Research Article
Reliability Evaluation for Cyber-Physical Smart Substation

Yangrong Chen,1 Jun’e Li,1 Ang Xu,2 Kai Yuan,3 and Kaipei Liu3

1Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China
2State Grid Wuhan Electric Power Supply Co., Ltd, Wuhan 430010, China
3School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China

Correspondence should be addressed to Jun’e Li; jeli@whu.edu.cn

Received 29 April 2021; Revised 6 July 2021; Accepted 7 October 2021; Published 21 October 2021

Academic Editor: Qiuye Sun

Copyright © 2021 Yangrong Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Smart substation is the key part of smart grid. The reliability of smart substation is extremely important to the safe and stable operation of the smart grid. Smart substation is a cyber-physical system (CPS). Hence, this paper conducts reliability evaluation study for smart substation from the perspective of CPS. Firstly, the basic reliability indices of cyber and physical elements of smart substation are presented. The reliability index of one cyber element takes into account the reliability factors of data leakage, tampering, loss and delay, etc., on the cyber side. Then, the cyber-physical interactions of smart substation are analyzed. It is concluded that the effect of the cyber side and cyber-physical interactions on the reliability of smart substation is reflected in the effect of measurement and control messages on circuit breaker operation. And, the new reliability indices considering cyber-physical interactions are proposed. Furthermore, the MALI-hybrid method, which combines the Monte Carlo method, analytical method, Latin hypercube sampling method, and important sampling method, is presented for evaluating the reliability of smart substation. Finally, the rationality of the proposed reliability indices, the efficiency, and correctness of MALI-hybrid method are verified by case studies.

1. Introduction

With the increasing intelligent electronic devices (IED) installation, smart substation can be regarded as a typical cyber-physical systems (CPSs), in which various types of information are being exchanged on a communication network [1]. Interruption, delay, communication errors, and various cyber attacks on the cyber side of smart substation probably cause misoperation or refusal of circuit breakers (CBs) and even affect the safe and stable operation of smart substation [2–6]. Meanwhile, malfunction on the physical side of smart substation may make cyber system lose right perception and real-time control for physical system, which in turn further affects the operation of power system and forms cascading failures [7, 8]. Thus, reliability evaluation for smart substation should consider the reliability factors on both the physical side and cyber side, and the interactions between the two sides.

1.1. Motivation. At present, there are few studies on the reliability evaluation of smart substation or power grid from the perspective of CPSs. Zhang [9] constructed a Markov model of physical elements under the influence of the secondary system and used state-space method to calculate the reliability of the physical elements considering the influence of the secondary system. However, the effect of the primary system on the reliability of the secondary system and the interactions between the two systems in smart substation are not considered. To evaluate the effect of communication system on power system, Tang et al. [10] established dynamic vulnerability matrix for evaluating real-time vulnerability of composite system considering communication faults such as time delay, bit error, and interruption. However, the effect of the power system on the communication system is not considered, and the research is not targeted at smart substation. Lei et al. [11] proposed a novel reliability modelling and analysis methodology using
cyber-physical interface matrix for modern substation protection systems. The study provides an idea for evaluating the reliability of substation based on cyber-physical integration, but research about reliability index system and quantitative calculations method is insufficient. Ten et al. [12] used existing power system simulators to evaluate the reliability of smart substations considering cyber attacks. However, this research focuses on analyzing the effect of cyber attacks on substations and does not consider the effect of the physical side on the cyber side and cyber-physical interactions on the reliability of substation. Liu et al. [13] presented an analytical method to quantify the effect of cyber fault on the reliability of physical system during distribution automation considering dynamic routing, delay, and communication error, particularly the cyber traffic. However, the study disregards the effect of the physical side on the cyber side and interactions between them. Aravinthan et al. [14] summarized the status and needs for reliability evaluation of cyber-physical power systems (CPPS) and standardized the CPPS model for reliability computation. This model could be a reference for research of reliability evaluation but cannot be directly used to evaluate the reliability of smart substation.

In addition, as we all know, stability is an important condition for maintaining the safe and reliable operation of the power system. The study about stability can help us do a better reliability evaluation. Wang et al. [15] proposed a droop coefficients stability region analysis approach for power system. Sun et al. [16] studied the stability analysis issues of Energy Internet. The authors in [17] have invented a novel small-signal modelling method based on the characteristic equation to assess the stability of complex microgrids. Reference [18] proposed a line impedance cooperative stability region identification method for grid-tied inverters under weak grids. Hu et al. [19] pointed that open-end winding machines provide better controllability and reliability than conventional start-connected machines. The above work provides guidance for power system reliability evaluation method researches.

Further, the data leakage, tampering, loss, network interruption, and delay also occur frequently in other industrial systems (e.g., pipeline network systems) [20]. And with the development of pipeline transportation, the requirements for safety and reliability of pipeline network systems have increased in recent years [21]. Thus, the study of new reliability indices considering cyber-physical interactions and evaluation methods can also provide the reference for other industrial systems.

From the above analysis, it can be seen that there are few literatures about reliability analysis and reliability evaluation method for smart substation from the perspective of CPSs. In our recent study, the interaction mechanism of the cyber side and the physical side of smart substation were analyzed preliminarily [22]. However, the reliability evaluation method is relatively simple and has low accuracy, the case study has some deficiencies, and the expression of formulas is not easy to read and understand for readers. Based on the above review of reliability evaluation and Ref. [22], this paper fully analyzes various reliability factors and how they affect the reliability of smart substation. Then, the calculation expressions of reliability indices are modified and improved so as to become easy to read and understand for readers. Furthermore, the MALI-hybrid reliability evaluation method, which has fast simulation speed and high precision, is presented. Finally, a more practical case is presented to verify the rationality of the proposed reliability indices and reliability evaluation method. Simulation results show that the proposed reliability indices are reasonable, and the presented reliability evaluation method can save simulation time with improving accuracy.

1.2. Contribution. The main contributions of this paper can be summarized as follows:

(1) A thorough analysis on the interactions between the cyber side and the physical side of smart substation is conducted. It is concluded that the reliability evaluation of smart substation should consider the effect of power grid disturbance and complicated operation states on the correctness of measurement information, and the effect of all factors on the reliability of smart substation is carried out by measurement and control messages, which affect the power system’s operation by the CB’s misoperation or refusal.

(2) The reliability indices are proposed for smart substation considering the reliability factors of the cyber side, the physical side, and the cyber-physical interactions. These indices involve the reliability index of cyber equipment considering its importance, the reliability index of communication links considering the reliability of data transmitting on them, and the equivalent reliability indices of CB considering cyber-physical interactions. The importance of cyber equipment refers to its effect on the communication business when the data leakage, packet error, message tampering or forgery, packet loss or interruption, and message delay occur, and it can be calculated by the proposed AHP model.

(3) A MALI-hybrid reliability evaluation method, which combines the Monte Carlo method, analytical method, LHS method, and important sampling method, is presented. This method has faster simulation speed and more precise evaluation results than the common reliability evaluation methods.

1.3. Organization. The rest of this paper is organized as follows. Section 2 presents the elements for reliability evaluation of smart substation. Section 3 gives the basic reliability indices of smart substation. Section 4 analyzes the interactions between the cyber side and the physical side of smart substation and proposes the reliability indices considering the effect of cyber-physical interactions. Section 5 presents a MALI-hybrid reliability evaluation method for smart substation. Section 6 verifies the rationality of the proposed reliability indices and the reliability evaluation method. Section 7 gives a summary and a future outlook.
2. Elements for Reliability Evaluation of Smart Substation

The D2-1 substation defined in IEC 61850 standard is widely used in practical engineering construction. Thus, we choose D2-1 smart substation as analysis object and elaborate the proposed reliability indices and reliability evaluation method. For better understanding the interactions between the cyber side and the physical side of smart substation, the communication network of D2-1 substation, of which the architecture is “three layers, two networks” as a common one of the present smart substations, is shown in Figure 1.

The topology of D2-1 smart substation is shown in Figure 2 [23]. The smart substation in Figure 2 contains 1 bus interval (BI), 6 feeder intervals (FI1-FI6), and 2 transformer intervals (TI1-TI2). The physical side contains buses, CBs, DSs, electrical voltage transformers (EVTs), and electrical current transformers (ECTs), which are connected by electrical lines. The cyber side contains merging unit (MU), intelligent electronic devices (IEDs), protection and control (P&C) IEDs, CB IEDs, and switches, which are connected by communication links.

Reliability evaluation of smart substation should consider the reliability of all the above elements. For formal description, the above elements are represented by nodes and branches as follows.

The MU IEDs, P&C IEDs, CB IEDs, and switches on the cyber side are abstracted as nodes of cyber system, which can be defined as the set $N_c:

$$N_c = \{N_{c1}, N_{c2}, \ldots, N_{cz} \},$$

where the set $\{N_{c1}, N_{c2}, \ldots, N_{cz} \}$ is the cyber equipment set on the cyber side.

The communication links are abstracted as branches of cyber system, which are defined as the set $B_c:

$$B_c = \{B_{c1}, B_{c2}, \ldots, B_{ck} \},$$

where the set $\{B_{c1}, B_{c2}, \ldots, B_{ck} \}$ is the communication link set on the cyber side.

The buses, transformers, CBs, DSs, EVTIs, and ECTs on the physical side are abstracted as nodes of physical system, which can be defined as the set $N_p:

$$N_p = \{N_{p1}, N_{p2}, \ldots, N_{pm} \},$$

where the set $\{N_{p1}, N_{p2}, \ldots, N_{pm} \}$ is the physical equipment set on the physical side.

In smart substation, though the connection wires between the physical devices are short, they are still abstracted as branches of physical system and are called primary electrical lines in this paper for the sake of generality. The connection wires are defined as the set $B_p:

$$B_p = \{B_{p1}, B_{p2}, \ldots, B_{pl} \},$$

where the set $\{B_{p1}, B_{p2}, \ldots, B_{pl} \}$ is the primary electrical line set on the physical side.

3. The Basic Reliability Indices

To study the factors affecting the reliability of smart substation, this section analyzes the basic reliability indices of elements in smart substation.

Reliability refers to the possibility of the equipment to operate normally under specified conditions over a period. Traditionally, the reliability of one element can be obtained according to the following equation:

$$R = \frac{\mu}{\lambda + \mu},$$

where $\lambda$ and $\mu$ are the failure rate and repair rate of the element, respectively.

3.1. Reliability Indices of Cyber Elements. As described in Section 2, cyber elements contain cyber equipment and communication links.

3.1.1. Reliability Indices of Cyber Equipment. The reliability factors of the cyber side play on the physical side through communication business. And the reliability of each communication device on the transmission link has different effects on communication business. Therefore, we use the equivalent failure rate $\lambda_{eq}$ of cyber equipment to take the place of $\lambda$ in equation (5). $\lambda_{eq}$ can be defined as follows:

$$\lambda_{eq} = \partial_i \cdot \lambda_i,$$

where $\partial_i$ is the importance degree of the cyber equipment (i.e., the effect of equipment failure on the reliable transmission of communication business; it is valued between 0 and 1); $\lambda_i$ is the failure rate of cyber equipment, the same as the meaning of $\lambda$ in equation (5).

In this paper, we employ an analytic hierarchy process (AHP) method to calculate the importance degree $\partial_i$ of cyber equipment. The AHP model is shown in Figure 3.

In Figure 3, the failure rate of cyber equipment is taken as the index layer. The effect of cyber equipment failure on the security, correctness, and real-time of communication business is taken as the criterion layer. The comprehensive effect of cyber equipment failure on communication business is taken as the target layer. In the criterion layer, the effect of cyber equipment failure on the security of communication business refers to data leakage caused by equipment failure; the effect of cyber equipment failure on the correctness of communication business refers to data error, tampering, and forgery of service messages caused by equipment failure; the effect of cyber equipment failure on the real-time of communication business refers to delay, loss, and interruption of service messages caused by equipment failure. It can be seen that the model takes into account both conventional faults and failures caused by cyber attacks. For the detailed calculation process of importance degree $\partial_i$, refer to Refs. [24].

3.1.2. Reliability Indices of Communication Links. The reliability of the communication link is not only related to the
**Figure 1:** The architecture of D2-1 smart substation.

**Figure 2:** Topology diagram of D2-1 smart substation.
reliability of the link itself, but also related to the reliability of data transmitting on it. According to the reliability calculation method of cascading systems, the reliability of one communication link can be calculated as follows:

\[
R(B_{k}) = R\left( B_{i_{1}} \cdots B_{i_{n}} \right) = CL_{i_{1} \cdots i_{n}} \cdot D,
\]

(7)

where \(R(B_{k})\) is the reliability of the \(k\)th communication link, a communication link from the cyber equipment \(N_{i_{1}}\) to \(N_{i_{n}}\), so it is also noted as \(R(B_{i_{1} \cdots i_{n}})\); \(CL_{i_{1} \cdots i_{n}}\) is the reliability of the link hardware, and \(D\) is the reliability of data transmitting on the link; \(CL_{i_{1} \cdots i_{n}}\) can be calculated by equation (5).

The reliability of data transmitting on the link is mainly related to propagation delay and error. In smart substation, optical fibers are used as the communication links, and the links are short. In the case of no attack, the delay is relatively stable and extremely small, so it can be ignored. Packets in smart substation have error detection mechanism, but any error detection mechanism has the possibility of missing detection. Therefore, this paper uses packet error rate (i.e., the omission rate of error detection method of the packet) to represent the effect of transmitting error on the reliability of data. We define \(P_{e}\) as the packet error rate. Thus, \(D\) in equation (7) can be calculated as follows:

\[
D = 1 - P_{e},
\]

(8)

3.2. Reliability Indices of Physical Elements. The reliability indices of the physical equipment and the primary electrical lines are usually obtained according to the operation of smart substation. This paper takes availability as the basic reliability index of physical elements, and the reliability can be calculated by equation (5).

4. Cyber-Physical Interactions and the Reliability Indices

The basic indices in Section 3 only consider the reliability factors of a single side, but do not consider the effect from another side and the interactions. This section analyzes the interactions between the cyber side and the physical side of smart substation, and then the reliability indices of smart substation considering the effect of the cyber side, the effect of the physical side, and the interactions are presented.

4.1. Interactions between Cyber Side and Physical Side. The main function of smart substation is to convert high and low voltage. The bus voltage monitoring and tripping, two of the communication business of smart substation, can best reflect the interactions between cyber side and physical side. Hence, we take the bus voltage monitoring and tripping as the example to analyze the cyber-physical interaction mechanism of smart substation.

The process of bus voltage monitoring and tripping can usually be described as follows. First, bus voltage from the physical side is sampled and converted into analog or digital signals by local measurement equipment. Second, the data enclosed in packets is transmitted to the control center of the station level via the communication networks. Third, a centralized application conducts online computation on the basis of the received packets and generates tripping commands to regulate physical equipment. Forth, these control commands are sent back to the physical side via the communication networks again, and the related physical devices take actions according to the tripping commands they received. Finally, the physical state of the smart substation is changed as a consequence of the closed-loop control. Both the beginning and end of the closed-loop control are connected to the physical side; thus, the cyber side and the physical side in smart substation show an interactive relationship [25–27].

4.1.1. Effect of the Cyber Side on the Physical Side. Measurement information (e.g., bus voltage) from the physical side transmits from EVTs/ECTs to MU IEDs, and then the measurement information enclosed in sampled value (SV) messages is relayed to P&C IEDs. P&C IEDs decide whether to send the control messages according to SV messages and control strategy. Finally, P&C IEDs send generic object oriented substation event (GOOSE) messages containing tripping messages to the corresponding CB IEDs and control the action of CBs.
During the above communication process, cyber contingencies, no matter whether they are accidental faults or malicious attacks, may lead to the inappropriate operation of CBs, even a large-scale power outage. Moreover, the above description shows that the effect of the cyber side on the physical side in smart substation is mainly conducted through controlling CBs. And the control process is carried out by communication messages and equipment of the cyber side.

4.1.2. Effect of the Physical Side on the Cyber Side and the Cyber-Physical Interactions. The effect of the physical side on the cyber side and the cyber-physical interactions of smart substation is as follows.

Physical equipment supplies power for local cyber equipment. Failure of physical system will result in the inability to supply power for cyber equipment [28]. While in practice, an independent uninterrupted power supply is usually used to supply power for cyber equipment when the power system fails. That is, a short power outage does not affect the normal operation of cyber system.

When the power system fails, it is very likely that multiple IEDs will send out a large number of GOOSE messages in a short interval [29]. The surge of GOOSE messages might cause the network congestion and messages to be delayed and even cause system decision-making error. The congestion caused by power system fails, excluding attacks, can be avoided by a well-planned network of the cyber system.

ETs are more susceptible to electromagnetic interference in operation than traditional transformers due to their diverse sensing principles and a large number of electronic components in the primary body [7]. Specially, since the installation site of ETs is close to the electrical lines, they are more susceptible to interference through direct conduction and electromagnetic field coupling under the conditions of on-off operation and short-circuit. The effect of electromagnetic interference on ETs may lead to errors in measurement information, and even malfunction of ETs, which may make protection or regulation go away.

Because of the complex structure of the power grid, there is sympathetic interaction between the nonlinear ferromagnetic elements, such as the transformers and the ETs, which might result in the complex transient process [30]. This might lead the existing detection methods to correctly identify the operation state of power grid, then the protective devices malfunction due to error of measurement information.

Due to the access of new energy systems, the application of AC/DC (alternating current/direct current) hybrid transmission, and the application of FACTS (flexible alternating current transmission) devices, the behavior of modern power systems is becoming more and more complicated. Meanwhile, most of the existing protective devices filter out high-frequency transient components and do not use high-frequency transient components. Therefore, for the AC/DC hybrid power systems connected with new energies, the detection method that only retains power frequency components and finite harmonic components cannot accurately detect the operating status of complicated power systems and may give wrong measurement information and lead to wrong protection actions.

The reliable operation of smart substation relies on accurate detection and identification to power system status (e.g., operating status, fault identification, etc.). According to the above analysis, we can conclude that (1) the measurement information errors caused by grid disturbance and complicated running state become the main factors to be considered in the reliability evaluation of smart substation; (2) in smart substation, both the effect of cyber side on physical side, the effect of physical side on cyber side, and the interaction are delivered through the measurement and control messages, and the misoperation or refusal of the CBs resulting from wrong measurement or control messages will further affect the safe and reliable operation of the power system. Thus, the effect of the cyber side and cyber-physical interactions on the reliability of smart substation can be obtained through analyzing the effect of measurement and control messages on the actions of CBs.

4.2. Message Flows Related to Cyber-Physical Interactions. To analyze the reliability of measurement and control messages and their effect on the action of CBs, it is needed to analyze the transmission paths of measurement and control messages. The reliability of the messages can be calculated according to the reliability of the elements on the transmission path. Further, equivalent reliability of CBs considering the cyber-physical interactions is obtained.

In smart substation, there are SV messages, GOOSE messages, manufacturing message specification (MMS) messages, etc. According to the analysis in Section 4.1, the interaction between the cyber side and the physical side is mainly related to the process level. Therefore, to simplify the analysis, this paper mainly focuses on analyzing the SV and GOOSE messages of the process level. The simplified communication network topology of the smart substation in Figure 4 and the message flows of its process level are shown in Figure 4. In this figure, only one transformer interval and one feeder interval are presented for simplifying the description, but all of the elements in smart substation should be involved in practice.

In Figure 4, the digit on each device is the node number of the device. S1, S2, . . . , S5 refer to the flows of SV messages encapsulating the measurement information (e.g., voltage, current, and system frequency). G1, G2, . . . , G14 refer to the GOOSE message flows, in which G1, G2, . . . , G4 are the flows of messages encapsulating breaker positions, G5, G6, . . . , G9 are the flows of messages encapsulating remote control commands, G10, G11 and G12 are the flows of messages encapsulating primary remote information, and G13 and G14 are the flows of messages encapsulating blocking signals.

We denote the transmission path as $L_{ij}$, referring to the set of nodes on the transmitting path of one message, in which $i$ is the number of the source nodes and $j$ is the number of the destination nodes of the message. Table 1
presents the transmission paths of the message flows in Figure 4.

### 4.3. Reliability Indices considering Cyber-Physical Interactions

The nodes of one transmission path are in series. Thus, the reliability of one message can be obtained according to the following equation:

\[
R_{\text{message}} = R(N_{c_1}) \cdot R(N_{c_2}) \cdot \ldots \cdot R(N_{c_n}) \cdot R(B_{c_1}) \cdot R(B_{c_2}) \cdot \ldots \cdot R(B_{c_k}),
\]

(9)

where \(R(N_{c_i})\) is the reliability of cyber equipment, the same as the meaning of \(R\) in equation (5); \(R(B_{c_i})\) is the reliability of communication link, the same as the meaning of \(R(B_{c_i})\) and \(R(B_{c_{i-1}})\) in equation (7).

#### 4.3.1. Reliability of CB considering the Reliability Factors of the Cyber Side

As concluded above, the cyber side affects the physical side through GOOSE messages controlling CBs and affected by SV messages in smart substation. Therefore, the reliability of one CB, considering the reliability factors of the cyber side, can be presented in the following equation:

\[
R'(N_{p\text{CB}}) = R(N_{p\text{CB}}) \cdot R_{SV} \cdot R_{\text{GOOSE}},
\]

(10)

where \(R(N_{p\text{CB}})\) is the reliability of one CB without considering the reliability factors of the cyber side; \(R_{SV}\) is the reliability of the SV messages without considering the measurement information errors; \(R_{\text{GOOSE}}\) is the reliability of the GOOSE messages; \(R_{SV}\) and \(R_{\text{GOOSE}}\) can be calculated according to equation (9).

---

**Figure 4**: Communication network topology and message flows of the process level in smart substation.

**Table 1**: Transmission paths of the message flows in Figure 4.

| Message flow | Denotation | Transmission path |
|--------------|------------|------------------|
| S1           | \(L_{1-2}\) | 1 \(\rightarrow\) 13 \(\rightarrow\) 2 |
| S2           | \(L_{4-5}\) | 4 \(\rightarrow\) 14 \(\rightarrow\) 5 |
| S3           | \(L_{4-6}\) | 4 \(\rightarrow\) 14 \(\rightarrow\) 6 |
| S4           | \(L_{4-9}\) | 8 \(\rightarrow\) 15 \(\rightarrow\) 9 |
| S5           | \(L_{4-10}\) | 8 \(\rightarrow\) 15 \(\rightarrow\) 10 |
| G1           | \(L_{3-1}\) | 3 \(\rightarrow\) 13 \(\rightarrow\) 1 |
| G2           | \(L_{7-4}\) | 7 \(\rightarrow\) 14 \(\rightarrow\) 4 |
| G3           | \(L_{11-8}\) | 11 \(\rightarrow\) 15 \(\rightarrow\) 8 |
| G4           | \(L_{12-8}\) | 12 \(\rightarrow\) 15 \(\rightarrow\) 8 |
| G5           | \(L_{2-3}\) | 2 \(\rightarrow\) 13 \(\rightarrow\) 3 |
| G6           | \(L_{2-7}\) | 2 \(\rightarrow\) 13 \(\rightarrow\) 16 \(\rightarrow\) 14 \(\rightarrow\) 7 |
| G7           | \(L_{2-11}\) | 2 \(\rightarrow\) 13 \(\rightarrow\) 16 \(\rightarrow\) 15 \(\rightarrow\) 11 |
| G8           | \(L_{6-7}\) | 6 \(\rightarrow\) 14 \(\rightarrow\) 7 |
| G9           | \(L_{10-12}\) | 10 \(\rightarrow\) 15 \(\rightarrow\) 12 |
| G10          | \(L_{1-2}\) | 3 \(\rightarrow\) 13 \(\rightarrow\) 2 |
| G11          | \(L_{1-6}\) | 7 \(\rightarrow\) 14 \(\rightarrow\) 6 |
| G12          | \(L_{12-10}\) | 12 \(\rightarrow\) 15 \(\rightarrow\) 10 |
| G13          | \(L_{6-2}\) | 6 \(\rightarrow\) 14 \(\rightarrow\) 16 \(\rightarrow\) 13 \(\rightarrow\) 2 |
| G14          | \(L_{16-2}\) | 10 \(\rightarrow\) 15 \(\rightarrow\) 16 \(\rightarrow\) 13 \(\rightarrow\) 2 |
4.3.2. Reliability of CB considering the Effect of the Physical Side on the Cyber Side and Cyber-Physical Interactions.

The effect of the physical side on the cyber side is mainly caused by measurement information and its transmission. The reliability of SV messages considering the effect of the physical side on the cyber side can be defined as

\[ R_{SV} = (1 - \zeta_r) \cdot R(N_{pca}) \cdot R_{SV}, \]

where \( R(N_{pca}) \) is the reliability of one ET; \( \zeta_r \) is the error rate of measurement information, which refers to the error occurrence probability of the measurement information transmitted to MU when the ET operates normally. The error rate is mainly affected by grid disturbance and complicated running state and can be obtained from actual statistics of running data. \( R_{SV} \) is the same as that in equation (10).

When the reliability of SV messages is reduced, the corresponding CBs cannot be controlled correctly by the cyber side in smart substation. That is, the effect of physical side on cyber side might be ultimately revealed on the physical side of smart substation. Therefore, considering the interactions between the cyber side and the physical side, the reliability of one CB can be defined as

\[ R'(N_{pca}) = R(N_{pca}) \cdot R_{SV} \cdot R_{GOOSE}, \]

where \( R(N_{pca}) \) and \( R_{GOOSE} \) are the same as those in equation (10), and \( R_{SV}' \) is the same as that in equation (11).

5. Reliability Evaluation Method for Smart Substation

We take D2-1 smart substation shown in Figure 2 as an example to illustrate the reliability evaluation method proposed in this paper.

5.1. System Reliability Index of Smart Substation

The main electrical connection can reflect the connection relationship of primary equipment in smart substation. The main electrical connection of D2-1 smart substation is shown in Figure 5.

To analyze the reliability of smart substation, we convert the main electrical connection diagram in Figure 5 into a logical correlation diagram as shown in Figure 6. To simplify the simulation and calculation, only two feeder lines are presented in Figure 6.

The circle in Figure 6 represents the combination of the primary equipment. L1 and L2 represent the series combination of transformer, electrical lines, EVT, buses, and DSs; L5 and L6 represent the series combination of buses, ECT, electrical lines, and DSs; L9 and L10 represent the series combination of transformer, electrical lines, and DSs; L3, L4, L7, L8, and L11 represent CBs. The reliability of each circle can be obtained based on the reliability calculation equation \( R_S = \prod R_i \) of Cascading Systems.

In the remaining sections, we define the probability \( P_S \) that the main electrical connection operates normally as the reliability index of smart substation. \( P_S \) is defined as follows:

\[ P_S = \sum_{i \in S} p_i, \]

where \( S \) is the set of all running states; \( p_i \) is the probability of smart substation working in the reliable state (i.e., Load1 and Load2 are supplied power normally), and \( p_i \) can be obtained according to the following reliability analysis method.

5.2. Reliability Evaluation Method

5.2.1. Analysis of Existing Reliability Evaluation Methods.

The common reliability evaluation methods are generally divided into analytical method and simulation method [31].

The analytical method is used for evaluating the reliability of smart substation through mathematical modelling. Lei et al. [11] used the cyber-physical interface matrix and analytical method to evaluate the effect of each component failure on load shedding in IEC 61850 based substation. Falahat et al. [25] used the analytical method to evaluate the reliability of smart substations and microgrid CPS with simple structure. However, obtaining high-precision results depends on some previous assumptions [32].

The simulation method mainly refers to the Monte Carlo method. Liu et al. [33] used the nonsequential Monte Carlo method for information domain and physical domain simulation, respectively, when evaluating the reliability of the active distribution network. Wang et al. [34] employed the nonsequential Monte Carlo method to simulate the operation of the microgrid CPS. However, the nonsequential Monte Carlo method does not consider the temporal properties of components in practice. Sun and Xie [35] used the sequential Monte Carlo method to describe the correlation between the time series of wind speeds and loads and evaluated the reliability of distribution systems containing wind turbine generator. Araújo et al. [36] used sequential Monte Carlo method to select the system scenarios resulting in uncertainties associated with load fluctuations, load forecasting errors, distributed generation unavailability, and intermittence of renewable energy resources. Zhou et al. [37] proposed a sequential Monte Carlo simulation method based on load path. The method can be used for evaluating the reliability of the power grid through traversal search for load paths, fault simulation, index statistics, and system index calculations. However, the calculation accuracy of the simulation method is inversely proportional to the calculation efficiency.

Therefore, some researchers focused on improving simulation method to reduce simulation variance and improve simulation efficiency. To the best of our knowledge, there are mainly stratified sampling method, control variable method, important sampling method, dual variable method, Latin hypercube sampling (LHS) method, and so on [38]. Zhang et al. [39] proposed an improved LHS method (hereinafter, ILHS) to evaluate the reliability of power system; this method combines LHS method and important method. In addition, some studies used the mixed method (hereinafter, MIXD) to evaluate the reliability of system, which combines the analytical method and Monte Carlo method. Han et al. [40] used analytical method to calculate
the availability of protection and monitoring functions and then used the nonsequential Monte Carlo method for reliability evaluation. Hou et al. [41] used the mixed method to obtain a system state distribution, which is more close to the true distribution probability. Based on the impact analysis of failure mode. These methods improved the efficiency of reliability evaluation in different degrees.

In conclusion, the analytical method improves the simulation efficiency of Monte Carlo method by reducing the time of each state evaluation. And it does not affect the application of the variance reduction techniques. Thus, the analytical method can be combined with the variance reduction methods, which not only shortens the time of each state evaluation, but also reduces the simulation variance.

5.2.2. MALI-Hybrid. According to the analysis in Section 5.2.1, we present MALI-hybrid method, which combines the Monte Carlo method, analytical method, LHS method, and important sampling method. This method improves the simulation efficiency in two aspects, which not only shortens the time of each state evaluation, but also reduces the simulation variance and improves simulation convergence speed.

The procedure of MALI-hybrid is shown in Figure 7, in which $f_{\text{sampling}}$ is the function of the improved LHS method, and its procedure is shown in Figure 8. We implemented MALI-hybrid in MATLAB to verify these two procedures.

In Figure 7, “Generate the minimum cut sets of the system” refers to getting the minimum cut sets of the smart substation based on Figure 6 and the minimum cut set theory of analytic method. The generated sets are \{L1, L2\}, \{L1, L4\}, \{L2, L3\}, \{L3, L4\}, \{L5, L11\}, \{L5, L6\}, \{L6, L11\}, \{L7, L8\}, \{L7, L9\}, \{L8, L9\}, and \{L9, L10\}. The different sets are connected in series. If any set fails, the system fails. Based on adjacency matrix method, we have programmed to generate the minimum cut sets in MATLAB. Thus, the obtained minimum cut sets are connected as shown in Figure 9.
In Figure 8, “Parameter initialization” refers to the set initial multiplier $K_0$ as 1.1 by referring to [39], the important sampling times Num as 5000, and the maximum sampling times $N_{\text{max}}$ as 10000. $K$ is the optimal multiplier, which can be calculated by equations (14) and (15). $|K - K_0| \leq 0.01$ refers to the criteria of optimizing $K$. The criteria are set as 0.01 by referring to [39]. The criteria value (i.e., 0.01) refers to the calculating accuracy. The smaller the criteria value is, the higher the calculating accuracy is, and the more simulation time is needed. $N_0$ are the iteration times.

$$K = \frac{B + \sqrt{B^2 - AC}}{A},$$

where

$$A = \frac{n_1}{n_0 + n_1} - \left(1 - \frac{n_1}{n_0 + n_1}\right)\lambda(1 - \lambda),$$

$$B = \frac{n_1}{n_0 + n_1},$$

$$C = \frac{n_1}{n_0 + n_1},$$

$$\lambda = \frac{1}{n} \sum_{i=1}^{n} \lambda_i,$$

where $n$ is the total number of elements in the system; $n_0$ and $n_1$ are the numbers of normal elements and faulty elements, respectively; $\lambda$ is the average failure rate of all elements.

6. Case Study

The case study in this section is based on the logic correlation diagram of the main electrical connection shown in Figure 6.

6.1. Reliability Calculation of Elements in Smart Substation

Based on the data about failure rate and repair rate in references [42–44], the reliabilities of physical equipment calculated by equation (5) are shown in Table 2. In actual evaluation, the connecting wires between physical equipment in smart substation are very short. Therefore, the reliability of electrical line is set as 1 in the following calculations, which is not presented in the table. Similarly, the reliabilities of electrical line are shown in Table 3.

We apply AHP model shown in Figure 3 to calculate the importance degree $\vartheta_i$. The results are shown in Table 4.
The reliability of data transmitting on communication links can be calculated by equation (8) based on packet error rate. Because the communications in smart substation is based on Ethernet, the packet error rate is equal to the omission rate of cyclic redundancy check (CRC) used in Ethernet (i.e., $P_e = 2E - 10$). Thus, the reliability of transmitted data is $D = 1 - (2E - 10)$. The equivalent reliabilities of cyber elements are calculated according to equations (5)–(8), and the results are shown in Table 5.

The reliability of data transmitting on communication links can be calculated by equation (8) based on packet error rate. Because the communications in smart substation is based on Ethernet, the packet error rate is equal to the omission rate of cyclic redundancy check (CRC) used in Ethernet (i.e., $P_e = 2E - 10$). Thus, the reliability of transmitted data is $D = 1 - (2E - 10)$. The equivalent reliabilities of cyber elements are calculated according to equations (5)–(8), and the results are shown in Table 5.

According to Section 4, the equivalent reliability of CB considering the reliability factors of the cyber side and cyber-physical interactions can be calculated by equations (9)–(12). The error rate of measurement information is set as 0.0001% in this calculation because of no relevant statistical data. The results are shown in Table 6.

### Table 3: Reliability data of cyber elements.

| Device name         | Failure rate ($a^{-1}$) | Repair rate ($a^{-1}$) | Reliability     |
|---------------------|-------------------------|------------------------|-----------------|
| Switch              | 0.02                    | 365                    | 0.999945        |
| P&C IED             | 0.0067                  | 365                    | 0.999982        |
| MU                  | 0.0067                  | 365                    | 0.999982        |
| CB IED              | 0.005                   | 365                    | 0.999986        |
| Communication link  | 0.001                   | 365                    | 0.999997        |

### Table 4: Importance degree of the cyber equipment.

| Device name | Importance |
|-------------|------------|
| Switch      | 0.2476     |
| P&C IED     | 0.3125     |
| MU IED      | 0.1768     |
| CB IED      | 0.2631     |

### Table 5: Equivalent reliability of cyber equipment considering importance degree or packet error rate.

| Device name         | Reliability     |
|---------------------|-----------------|
| Switch              | 0.999986        |
| P&C IED             | 0.999994        |
| MU IED              | 0.999997        |
| CB IED              | 0.999996        |
| Communication link  | 0.999997        |

### 6.2.21. Rationality Verification for Indices.

To verify the rationality of the reliability indices proposed in this paper, the following three scenarios are presented.

**Scenario 1:** Assume that the cyber side and the measurement information of the physical side are completely reliable. Therefore, the reliability evaluation of smart substation is conducted only considering the factors of the physical side.
Scenario 2: Assume that the measurement information of the physical side is completely reliable, but the cyber side is not. Therefore, the reliability evaluation of smart substation is conducted considering the effect of the cyber side on the physical side.

Scenario 3: Assume that both the cyber side and the measurement information of the physical side are not reliable. Therefore, the reliability evaluation of smart substation is conducted considering the interactions between the cyber side and the physical side.

Table 7 shows the evaluation results of smart substation in the three scenarios based on the data in Section 6.1 and the MALI-hybrid method presented in Section 5.2.2.

Table 7 shows that the reliability of the smart substation in Scenario 1, Scenario 2, and Scenario 3 is successively reduced, which is consistent with the actual situation. Therefore, the presented reliability indices in this paper are rational and feasible.

6.2.2. Efficiency Verification for MALI-Hybrid. According to the analysis in Section 5, the MALI-hybrid method can reduce the simulation variance and improve simulation speed. Thus, to verify the efficiency of the MALI-hybrid method, we evaluated the reliability of the smart substation in Scenario 3 from Section 6.2.1 using the MALI-hybrid method presented in Section 5.2.2, ILHS method [33], and MIXD method [35], respectively. The dynamic variation of variance coefficient with the number of simulations is shown in Figure 10.

As shown in Figure 10, MALI-hybrid method has a smaller variance coefficient than the other two methods when the numbers of simulations are the same. It shows that...
MALI-hybrid method does improve the simulation efficiency compared to the other two methods.

6.2.3. Correctness Verification for MALI-Hybrid. To verify the correctness of MALI-hybrid method, we evaluated the reliability of the smart substation in Scenario 3 from Section 6.2.1 using the MALI-hybrid method and Monte Carlo method. The results are shown in Table 8.

By analyzing the results from Table 8, it can be seen that the reliability difference between the MALI-hybrid method and Monte Carlo method is small and within the engineering error range. That is, the calculation precision of the MALI-hybrid method is reasonable. Therefore, MALI-hybrid method presented in Section 5.2.2 is correct.

### 7. Conclusions

This paper studies the reliability evaluation method for smart substation from the perspective of cyber-physical system. We point out that reliability evaluation of smart substation should consider the reliability factors on both the cyber side and the physical side, and their interactions. And the problem how cyber-physical interactions affect the reliability of smart substation can be converted into analyzing the effect of measurement and control messages on CBs’ action. Based on this view, new reliability indices for smart substation are proposed: (1) reliability index of cyber equipment considering its effect on the communication business when the data leakage, packet error, message tampering or forgery, packet loss or interruption, and message delay occur, (2) reliability index of communication links considering the reliability of the transmitted data on them, and (3) equivalent reliability indices of CB considering the cyber-physical interactions. Furthermore, a MALI-hybrid reliability evaluation method is presented. This method combines the Monte Carlo method, analytical method, LHS method, and important sampling method. The case studies show that the indices and the method in this paper are reasonable, and our MALI-hybrid method is superior to the existing methods in terms of simulation speed.

In the future, we will further conduct a study on smart grid from the perspective of cyber-physical system based on this work, so as to propose broadly applicable reliability evaluation indicators and methods for smart grid.

### Data Availability

The data used to support the findings of this study are currently under embargo, while the research findings are commercialized. Requests for data after publication of this article will be considered by the corresponding author.

### Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

### Acknowledgments

This work was supported by the National Natural Science Foundation of China (Research on the evolution mechanism and early defense of cascading failures across spaces caused by coordinated cyberattacks in Grid CPS, No. 51977155).

### References

1. A. Zheng, Q. Huang, and D. Cai, "Quantitative assessment of stochastic property of network-induced time delay in smart substation cyber communications," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2407–2416, 2020.
2. L. J. Chen, S. W. Mei, and Y. Chen, "Smart grid information security and its influence on power system survivability," *Control Theory & Application*, vol. 29, no. 2, pp. 240–244, 2012.
3. Y. Tang, Q. Chen, and M. Y. Li, “The research overview of network attack in Cyber-Physical System,” *Automation of Electric Power Systems*, vol. 40, no. 17, pp. 59–69, 2016.
4. Y. M. Xia, *Performance analysis of communication networks and cyber security assessment of power systems*, Ph.D. Thesis, Zhejiang University, Zhejiang, China, 2015.
5. Y. Zhou and Z. H. Chen, “The analysis of 7.10/central China (Henan) grid accident,” *Hunan Electric Power*, vol. 28, no. 3, pp. 28–31, 2008.
6. Q. L. Guo, S. J. Xin, J. H. Wang, and H. B. Sun, “Comprehensive security assessment for cyber physical energy system: a Lesson from Ukraine’s blackout,” *Automation of Electric Power Systems*, vol. 40, no. 5, pp. 145–147, 2016.
7. Z. H. Li, *Research on the key techniques of performance evaluation system for electronic transformers*, Ph.D. Thesis, Huazhong University of Science and Technology, Wuhan, China, 2014.
8. Y. Cai, Y. Chen, Y. Li, and Y. J. Cao, “Reliability analysis of cyber–physical systems: case of the substation based on the IEC 61850 standard in China,” *Energies*, vol. 11, no. 10, p. 2589, 2018.
9. Y. L. Zhang, “The reliability and related issues of secondary system of intelligent substation,” M.S. Thesis, Shanghai Jiao Tong University, Shanghai, China, 2013.
10. Y. Tang, X. Han, and Y. J. Wu, "Electric power system vulnerability assessment considering the influence of communication system,” *Proceedings of the CSEE*, vol. 35, no. 2, pp. 6066–6074, 2015.

### Table 8: Comparison of the MALI-hybrid method in Section 5.2.2 and Monte Carlo method.

| Numbers of simulation | Reliability evaluation results based on the presented method | Reliability evaluation results based on the Monte Carlo method |
|-----------------------|-------------------------------------------------------------|---------------------------------------------------------------|
| 2000                  | 0.999989                                                   | 0.999289                                                     |
| 4000                  | 0.999759                                                   | 0.999269                                                     |
| 6000                  | 0.999659                                                   | 0.999259                                                     |
| 8000                  | 0.999539                                                   | 0.999239                                                     |
| 10000                 | 0.999326                                                   | 0.999229                                                     |
[11] H. T. Lei, C. Singh, and S. Aprintson, “Reliability modeling and analysis of IEC 61850 based substation protection systems,” IEEE Transactions on Smart Grid, vol. 5, no. 5, pp. 6066–6074, 2014.

[12] C. W. Ten, K. Yamashita, Z. Y. Yang, A. V. Vasilakos, and A. Ginter, “Impact assessment of proposed cyber attacks on interconnected bulk power systems,” IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4405–4425, 2018.

[13] X. W. Liu, Q. Gong, H. Han, Z. Q. Wang, and L. F. Wang, “Reliability modeling and evaluation of active cyber physical distribution system,” IEEE Transactions on Power Systems, vol. 33, no. 6, pp. 7096–7108, 2018.

[14] V. Aravinthan, T. Balachandran, and M. Ben, “Reliability modeling considerations for emerging cyber–physical power systems,” in Proceedings of the 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), pp. 24–28, Boise, ID, USA, June 2018.

[15] R. Wang, Q. Y. Sun, and W. Hu, “SoC-based droop coefficients stability region analysis of the battery for stand-alone supply systems with constant power loads,” IEEE Transactions on Power Electronics, vol. 36, no. 7, pp. 7866–7879, 2021.

[16] Q. Y. Sun, R. K. Han, and H. G. Zhang, “A multiagent-based consensus algorithm for distributed coordinated control of distributed generators in the energy internet,” IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 3006–3019, 2015.

[17] R. Wang, Q. Y. Sun, and D. Z. Ma, “The small-signal stability analysis of the droop-controlled converter in electromagnetic timescale,” IEEE Transactions on Sustainable Energy, vol. 10, no. 3, pp. 1459–1469, 2019.

[18] R. Wang, Q. Y. Sun, D. Z. Ma, and X. G. Hu, “Line impedance cooperative stability region identification method for grid-tied inverters under weak grids,” IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 2856–2866, 2020.

[19] W. Hu, C. H. Ruan, and H. Nian, “Simplified Modulation scheme for open-end winding PMSM system with common dc bus under open-phase fault based on circulating current suppression,” IEEE Transactions on Power Electronics, vol. 35, no. 1, pp. 10–14, 2020.

[20] X. G. Hu, H. G. Zhang, D. Z. Ma, and R. Wang, “Hierarchical pressure data recovery for pipeline network via generative adversarial networks,” IEEE Transactions on Automation Science and Engineering, 2021, in press.

[21] D. Z. Ma, Y. B. Li, X. G. Hu, H. Zhang, and X. Xie, “An optimal three-dimensional drone layout method for maximum signal coverage and minimum interference in complex pipeline networks,” IEEE Transactions on Cybernetics, 2021, in press.

[22] Y. G. Chen, J. E. Li, and A. Xu, “Reliability evaluation method for smart substation based on cyber-physical fusion,” Automation of Electric Power Systems, vol. 45, no. 3, pp. 102–110, 2021.

[23] IEC, Communication Network and Systems in Substations-Part 5: Communication Requirements for Function and Device Models, IEC, Geneva, Switzerland, 2003.

[24] H. C. Zhao, Analytic Hierarchy Process, Science Press, Beijing, China, 1986.

[25] B. Falahati, Y. Fu, and L. Wu, “Reliability assessment of smart grid considering direct cyber-power interdependencies,” IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1515–1524, 2012.

[26] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, “A framework for modeling cyber-physical switching attacks in smart grid,” IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 2, pp. 273–285, 2013.

[27] Y. C. Zhang, L. F. Wang, and W. Q. Sun, “Trust system design optimization in smart grid network infrastructure,” IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 184–195, 2013.

[28] K. R. Chen, F. S. Wen, and J. H. Zhao, “Vulnerability assessment of cyber-physical power system considering virtual cyber-physical connections,” Electric Power Automation Equipment, vol. 37, no. 12, pp. 67–72, 2017.

[29] S. Wang and X. M. Huang, “Filtering methods of GOOSE messages,” Automation of Electric Power Systems, vol. 32, no. 19, pp. 54–57, 2008.

[30] X. G. Yin, Z. Zhang, and H. Y. Wang, “Multiple transformers and CTs interactive effect and its impact on the protective relay,” Power System Protection and Control, vol. 44, no. 23, pp. 1–9, 2016.

[31] Y. Zhao and K. G. Xie, “An analytical approach to compute the probability density distributions of reliability indices for bulk power systems,” Proceeding of the CSEE, vol. 31, no. 4, pp. 31–38, 2011.

[32] Y. Liu, “Technology and economy evaluation of the new generation intelligent substation electrical main wiring design scheme,” M.S. Thesis, North China Electric Power University, Beijing, China, 2017.

[33] W. X. Liu, Q. Gong, and J. Guo, “Reliability simulation of AND cyber-physical system based on hybrid communication network,” Proceedings of the CSEE, vol. 36, no. 6, pp. 1706–1718, 2018.

[34] C. Wang, T. Zhang, and F. Luo, “Impacts of cyber system on microgrid operational reliability,” IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 105–115, 2019.

[35] R. D. Sun and K. G. Xie, “Reliability evaluation of distribution networks using Monte Carlo method considering correlations between wind speed and load,” Power System Protection and Control, vol. 40, no. 18, pp. 12–18, 2012.

[36] J. R. Araújo, E. N. M. Silva, and A. B. Rodrigues, “Assessment of the impact of microgrid control strategies in the power distribution reliability indices,” Journal of Control, Automation and Electrical Systems, vol. 28, no. 2, pp. 271–283, 2017.

[37] C. Zhou, X. Li, J. T. Wang, W. H. Liang, and W. Z. Yin, “Reliability calculation of distribution network based on sequential Monte Carlo simulation of load path,” Mechanical and Electrical Information, vol. 12, pp. 24–27, 2019.

[38] X. Z. Xie, “Reliability improvement and its assessment method for distribution network,” Electrical Equipment, vol. 9, pp. 76–78, 2004.

[39] W. F. Zhang, Y. B. Che, and Y. S. Liu, “Improved Latin hypercube sampling method in power system reliability evaluation,” Automation of Electric Power Systems, vol. 39, no. 4, pp. 52–57, 2015.

[40] Y. Q. Han, Y. F. Wen, C. X. Guo, and H. Huang, “Incorporating cyber layer failures in composite power system considering virtual cyber-physical power system reliability evaluations,” Energies, vol. 8, no. 9, pp. 9064–9086, 2015.

[41] Y. S. Hou, X. L. Wang, and Y. Zhang, “Dimensional importance based quasi-Monte Carlo for power system reliability evaluation,” Automation of Electric Power Systems, vol. 40, no. 16, pp. 31–37, 2016.

[42] P. Brani, The Automation of Substations, pp. 191–200, China Electric Power Press, Beijing, China, 2009.

[43] L. Cheng and J. He, Power System Reliability Principle and Application, pp. 356–358, Tsinghua University Press, Beijing, China, 2015.

[44] T. W. Wang, M. Xie, and Y. Q. Sun, “Analysis of reliability for relay protection systems in smart substations,” Power System Protection and Control, vol. 43, no. 6, pp. 58–66, 2015.