "Selection of relevant failure modes and system states for the evaluation of reliability in distribution grids depending on ICT," *CIRED Workshop 2016*, Helsinki, pp. 1-4, 2016.

[34] S. Wang, D. Liang, L. Ge and X. Wang, "Analytical FRTU deployment approach for reliability improvement of integrated cyber-physical distribution systems," *IET Gener., Transm. Distrib.*, vol. 10, no. 11, pp. 2631-2639, 2016.

[35] D. Guo and X. Wang, "Bayesian inference of network loss and delay

characteristics with applications to TCP performance prediction," *IEEE Trans. Signal Processing*, vol. 51, no. 8, pp. 2205-2218, Aug. 2003.
[36] W. Ma, Y. Zhang, Z. Xia, Y. Si, H. Zhang, Y. Zhu, W. Wang, and M. Xu, "The Application of EPON Communication Technology in Intelligent Substation Automation Equipment," *Int. Conf. on Machinery, Mater. and Comput. Technol.* 2016.
[37] H. Li, H. Zhang and D. Peng, "Research and design of Industrial Ethernet communication gateway on power station," *Int. Conf. on Transport., Mechanical, and Electr. Eng. (TMEE)*, 2011, pp. 986-989, Changchun.
[38] B. Falahati, and Y. Fu, "Faults and failures in cyber-power interdependent networks," *T&D Conf. and Exposition, 2014 IEEE PES*, pp. 1-5, 2014.
[39] T. Skeie, S. Johannessen, and O. Holmeide, "Timeliness of Real-Time IP Communication in Switched Industrial Ethernet Networks," *IEEE Trans. on Ind. Informat.*, vol. 2, no. 1, pp. 25-39, 2006.
[40] B. Falahati, M. J. Mousavi, M. Vakilian, "Latency considerations in IEC 61850-enabled substation automation systems," *IEEE Power and Energy Society Gen. Meeting*, pp. 1-8, 2011.
[41] J. Shen, and C. Yu, "The Study on the Self-Similarity and Simulation of CPS Traffic," *2013 IEEE 11th Int. Conf. on Dependable, Autonomic and Secure Comput.*, Chengdu, pp. 215-219, 2013.
[42] W. Zhang and J. He, "Statistical Modeling and Correlation Analysis of End-to-End Delay in Wide Area Networks," *Conf. on Softw. Eng., Artif. Intell., Netw., and Parallel/Distrib. Comput. (SNPD)*, Qingdao, pp. 968-973, 2007.
[43] I. Lokshina, T. Wendt and C. Lanting, "Accelerated buffer overflow simulation in self-similar queuing networks with long-range dependent processes and finite buffer capacity," *Symp. on Wireless Syst. within the Conf. on Intell. Data Acquisition and Adv. Comput. Syst.*, Offenburg, pp. 5-10, 2016.
[44] Y. Wang, D. Liu and Q. S. Li, "A hybrid system based cps model and control of loads in active distribution network," *2016 IEEE Int. Conf. on Power Syst. Technol. (POWERCON)*, 2016, pp. 1-8, Wollongong.
[45] A. Heidari, V. G. Agelidis, M. Kia, J. Pou, J. Aghaei, M. Shafie-Khah, and J. P. S. Catalão, "Reliability Optimization of Automated Distribution Networks with Probability Customer Interruption Cost Model in the Presence of DG Units," *IEEE Trans. on Smart Grid*, vol. 8, no. 1, pp. 305-315, 2017.
[46] C. Bhargava and P. S. R. Murty, "Reliability evaluation of radial distribution system using analytical and time sequential techniques," *2016 7th India Int. Conf. on Power Electron. (IICPE)*, pp. 1-6, 2016, Patiala.
[47] A. L. A. Syrri and P. Mancarella, "Reliability evaluation of demand response to increase distribution network utilisation," *2014 Int. Conf. on Probabilistic Methods Appl. to Power Syst. (PMAPS)*, Durham, pp. 1-6, 2014.
[48] D. Roberts, *Network Management Systems for Active Distribution NetworksA Feasibility Study*, DTI, 2004.
[49] F. Tang and X. Zha, "Reliability Analysis of Smart Distribution Grid Communication System Based on EPON," *2012 IEEE Asia-Pacific Power and Energy Eng. Conf.*, Shanghai, pp. 1-4, 2012.
[50] V. Madani, R. Das, F. Aminifar, J. McDonald, S. S. Venkata, D. Novosel, A. Bose, and M. Shahidehpour, "Distribution Automation Strategies Challenges and Opportunities in a Changing Landscape," *IEEE Trans. on Smart Grid*, vol. 6, no. 4, pp. 2157-2165, 2015.

Wenxia Liu (M'11) received her B.S. in Radio Eng. from Nanjing University of Science and Technology in 1990. And she received her M.S. in Power System & Automation from Northeast Electric Power University in 1995, and Ph.D. 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 system, power system risk assessment, power communication system, and reliability and planning of Cyber-Physical System (CPS).

Qi Gong (S'17) received the B.S. in Smart Grid Engineering from North China Electric Power University (NCEPU), Beijing, China in 2016. Currently, he is a M.S. student in Elec. Eng. with the same university. His research interests are CPS reliability, CPS operation, and distribution system operation.

Hui Han (S'18) received the B.S. in Electron. Sci. Technol. from North China Electric Power University (NCEPU), Beijing, China in 2017. Currently, she is a M.S. student in Elec. Eng. with the same university. Her research interests are cyber physical distribution system and active distribution network.

Zhiqiang Wang (M'12) received his B.S. in Elec. Eng. from Nanjing University of Science and Technology, in 1990. And he received his M.S. 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.

Lingfeng Wang (S'02-M'09-SM'18) received the B.E. degree in measurement and instrumentation from Zhejiang University, Hangzhou, China, in 1997; 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, where he directs the cyber-physical energy systems research group. He also serves as a Co-Director for the Department of Energy (DOE)'s Industrial Assessment Center. He was a faculty member with the University of Toledo, Toledo, OH, USA, and an Associate Transmission Planner with the California Independent System Operator, Folsom, CA, USA. His current research interests include power system reliability and resiliency, smart grid cybersecurity, critical infrastructure protection, energy-water nexus, renewable energy integration, intelligent and energy-efficient buildings, electric vehicles integration, microgrid analysis and management, and cyber-physical systems.

Dr. Wang is an Editor of the IEEE TRANSACTIONS ON SMART GRID, IEEE TRANSACTIONS ON POWER SYSTEMS, and IEEE POWER ENGINEERING LETTERS, and serves on the Steering Committee of the IEEE TRANSACTIONS ON CLOUD COMPUTING. He is also an Editorial Board Member for several international journals, including *Journal of Modern Power System and Clean Energy, Sustainable Energy Technologies and Assessments*, and *Intelligent Industrial Systems*. He served as a Co-chair for IEEE SmartGridComm'15 Symposium on Data Management, Grid Analytics, and Dynamic Pricing. He is a recipient of the Outstanding Faculty Research Award of College of Engineering and Applied Science at UWM in 2018.