energies

MDPI

Article

Reliability Analysis of Cyber–Physical Systems: Case of the Substation Based on the IEC 61850 Standard in China

Ye Cai [1], Yu Chen [2], Yong Li [2,*], Yijia Cao [1] and Xiangjun Zeng [1]

[1] Hunan Province 2011 Collaborative Innovation Center of Clean Energy and Smart Grid, Changsha University of science and technology, Changsha 410082, China; caiye@csust.edu.cn (Y.C.); yjcao@hnu.edu.cn (Y.C.); xjzeng@csust.edu.cn (X.Z.)

[2] College of Electrical and Information Engineering, Hunan University, Changsha 410082, China; yuyuchenyu@163.com

* Correspondence: liyong1881@163.com

Received: 7 August 2018; Accepted: 26 September 2018; Published: 28 September 2018

Abstract: With the increasing interaction between physical devices and communication components, the substation based on the IEC 61850 standard is a type of cyber–physical system. This paper proposes a reliability analysis method for substations with a cyber–physical interface matrix (CPIM). This method calculates the influences from both the physical device failures and the communication devices failures. Two indices, Probability of Load Curtailments and Expected Demand Not Supplied, are used in the reliability analysis. Given the simplified model of the practical substation based on the Chinese IEC 61850 standard, the results show that the substation system had a potential risk of cascading failure under the cyber–physical fusion trend, as the failure in cyber layer would increase the power loss of the whole system. The changing magnitude of Expected Demand Not Supplied increased significantly with increasing transmission delay rate of the process bus.

Keywords: cyber–physical system; intelligent substation; reliability analysis; cyber–physical interface matrix (CPIM)

1. Introduction

Over the years, cyber–physical systems (CPSs) have attracted considerable attention given their wide applications in grids, intelligent robot networks, embedded systems, and other fields. A typical CPS is capable of real-sensing, dynamic control, and information services [1–3]. Smart cyber systems provide better monitoring, transferring, and controlling functions for the substation, but produce a trade-off, as the substation will experience more cyber-attacks. The Supervisory Control and Data Acquisition (SCADA) system of a nuclear plant recently experienced a severe cyber-attack [4], so the study of cyber security has become a hot topic in smart grids. However, the interactions between cyber devices and physical devices in substations based on the IEC 61850 standard might create new failure scenarios to substations. Thus, it is important to address the reliability of the substation considering the interactions between the cyber layer and physical layer.

In recent years, more research has focused on the cyber-security in power grid. Cyber security in a typical smart grid is illustrated by S. Lim et al. [5], and four types of cyber-power interdependencies were categorized by B. Falahati et al. [6]. For evaluating the direct element–element interdependency between power grid and communication network, B. Falahati et al. [6] proposed a probability table, denoted as the P-Table, to analyze the reliability in integrated systems. Based on the state updating-based model, indirect cyber-power interdependency was proposed to evaluate the reliability of cyber-power networks.

Because of the transformation from traditional substations to the substations based on the IEC 61850 standard, it is important to model the interaction mechanism of the primary equipment and communication equipment in the substation [7,8]. The communication system based on IEC 61850 is complex and the security of Intelligent Electronic Devices (IEDs) [9], GOOSE (Generic Object Oriented Substation Event) [10], and other parts have been discussed. Comprehensive methods combining the physical equipment and the communication components are rare, but the direct and indirect influence of the communication components in substation automation systems could be proposed [6,11]. The influence of the usual parts, widely considered in communication, was analyzed based on a new method, the CPIM [12]. This matrix uses a mathematical approach to understand the cyber effects caused by physical failures within one cyber–physical system. However, a specific analysis was not carried out, so further study of the reliability of the cyber–physical system is required.

This paper proposes a new approach for analyzing the reliability of the IEC 61850 substation, focusing on the relationship between the cyber device and physical device. There are three types of failures mentioned and classified in the paper: Low-impact failure, local-impact failure, and wide-impact failure. Based on the different failures, reliability indices are proposed to quantify the effects of the failures. Finally, a sensitivity analysis of the Expected Demand Not Supplied is designed to analyze the IEC 61850 substation reliability.

The remainder of this paper is organized as follows. In Section 2, the interactive mechanism between the primary equipment and communication components is described for the substation, and three types of direct impacts are discussed. The impacts of the cyber layer on the cyber-physical substation and CPIM are defined in Section 3. The reliability of the method based on the CPIM is studied in Section 4. Case studies based on Monte Carlo simulation are provided in Section 5. Finally, some remarks provide a conclusion in Section 6.

2. Interactions between Cyber Layer and Physical Layer

2.1. Simplified Model of the Substation System Based on IEC 61850

Figure 1a shows a logical view of an example substation network architecture [13], commonly known as the substation based on the IEC 61850 standard automation model. IEC 61850 specifies how instantaneous sampled value (SV) measurements shall be transmitted over an Ethernet network by a merging unit (MU) or instrument transformer with an electronic interface. The IEC 61850 standard establishes a unified protocol for communication. Based on the standard, the main physical components are transmission lines, buses, circuit breakers, and main transformers. The cyber layer is divided into station level, bay level, and process level [14]. As a communication bus and a process bus can transmit and receive digital signals between the process level and bay level, they establish a communication connection between the protection unit, merging unit, and circuit breaker.

The circuit breaker, as the connecting and coupling component between the physical layer and cyber layer, plays the role of a controlling terminal. The components of a cyber layer under IEC 61850 standard mainly include the process bus, merging unit, and physical component protection unit [15]. The protection unit includes the transmission line protection unit, transformer protection unit, and bus protection unit.

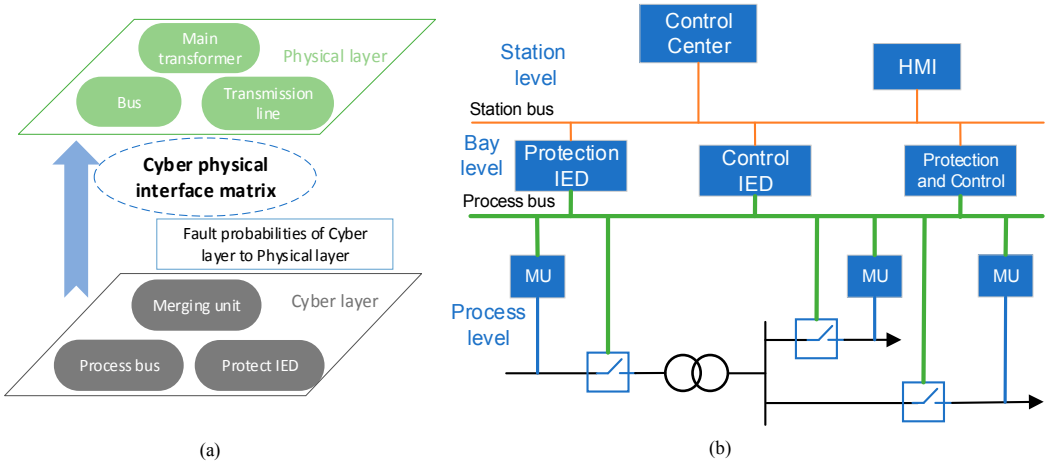

Figure 1. (**a**) The components, and (**b**) structure of cyber–physical substation system. IED, Intelligent Electronic Devices; MU, merging unit.

2.2. Interaction Framework of the Cyber-Physical Substation

In Figure 1, once one physical device breaks, the physical fault clearing process is the key factor for maintaining the correct functioning of the substation. The definition of fault clearing is when a physical component fails, the corresponding transformers or current transformers monitor the fault information, and then send the analog signal to the merging unit (MU) [13,16]. The MU digitizes the information and sends the information to the protection Intelligent Electronic Devices (IEDs) of the corresponding physical components. Protection IEDs generate the tripping-signal through the protection algorithm. Finally, the process bus sends the signal to the circuit breaker for corresponding actions, thus limiting the scope of the failure of the physical components. This process is partially affected by the cyber components. If all the components in the process act normally and actually, the fault clearing is successful, thus limiting the scope of the failure of the initial physical components. Otherwise, the fault clearing fails, thus the scope of the failure propagating to other physical components.

As summary above, the reliability of cyber elements, such as MU, IEDs, and the process bus, is important to alert the primary equipment failure and help the substation continue working. Once some failures occur in the primary equipment in the substation, three types of scenarios occur during the physical fault clearing process, low-impact failure, local-impact failure, and wide-impact failure. Assuming a failure happened to the busbar, the three types of impacts are shown in Figure 2. In the paper, during the physical fault clearing process, if the e related cyber devices work correctly and actually, we call it working functionally, otherwise, call it working malfunctioning.

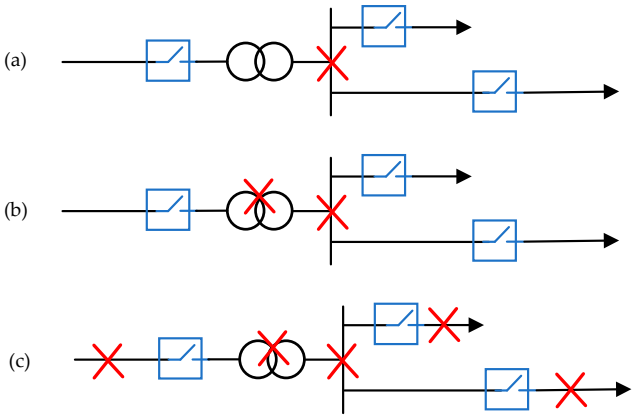

Figure 2. Three types of cascading failures in the substation: (**a**) Llow-impact; (**b**) local-impact; and (**c**) wide-impact.

The first type is the low-impact situation where no fault occurs in the cyber components (Figure 2a). All the information from the primary equipment can be sent out; thus, the physical fault clearing process can work normally. For example, in Figure 2a, the fault occurs in busbar and it does not spread elsewhere.

The second type is local-impact. Once some cyber components malfunction during the physical fault clearing process (excluding the process bus), the failures might spread to their surroundings, triggering them to malfunction, but the failure can be limited to the local scope by other functional cyber components. For example, in Figure 2b, the initial fault also occurs in the busbar; the final fault spreads to the main transformer, due to the MU failures.

The third type is wide-impact. The entire communication of the cyber-physical substation breaks down if the core of the communication components is damaged. For example, the process bus in the communication process plays the core role. Once it fails, all the information from the substation operation states would not be sent out. For example, in Figure 2c, the initial fault still occurs in the busbar, and the whole system breaks, due to the failure of the process bus.

3. Model Quantifying the Interactions

Considering the three kinds of impact caused by cascading failures in substations, listed in Section 2, cascading failures chains can be described by a probabilistic model. To describe final cascading failure impact, we attempted to define the working states of the cyber components. A 0,1 sequence of related cyber components can reflect the final system state under different physical faults. For example, if 0 means functioning and 1 means malfunctioning, given the original failure in the substation, the working states of all related cyber components in the cascading failure chain can be obtained, and the impact of the cascading failure chain can be quantified as:

$$CPM = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{m,1} & p_{m,2} & \cdots & p_{m,n} \end{bmatrix}_{m \times n} . \quad (1)$$

In (1), m is the number of the physical components, n is the amounts of cascading scenarios of each physical component; $p_{m,n}$ is the probability of causing the cascading scenario nth of the physical component mth, thus, the row vector $[p_{m,i}]$, $i \in [0, n]$ is the cascading scenario set of the physical component mth.

However, in practice, the cyber component working state is not actually 0 or 1. Thus, in the paper, we modeled this as a two-state model, as shown in Figure 3. The state of the cyber component is set to [0,1], where 0 represents working functionally (down), and 1 represents working malfunctioning (up). In Figure 3, λ denotes the failure rate of one individual component, and μ denotes the repair rate. The detailed data are given in Table 1.

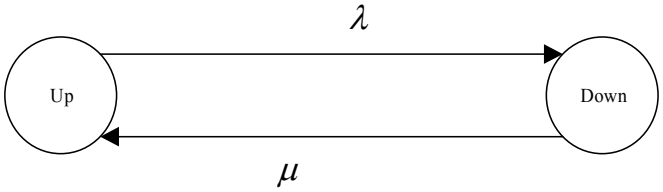

Figure 3. Working states of cyber a component.

Table 1. Data for cyber components.

	Mean Time to Failure (Years)	Failure Rate λ (per Year)	Mean Repair Time (h)	Repair Rate μ (per Year)
Protection IED	50	0.02	7.99998	1095.002
Merging Unit	150	0.00667	7.99998	1095.002
Circuit Breaker	100	0.01	7.99998	1095.002
Process Bus	100	0.01	7.99998	1095.002

The occurrence probability of a functionally working state p and unfunctional working state p' are calculated with Equations (2) and (3), respectively.

$$p = \frac{\mu}{\lambda + \mu} \tag{2}$$

$$p' = \frac{\lambda}{\lambda + \mu} \tag{3}$$

There are some delays in the communication process [11]. The delay transmission of the process bus is denoted by probability η (η = 0.3% in the case study). Thus, Equations (2) and (3) can be updated as Equations (4) and (5) considering the delay, respectively.

$$p = \frac{\mu}{\lambda + \mu}(1 - \eta) \tag{4}$$

$$p' = 1 - p \tag{5}$$

The functional working state and unfunctional working state probabilities of each cyber components are calculated, as shown in Table 2. The functional working state probability of the process bus is smaller than that of the other components according to Equation (4).

Table 2. Working state probability of individual cyber components.

Component	Functionally Working State p	Unfunctional Working State p'
Protection IED	0.999981735	0.000018265
Merging Unit	0.999993912	0.000006088
Circuit Breaker	0.999990868	0.000009132
Process Bus	0.996990895	0.003009105

4. Reliability Analysis of the Cyber–Physical Substation

4.1. Indices of Cyber Physical Substation Reliability

Probability of Load Curtailments *(U_k)* and Expected Demand Not Supplied (EDNS) were used to calculate the reliability of the cyber–physical substation, and they are displayed in Equations (6) and (7), respectively.

$$U_k = \frac{\sum_{i=1}^{N} T_{dnik}}{\sum_{i=1}^{N} \left(T_{upik} + T_{dnik} \right)} \tag{6}$$

where N is the number of the simulation, T_{dnik} is the duration of load k in ith curtailments, and T_{upik} is the duration of load k in the ith functionally working state.

$$EDNS_k = \sum_{i=1}^{N_k} P_{ik} L_k, \tag{7}$$

where L_k is the average load not supplied of load-point k during the simulation, P_{ik} is the probability of failure of sub-state i at load-point k, and N_k is the total number of states or sub-states that cause load curtailment at load-point k.

4.2. Reliability Simulation Method

The simulation was based on the sequential Monte Carlo method. Considering the cascading failures in the substation, the reliability simulation steps were as follows:

(1) Simulate time $t = 0$: Initialize both cyber layer and physical components.

(2) Randomly generate states of all physical components. The working state of each physical component is based on the exponential distribution:

$$T_i = -\frac{1}{\sigma_i} \ln U_i, \tag{8}$$

where U_i of item i is within the interval [0,1], which obeys uniform distribution. If the current working state of the item i is functional, σ_i is the failure rate of the physical component; otherwise, the current state is unfunctional, and σ_i is the repair rate of physical component. Finally, based on Equation (8), we can find the $min\{T_i\}$, and its corresponding component j. The working state of the physical component j will change at the next simulation time.

(3) The simulation time can be described as $t = t + 1$. Update the working states of all components.

(4) Calculate the cyber–physical interface matrix (CPIM), as shown in Section 3. Identify if a cascading failure happens according to Equation (9). If so, then repeat step (3). Repeat this step until the failure no longer spreads. For component j, compare the value $p_{j,y}$ in the cyber–physical interface matrix(CPIM) with a random number P in the interval [0,1]. If P satisfies:

$$\sum_{y=0}^{s-1} p_{j,y} < P < \sum_{y=0}^{s} p_{j,y}, \tag{9}$$

the sth scenario of the physical component j occurs.

(5) Calculate the reliability indices.

(6) Repeat steps (3) to (5) until the variance coefficient is less than the allowable value with:

$$\beta = \frac{\sqrt{V(F)/NS}}{E(F)}, \tag{10}$$

where $V(F)$ is the variance of the test function, NS is the number of simulation years, and $E(F)$ is the expected value of the function.

5. Case Study

5.1. CPIM of the Each Component in the Cyber-Physical Substation

A simplified model of a typical the substation based on the IEC 61850 standard in China is shown in Figure 4, which is a 220/121/38.5 kV step-down substation. The annual average load of both load-point-1 and load-point-2 are 100 MW. The details for the primary devices of the substation are shown in Table 3.

Table 3. Equipment reliability data for the primary device

	Failure Rate (per Year)	Mean Repair Time (h)
Bus	0.002	13.0
Transformer	0.025	43.1
Transmission line	0.02	10.0

In Figure 4, there are 11 breakers, denoted as 1, 2, 3 . . . ; A and J stand for the transmission lines; C, D, E are main transformers; MU is the merging unit, and the number of MUs is 8, denoted as by MU1, MU2 . . . ; B, F, G, H, I are the buses. According to (1), the shape of the CPM of Figure 4 is shown as (11). In (11), there are 10 physical devices, denoted as A, B, . . . J, thus the row number is $m = 10$, each row vector means the CPIM of a physical device. For example, the CPIM of the physical device A is denoted as $CPIM_{A_{1\times a}}$, where a is the number of cascading scenarios of A; similarly, the CPIM of the physical device B is denoted as $CPIM_{B_{1\times b}}$, where b is the number of cascading scenarios of B; the $CPIM$ of the physical device J is denoted as $CPIM_{J_{1\times j}}$, where j is the number of cascading scenarios of J; Thus, the number of columns of CPM is $a + b \ldots + j$. The $CPIM$ of each physical device shows from Tables 4–13.

$$CPM = \begin{bmatrix} \mathrm{CPI}M_{A_{1\times a}} & \vdots & 0 & \vdots & \ldots & \vdots & 0 \\ 0 & \vdots & \mathrm{CPI}M_{B_{1\times b}} & \vdots & \ldots & \vdots & 0 \\ \vdots & & & & & & \\ 0 & \vdots & 0 & \vdots & \ldots & \vdots & \mathrm{CPI}M_{J_{1\times j}} \end{bmatrix}_{10\times(a+b+\ldots+j)} \quad (11)$$

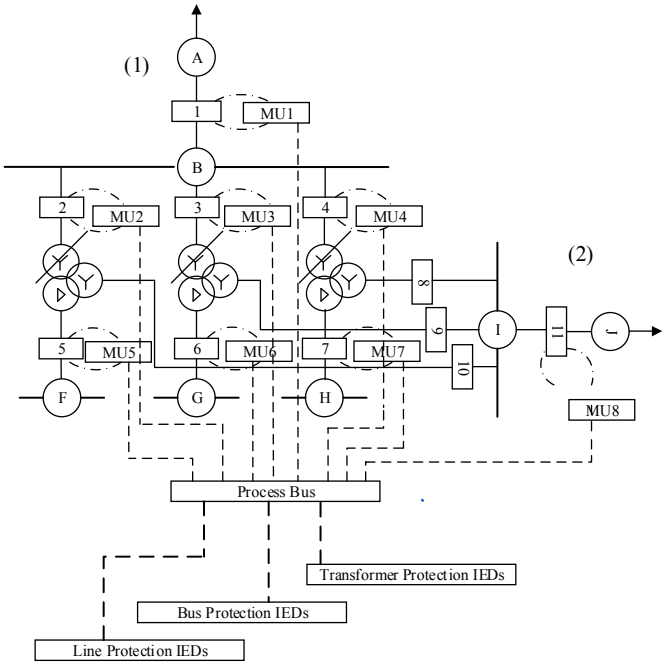

Figure 4. The structure of a real IEC 61850 substation in China.

Based on the CPIM method in Section 3, considering a failure clearing at line A, the $\mathrm{CPIM_A}$ are shown in Table 4. In this case, there are three kinds of cascading chains within the substation. scenario 1: If all the related cyber devices are working functionally, the breaker can obtain the failure information, and then locate and clear the failure. The failure scope would be limited within A, which is the low-impact case mentioned in Section 2. In Table 4, the results show that when line fault clearance occurs at A, more than 99% failures are limited to within A. However, in extremely few cases, the failure scope would extend to the entire system, due to the dysfunctional working of the process bus connected to A, which is the wide-impact case mentioned in Section 2. In Table 4, the probability of this occurrence is the smallest. With a small probability of 0.3%, among breaker 1, merging unit 1, and protection IED of A, more than one cyber device may be malfunctioning; thus, it leads to breaker 1 failure and then resulting in the failure of B. At this time, breakers 2, 3, and 4 can work functionally, thus limiting the failure scope to within A and B, which is the

local-impact case mentioned in Section 2. Thus, based on Table 4, the number of cascading scenario is 3, and the $CPIM_A$ = [0.996957511, 0.003009105, 0.000033384]$_{1\times3}$; it satisfied sum{$CPIM_A$} = 1. Using the same method, the CPIM of the line fault clearance at transmission line J can be obtained as the $CPIM_J$ = [0.996957511, 0.003009105, 0.000033384]$_{1\times3}$, results showing as Table 5.

Table 4. Cyber Physical Interface Matrix ($CPIM_A$) of the line fault clearance at A.

Cascading Scenario	Effects Scope	Probability
1	A	0.996957511
2	The entire system	0.000033384
3	AB	0.003009105

Table 5. $CPIM_J$ of the line fault clearance at transmission line J.

Cascading Scenario	Effects Scope	Probability
low-impact	J	0.996957511
wide-impact	The entire system	0.000033384
local-impact	IJ	0.003009105

Table 6 shows a similar analysis in the case of a failure clearing at bus B. In this case, consider all cyber devices are connected to B, such as merging units 1, 2, 3, and 4; breakers 1, 2, 3, and 4; and the process bus. The three kinds of cascading chains could occur within the substation: Low-impact, wide-impact, and local impart. In Table 6, more than 99% of failures are limited to within B, due to all the related cyber devices functioning properly. However, having a smaller probability 0.3%, the failure scope would extend to entitle system, due to the dysfunctional working of the process bus. According to the different sizes of failure scopes caused by different related cyber devices, four kinds of local-impact may occur with minimal probability.

Table 6. $CPIM_B$ of the line fault clearance at bus B.

Cascading Scenario	Effect Scope	Probability
low-impact	B	0.996911991
wide-impact	The entire system	0.003009105
local-impact 1	(AB)/(BC)/(BD)/(BE)	0.000015173
local-impact 2	(ABC)/(ABD)/(ABE)/(BCD)/(BCE)/(BDE)	1.38564396^{-10}
local-impact 3	(ABCD)/(ABCE)/(ABDE)/(BCDE)	3.51492326^{-15}
local-impact 4	ABCDE	1.82105929^{-5}

In Table 6, there are four types of local-impacts, denoted as local-impact 1, 2, 3, 4, and the number of cascading scenarios is 17. Local-impact 1: If one of the merging units or related breakers malfunctions, the failure effect scope would be limited to B and one of its connecting physical devices. The number of cascading scenarios belongs to local-impact 1 is 4. For example, either merging unit 2 or the breaker 2 is dysfunctional, while the others are functional, then the effect scope is limited to within B and C. Local-impact 2: If two of merging units or related breakers are dysfunctional, this case would limit the failure effect scope to B and two of its connecting physical devices. The number of cascading scenarios belongs to local-impact 2 is 6. For example, the effect scope ABE might result from the failure at breakers 1 and 4, and merging units 1 and 4. Similarly, If three (four) of the merging units or related breakers malfunction, this would limit the failure effect scope to B and three (four) of its connecting physical devices. The number of cascading scenarios belongs to local-impact 3 and local-impact 4 are 4 and 1.

Thus, based on Table 6, the number of cascading scenarios is 17, and the $CPIM_B$ = [0.996911991, 0.000015173, 0.000015173, 0.000015173, 0.000015173, 1.38564396^{-10}, 1.38564396^{-10}, 1.38564396^{-10}, 1.38564396^{-10}, 1.38564396^{-10}, 1.38564396^{-10}, 3.51492326^{-15}, 3.51492326^{-15}, 3.51492326^{-15},

3.51492326^{-15}, 1.82105929^{-5}, $0.003009105]_{1\times17}$, it satisfied sum{$CPIM_B$} = 1. Using the same method, the CPIM of the line fault clearance at bus F, H, G, I can be obtained as follows: The $CPIM_F$ = $[0.996957511, 0.003009105, 0.000033384]_{1\times3}$, the $CPIM_G$ = $[0.996957511, 0.003009105, 0.000033384]_{1\times3}$, the $CPIM_H$ = $[0.996957511, 0.003009105, 0.000033384]_{1\times3}$, $CPIM_I$ = [0.996911991, 0.000015173, 0.000015173, 0.000015173, 0.000015173, 1.38564396^{-10}, 1.38564396^{-10}, 1.38564396^{-10}, 1.38564396^{-10}, 1.38564396^{-10}, 1.38564396^{-10}, 3.51492326^{-15}, 3.51492326^{-15}, 3.51492326^{-15}, 3.51492326^{-15}, 1.82105929^{-5}, $0.003009105]_{1\times17}$, all results showing from Tables 7–10.

Table 7. $CPIM_F$ of the line fault clearance at bus F.

Cascading Scenario	Effects Scope	Probability
low-impact	F	0.996957511
wide-impact	The entire system	0.000033384
local-impact	FC	0.003009105

Table 8. $CPIM_G$ of the line fault clearance at bus G.

Cascading Scenario	Effects Scope	Probability
low-impact	G	0.996957511
wide-impact	The entire system	0.000033384
local-impact	GD	0.003009105

Table 9. $CPIM_H$ of the line fault clearance at bus H.

Cascading Scenario	Effects Scope	Probability
low-impact	H	0.996957511
wide-impact	The entire system	0.000033384
local-impact	HE	0.003009105

Table 10. CPIMI of the line fault clearance at bus I.

Cascading Scenario	Effect Scope	Probability
low-impact	I	0.996911991
wide-impact	The entire system	0.003009105
local-impact 1	(IJ)/(IC)/(ID)/(IE)	0.000015173
local-impact 2	(IJC)/(IJD)/(IJE)/(ICD)/(ICE)/(IDE)	1.38564396^{-10}
local-impact 3	(IJCD)/(IJCE)/(IJDE)/(ICDE)	3.51492326^{-15}
local-impact 4	IBCDE	1.82105929^{-5}

Using the same analysis method, Table 11 shows the results under failure clearing at transformer C. The results summary is similar to Table 6: (1) More than 99% failures are low-impact, limited to within C; (2) within a smaller probability of 0.3%, the failure scope extends to the entire system, due to the dysfunctional working of the process bus, being a wide-impact; and (3) local-impact are classified according to the failure number of the related cyber device, of which the occurrence has low probability. Thus, based on Table 11, the number of cascading scenarios is 9, and the $CPIM_C$ = $[0.996927164, 1.51734070^{-5}, 1.51734070^{-5}, 1.51734070^{-5}, 2.30941925^{-10}, 2.30941925^{-10}, 2.30941925^{-10}, 1.82100387^{-5}, 0.003009105]_{1\times9}$, satisfied sum{$CPIM_C$} = 1.

Table 11. $CPIM_C$ of the line fault clearance at transformer C.

Cascading Scenario	Effect Scope	Probability
low-impact	C	0.996927164
wide-impact	The entire system	0.003009105
local-impact 1	(BC)/(CF)/(CI)	1.51734070^{-5}
local-impact 2	(BCF)/(CIF)/(BCI)	2.30941925^{-10}
local-impact 3	BCFI	1.82100387^{-5}

Using the same method, the CPIM of the line fault clearance at transformer D, E can be obtained as follows: $CPIM_D$ = [0.996927164, 1.51734070^{-5}, 1.51734070^{-5}, 1.51734070^{-5}, 2.30941925^{-10}, 2.30941925^{-10}, 2.30941925^{-10}, 1.82100387^{-5}, 0.003009105]$_{1\times9}$, $CPIM_E$ = [0.996927164, 1.51734070^{-5}, 1.51734070^{-5}, 1.51734070^{-5}, 2.30941925^{-10}, 2.30941925^{-10}, 2.30941925^{-10}, 1.82100387^{-5}, 0.003009105]$_{1\times9}$, all results showing from Tables 12 and 13.

Table 12. $CPIM_D$ of the line fault clearance at transformer D.

Cascading Scenario	Effect Scope	Probability
low-impact	D	0.996927164
wide-impact	The entire system	0.003009105
local-impact 1	(DB)/(DG)/(DI)	1.51734070^{-5}
local-impact 2	(DBG)/(DBI)/(DGI)	2.30941925^{-10}
local-impact 3	DBFI	1.82100387^{-5}

Table 13. $CPIM_E$ of the line fault clearance at transformer E.

Cascading Scenario	Effect Scope	Probability
low-impact	E	0.996927164
wide-impact	The entire system	0.003009105
local-impact 1	(EB)/(EH)/EI)	1.51734070^{-5}
local-impact 2	(BEF)/(EBI)/(EIH)	2.30941925^{-10}
local-impact 3	BEHI	1.82100387^{-5}

5.2. Reliability Analysis Results

Consider the reliability of load-point-1, load-point-2, and the entire system in Figure 4. The Probability of Load Curtailment (PLC) was calculated, as shown in Table 14. A traditional simulation without considering the impact of the cyber layer and our method with integrated CPIM was carried out. As seen from the growth rate (Δ%), the probability of load curtailment slightly increased to 4.43% compared to without considering the influence of cyber layer. The improvement as not obvious compared with the traditional simulation, especially for the entire substation. The risk of cascading failure was low, due to the high reliability of the cyber components.

Table 14. CPIM of the line Probability of Load Curtailments (PLC) comparison.

Load Point	Probability of Load Curtailments		Growth Rate Δ(%)
	without Cyber Layer (Traditional Simulation)	with Cyber Layer	
(1)	3.78466667^{-5}	3.95233333^{-5}	4.43
(2)	3.81300000^{-5}	3.92400000^{-5}	2.91
Entire System	7.59766667^{-5}	7.73433333^{-5}	1.80

Compared that in the traditional simulation. The *EDNS* of entire substation than that with traditional simulation increase 7.41%. Compared the results of Table 15 with Table 14, the failures in

the cyber layer have more significant impacts on electricity unavailability than on the probability of load curtailment.

The comparison of EDNS is shown in Table 15. The EDNS in load-point 1 increased 11.93%.

Table 15. Expected Demand Not Supplied (EDNS) comparison.

Load Point	EDNS (MWh/Year)		Growth Rate Δ(%)
	without Cyber Layer (Traditional Simulation)	with Cyber Layer	
(1)	3.785	4.236	11.93
(2)	3.813	4.208	10.36
Entire system	7.598	8.160	7.41

5.3. Effects of Delay Rates

Values from 0 to 0.005 were assumed to be the delay rates for all process buses. In practice, a delay rate may be prolonged, due to electromagnetic interference was be influenced by other factors. The quantitative relationship between simulation time and the ENDS is studied, and the results are shown in Figure 5. The value of the system ENDS increased considerably, and the growth rate of ENDS increased linearly with prolonged switching time. This illustrates that the delay rate of the process bus signifies the fault clearing. Advanced technologies for smart grids are important. Highly reliable control components and fast information transmission accelerate the process of cyber failure identification and physical fault clearing.

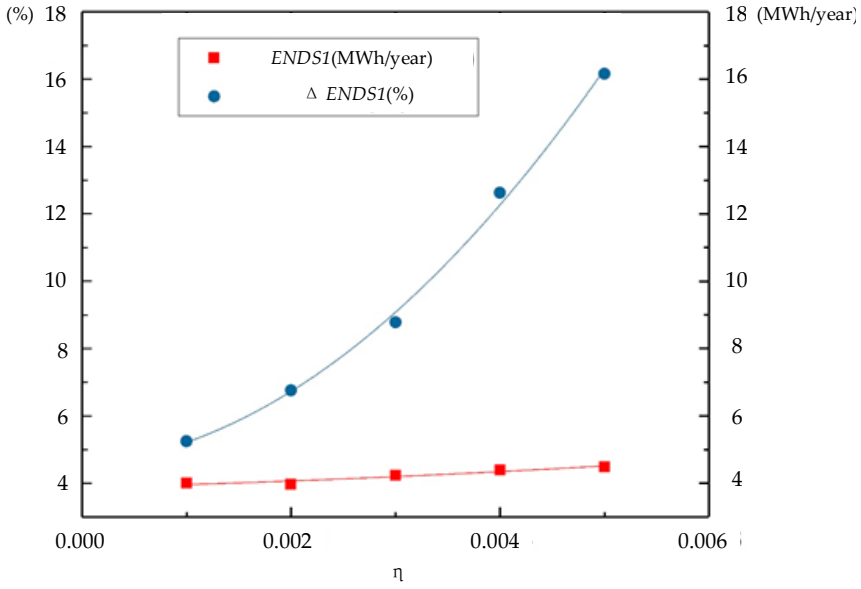

Figure 5. Expected Demand Not Supplied (EDNS) and EDNS changing with delay rate at load-point 1.

6. Conclusions

With the development of substation system automation applications, the interdependency between the communication network and the primary equipment must be considered. This paper extended the Cyber Physical Interface Matrix (CPIM) methodology to reliability analysis. Two reliability indexes were presented, and the results of the case study verified that failures in the cyber layer increase the substation system's reliability, and the sensitivity analysis revealed that the process bus plays a key role in the reliability of the entire substation. Although the probability of time delay in information transmission is small, it is the critical factor leading to reliability changes in cyber–physical substations.

The proposed reliability assessment method can also be used to address the reliability problem faced by cyber physical power systems. In such systems, for future study, more detailed analysis on the interdependency between physical side and cyber layer is needed.

Author Contributions: Writing-original draft, Writing-review and editing, Y.C. (Ye Cai) and Y.C. (Yu Chen); Y.L., methodology and resources; Y.C. (Yijia Cao) and X.Z., supervision.

Funding: This work was supported in part by the National Key R&D Program of China 2018YFB0904903, the national Natural Science Foundation of China (NSFC) 51607011 and 51577014.

Acknowledgments: This work was also supported by the Scientific Research Foundation of Hunan Education Department 17B006

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lee, E.A. Cyber Physical Systems: Design Challenges. In Proceedings of the 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA, 5–7 May 2008.
2. Anders, G.J. *Probability Concepts in Electric Power Systems*; OSTI.GOV: New York, NY, USA, 1990.
3. Cheng, X.; Lee, W.J.; Pan, X. Modernizing Substation Automation Systems: Adopting IEC Standard 61850 for Modeling and Communication. *IEEE Ind. Appl. Mag.* **2017**, *23*, 42–49. [CrossRef]
4. Bobbio, A.; Portinale, L.; Minichino, M.; Ciancamerla, E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliab. Eng. Syst. Saf.* **2001**, *71*, 249–260. [CrossRef]
5. Lim, S. A service interruption free testing methodology for IEDs in IEC 61850-based substation automation systems. *Electr. Power Energy Syst.* **2017**, *87*, 65–76. [CrossRef]
6. Falahati, B.; Fu, Y.; Wu, L. Reliability assessment of smart grid considering direct cyber-power interdependencies. *IEEE Trans. Smart Grid* **2012**, *3*, 1515–1524. [CrossRef]
7. Yoo, H.; Shon, T. Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements and security architecture. *Future Gener. Comput. Syst.* **2016**, *61*, 128–136. [CrossRef]
8. Moreira, N.; Molina, E.; Lázaro, J.; Jacob, E.; Astarloa, A. Cyber-security in substation automation systems. *Renew. Sustain. Energy Rev.* **2016**, *54*, 1552–1562. [CrossRef]
9. Mamo, X.; Mallet, S.; Coste, T.; Grenard, S. Distribution automation: The cornerstone for smart grid development strategy. In Proceedings of the 2009 IEEE Power & Energy Society General Meeting, Calgary, AB, Canada, 26–30 July 2009.
10. Kirschen, D.; Bouffard, F. Keep the lights on and the Information Flowing. *IEEE Power Energy Mag.* **2008**, *7*, 50–60. [CrossRef]
11. Falahati, B.; Fu, F. Reliability assessment of smart grids considering indirect cyber-power interdependencies. *IEEE Trans. Smart Grid* **2014**, *5*, 1677–1685. [CrossRef]
12. Lei, H.; Singh, C.; Sprinston, A. Reliability modeling and analysis of IEC 61850 based substation protection systems. *IEEE Trans. Smart Grid* **2014**, *5*, 2194–2202. [CrossRef]
13. Chen, J.; Thorp, J.S.; Dobson, I. Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model. *Int. J. Electr. Power Energy Syst.* **2005**, *27*, 318–326. [CrossRef]
14. Ferreira, L.C.; Crossley, P.; Allan, R. The impact of functional integration on the reliability of substation protection and control systems. *IEEE Trans. Power Del.* **2001**, *16*, 83–88. [CrossRef]
15. Cherdantseva, Y.; Burnap, P. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
16. Aghili, S.J.; Hoseinabadi, H.H. Reliability evaluation of repairable systems using various fuzzy-based methods-A substation sutomation case study. *Electr. Power Energy Syst.* **2017**, *85*, 130–142. [CrossRef]