energies

MDPI

Article

Reliability Evaluation of Smart Substation Based on Time-Varying Probabilistic Hybrid Attack Graph

Zhiyong Li [1,*], Wubin Wen [1], Rende Dai [2] and Wanting Xi [1]

[1] School of Automation, Central South University, Changsha 410083, China
[2] Hunan Zhongda Design Institute Co., Ltd., Changsha 410205, China
* Correspondence: lizy@csu.edu.cn; Tel.: +86-138-7312-7689

Abstract: A substation is the portion of a power grid that forms a link between the cyber system and the physical system. Reliability evaluation of smart substations based on a time-varying probabilistic hybrid attack graph (TVPHAG) is studied in this paper. First, the topology network of the smart substation is established, whose attributes are represented by probability. Then, in order to solve the problem of asynchrony in the cyber-physical system and the hybrid caused by heterogeneity, time-varying state equation in topology and cuts in algebra are introduced to TVPHAG. Based on TVPHAG, the evaluation of the reliability of cyber-physical systems with multiple equipment and multiple timescales is established. On this basis, the influences of physical conditions, cyberattacks, physical attacks, and cyber-physical attacks on substations are analyzed, respectively. Finally, the simulation shows that the method is effective in evaluating the reliability of smart substations, providing a new method for the evaluation of reliability.

Keywords: reliability evaluation; TVHPAG; smart substation; cyber-physical attack

Citation: Li, Z.; Wen, W.; Dai, R.; Xi, W. Reliability Evaluation of Smart Substation Based on Time-Varying Probabilistic Hybrid Attack Graph. *Energies* **2022**, *15*, 6724. https://doi.org/10.3390/en15186724

Academic Editors: Hugo Morais, Junjie Hu and Matej Zajc

Received: 11 August 2022
Accepted: 8 September 2022
Published: 14 September 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

The modern power grid is developing toward the cyber-physical power system (CPPS), which coordinates the cyber system and the physical power system [1]. A substation is the portion of a power grid that forms a link between the cyber system and the physical system. The cyber system monitors the state of the physical system and then sends real-time control information to the physical system [2,3]. The process is time-varying because of the asynchrony on the control system and interdependence between the cyber-physical system [4,5]. The cascading failure of the power grid has caused several incidents around the world, such as the large-scale blackout in Ukraine caused by a deliberate cyberattack in 2015 [6], the blackout in Israel in 2016 [7], and the blackout in Venezuela in 2019. The cyberattack may destroy the transient stability of the power grid through cross-space spreading, thus breaking the physical system, causing large-scale power outages [8,9], and even inducing power grid splitting [10]. Therefore, the reliability assessment of smart substations is of great importance.

Attack graph is a technology of security assessment. The possibility of attack paths can be calculated through the causality among attack steps [11]. Attack graphs can be used to identify network vulnerabilities and evaluate the safety of the system [12,13]. The reliability of substations is affected by physical equipment [14], and attack graphs are also used to identify hazards of physical conditions [15], such as risk assessment of power distribution equipment [16] and assessment of the status of the power grid attacked [17], etc.

To avoid the spread of risks between the cyber system and the physical system, one approach is to establish a model of interdependence using complex network theory to abstract the power grid and cyber grid into a stochastic network [18,19].

However, those papers ignore the complex coupling between them. In order to obtain quantitative results, the attack tree theory was used for vulnerability analyses and security assessments of SCADA (supervisory control and data acquisition system) [20–22].

Then, a quantifiable method combined with CVSS (Common Vulnerability Scoring System) was proposed. With the help of the Bayesian network, the method solved the problems of lacking quantification, lacking confidence, and lacking readability in the attack graph [23]. The Bayesian network was proposed to study the probability of cascading failures and their consequences of cyberattacks [24–26] and to trace the complete path of attacks [27].

The above papers have put forward probabilistic methods for the reliability evaluation of smart substations. However, being limited to static characteristics, they have difficulty capturing the time-varying and dynamic relationships of components and systems. Then a hierarchical Bayesian model was proposed, which achieved dynamic reliability evaluation by integrating historical data and real-time data [28], but it was not suitable for cyber-physical systems. In [29,30], the Bayesian network was used to track the complete path of attacks, which caused a cascading failure in the order of vulnerability on the network, host authority, and executor sequence. Taking probability and coupling into consideration, the model was used to study the relevance between the transition of system state and attack interval. Petri net was also used in the modeling of cyber-physical systems to figure out vulnerability cascade propagation [31,32]. Being used as a substation fault diagnosis method, it incorporates time sequence and probabilistic features and obtains the diagnosis results with the help of failure information [33]. However, the above methods were essentially used to study the time-invariant dynamic response under attack, ignoring the asynchrony and reconstruction of the network in a cascading failure process. The discrete-time state-space model provides another method for solving problems in the time domain [34]. However, so far, the research has usually established a linear time-invariant model of system state. Although it is applicable for physical conditions [35], cyberattacks [36], and Gaussian noise [37], it still fails to solve time-varying problems.

In addition, current research often ignored the complex time-varying coupling inside the substation. Some papers tried to study interdependence by using correlation matrices, but they only considered the one-to-one correspondence between the two layers to establish a 0–1 logical matrix [38]. The Petri net has the ability to analyze internal situations of substations, while it is a post-mortem diagnosis method, which requires the alarm information at the time of failure as a basis [39]. Some scholars have tried to use the artificial neural network (ANN) to evaluate its reliability. However, due to difficulties in obtaining fault samples and the lack of confidence [40], it is necessary to analyze the coupling between equipment inside the substation.

Aiming to solve the problem of poor practicability on reliability evaluation, this paper proposes a time-varying probabilistic hybrid attack graph and its generation algorithm. The method takes the cyber-physical conditions and the hybrid coupling of the substation into consideration, and it abstracts the equipment as a vertex to establish the attack graph based on the structure of the smart substation. Considering the timeliness of transmission in the network, the established model reflects asynchrony and reconstruction of the network and then infers the dynamic changes in the reliability of each piece of equipment and the substation. The simulations of TVPHAG illustrate the characteristics of physical conditions, cyberattacks, physical attacks, and cyber-physical attacks, which provides guidance for ensuring the safety of substations.

2. Definition and Description of TVPHAG

This paper proposes the time-varying probabilistic hybrid attack graph (TVPHAG), whose vertices and edges will be explained by probability weighing. The model is suitable for smart substations with heterogeneous components, dynamics, and asynchronous behaviors. Moreover, the evaluation for each vertex in the grid is proposed. The definition and algorithm of TVPHAG $G(V, E, \boldsymbol{\alpha}, T)$ are given as follows:

2.1. Establishment of Network

TVPHAG is a directed graph whose topology is determined by V, E.

The set of vertices is defined as:

$$\begin{cases} V = V_e \cup V_C \\ V_e = \{v_1^e, v_2^e \cdots v_i^e \cdots v_M^e\} \\ V_C = \{v_1^c, v_2^c \cdots v_j^c \cdots v_N^c\} \end{cases} \tag{1}$$

In Equation (1), V represents the set of all vertices in TVPHAG, where V_e represents the set of vertices of equipment, and V_c represents the set of vertices of consequence. v_i^e represents equipment, with a total of M. v_j^c represents the consequences of cascading failures, with a total of N.

The set of edges is defined as:

$$\begin{cases} E = E_A \cup E_B \\ E_A = \left\{e_{i,j}^A \middle| v_i^e \in V_e, v_j^e \in V_e\right\} \\ E_B = \left\{e_{k,r}^B \middle| v_k^e \in V_e, v_r^c \in V_c\right\} \end{cases} \tag{2}$$

In Equation (2), $e_{k,r}$ represents a directed edge $\langle v_k, v_r \rangle$. E is the set of directed edges with coupling between vertices, i.e., the set of paths of spread.

The geometric topology of TVPHAG is established through the following rules: (1) The messages and instructions on the secondary side are directed from the previous level to the next level; (2) The secondary equipment points to the primary equipment controlled by it; (3) The primary equipment points to the measuring equipment, (4) Other couplings between the equipment; (5) The primary equipment with abnormality points to the corresponding consequences.

2.2. Establishment of Parameter

The parameter of TVPHAG includes $\boldsymbol{\alpha}$,T, where:

The vector of the device's attribute is defended as:

$$\boldsymbol{\alpha} = [\alpha_1, \alpha_2 \cdots \alpha_i \cdots \alpha_M]^T,\ \alpha_i \in [0,1] \tag{3}$$

$$f: V_e \to \{\alpha_i\}, f(v_i^e) = \alpha_i \tag{4}$$

In Equation (3), α_i represents the self-triggering probability of the vertex of equipment v_i in TVPHAG, i.e., the probability of equipment spontaneously failing, which is affected by operating conditions, working years, and other factors.

In Equation (4), $\to$ represents the mapping from the left set to the right set, f represents the mapping function. The mapping of $V_e \to \{\alpha_i\}$ is a one-to-one correspondence, i.e., a bijection.

The matrix of the directed edge is defined as:

$$T = [A\ B], A = \begin{bmatrix} 0 & \beta_{2,1}^A & \cdots & \beta_{M,1}^A \\ \beta_{1,2}^A & 0 & \cdots & \beta_{M,2}^A \\ \vdots & \vdots & \beta_{i,j}^A & \vdots \\ \beta_{1,M}^A & \beta_{2,M}^A & \cdots & 0 \end{bmatrix}, B = \begin{bmatrix} \beta_{1,1}^B & \beta_{2,1}^B & \cdots & \beta_{M,N}^B \\ \beta_{1,2}^B & \beta_{2,2}^B & \cdots & \beta_{M,2}^B \\ \vdots & \vdots & \beta_{k,r}^B & \vdots \\ \beta_{1,N}^B & \beta_{2,N}^B & \cdots & \beta_{M,N}^B \end{bmatrix}, \beta_{k,r} \in [0,1] \tag{5}$$

$$g: E \to \{\beta_{k,r}\}, g\left(e_{i,j}^A\right) = \beta_{i,j}^A, g\left(e_{k,r}^B\right) = \beta_{k,r}^B \tag{6}$$

In Equation (5), $\beta_{k,r}$ is defined as the triggering probability. A is defined as the matrix of probability that faults are triggered by other vertices, whose element $\beta_{i,j}^A$ represents the probability that v_i^e causes v_j^e a malfunction ($v_i^e \in V_e, v_j^e \in V_e$). The element $\beta_{k,r}^B$ in the matrix B represents the probability of v_k^e causing v_r^c a malfunction ($v_k^e \in V_e$, $v_r^c \in V_e$).

In Equation (6), g is the mapping relationship between the sets formed by elements in T and sets E_A and E_B, which is a bijection.

In this paper, the MTTF (Mean Time To Failure) λ of equipment is used as the self-triggering probability $\boldsymbol{\alpha}$. However, the conditions of the substation and equipment are different. The influence of temperature, operating years, precipitation, loading rate, etc., should be considered. The above factors are set as independent variables of $\Omega = [\omega_1(℃)\ \omega_2(y)\ \omega_3(mm)\ \omega_4(\%)]$, and the relative failure probability is recorded as $F(\Omega) = F(f_1(\omega_1), f_2(\omega_2), f_3(\omega_3), f_4(\omega_4))$. According to the big data on equipment failure, the following relationship is obtained [41]:

$$\begin{cases} f_1(\omega_1) = 6.7463 \times 10^{-5}\omega_1^2 - 0.0011\omega_1 + 0.0192 \\ f_2(\omega_2) = 0.02576 \times (1.1861)^{\omega_2} \\ f_3(\omega_3) = 0.1306\omega_3 + 0.0148 \\ f_4(\omega_4) = \begin{cases} 0.0066 & (0 < \omega_4 \le 36) \\ 0.46\omega_4 - 0.159 & (36 < \omega_4 \le 150) \end{cases} \end{cases} \quad (7)$$

Those factors, viz. temperature, operating years, precipitation, and loading rate, should be calculated respectively for reliability because of different weights. According to technical standards and actual operating conditions of power equipment, such information is collected for the preparation of calculation. The correction coefficient F of λ is calculated by Equation (8):

$$F(\Omega) = \prod_{i=1}^{4} \frac{f_i(\omega_i)}{f_i(\omega_i^*)} \quad (8)$$

where $\omega_i^*(i = 1,2,3,4)$ are the reference, contributing to vector $\Omega^* = [\omega_1^*\ \omega_2^*\ \omega_3^*\ \omega_4^*] = [15\ 6\ 10\ 50]$, which is selected according to the statistical data. The MTTF is replaced by $\lambda_j' = F(\Omega_j) \times \lambda_j$. Finally, the self-triggering probability can be described as $\boldsymbol{\alpha_e'} = \boldsymbol{F} \cdot \boldsymbol{\alpha_e}, \boldsymbol{F} = [F(\Omega_1), F(\Omega_2) \cdots F(\Omega)]^T$.

2.3. Analysis of the Spread of Faults

Abnormal data or actions are accompanied by abnormal states of the equipment. In TVPHAG, the probability of failure changes as the abnormal state spreads through the equipment. The spread of state is asynchronous due to the delay of physical equipment's action, information transmission, data sampling, etc. The process is analyzed as follows:

According to the standard of IEC61850, all messages of smart substation are divided into seven categories according to the time range of transmission. The main information flow of the process layer is GOOSE, SV, and synchronization messages. The transmission time of the secondary message [42] and the response time of the primary device [43] are given below and shown in Tables 1 and 2:

Table 1. Typical response delay of the primary equipment.

Category	Name	Requirements of Delay Time
1a	Fast message—trip	*P*1 [1]: 10 ms, *P*2 [2]: 3 ms
1b	Fast message—other	*P*1: 100 ms, *P*2: 20 ms
2	Medium-speed message	100 ms
3	Low-speed message	500 ms
4	Raw data	/
5	File transfer	1000 ms
6	Synchronization message	10 ms
7	Command message	Cat 7 = Cat 3, downloading = Cat 1

[1] *P*1: Feeder bay; [2] *P*2: General bay or no specific requirements.

Table 2. Response delay of the primary equipment.

Category		Delay Time
Circuit breaker	Open	25 ms
	Closing	100 ms
Disconnect switch		1000 ms
Current/voltage transfer(C/VT)		1 ms

The transfer of the device's state has a delay caused by the period of sampling, transmission, and processing of messages and the action of the equipment. In TVPHAG, it is manifested as the delay of the failure cascading. Therefore, TVPHAG is a dynamic directed graph with asynchrony. Figure 1 shows a simple TVPHAG, which can be divided into multiple subgraphs according to the period of delay. In this paper, the transmission mechanism of failure probability is represented by matrices A and B. Through the above analyses, matrices A and B are time-varying.

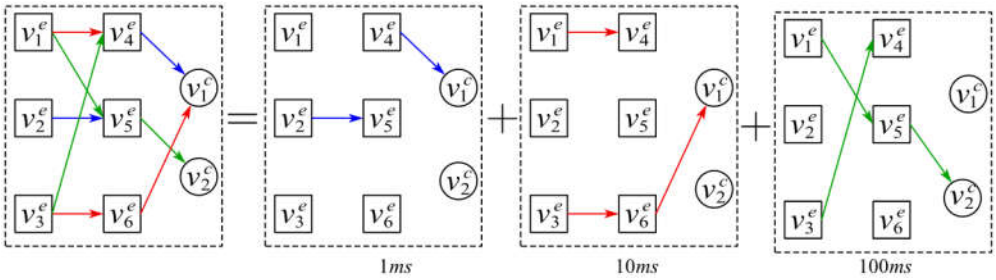

Figure 1. A simple example of TVPHAG.

Through the above methods, the reliability of equipment and bays can be calculated and expressed as a probability, and then the loss-of-load probability (LOLP) of the substation can be calculated according to the connection relationship and operation mode of each bay. LOLP is defined as expected losses of load per unit.

2.4. Algorithm of TVPHAG

The failure probability of equipment x_n is influenced by the following factors: the equipment spontaneously transfers to an abnormal state with the probability α_n; the equipment state is affected by other equipment with the probability $\sum_{m\in R(n)} x_m \times \beta_{m,n}$. Where $m \in R(n)$, $R(n)$ represents the set of the entering edge of v_n. x_m represents the failure probability of v_m.

Therefore, the failure probability of v_n is obtained as Equation (9):

$$x_n = \alpha_n + \sum_{m\in R(n)} x_m \times \beta_{m,n} \tag{9}$$

A discrete-time system is established by discretizing time. $x_i^{(k)}$ represents the failure probability of v_i at time k. Equation (9) is extended to all vertices in sets V_e and V_c and expressed in matrix forms in Equation (10) and Equation (13):

$$\begin{bmatrix} x_1^{(k+1)} \\ x_2^{(k+1)} \\ \vdots \\ x_M^{(k+1)} \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_M \end{bmatrix} + \begin{bmatrix} 0 & \beta_{2,1}^A & \cdots & \beta_{M,1}^A \\ \beta_{1,2}^A & 0 & \cdots & \beta_{M,2}^A \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{1,M}^A & \beta_{2,M}^A & \cdots & 0 \end{bmatrix} \begin{bmatrix} x_1^{(k)} \\ x_2^{(k)} \\ \vdots \\ x_M^{(k)} \end{bmatrix} \tag{10}$$

$$\begin{bmatrix} y_1^{(k)} \\ y_2^{(k)} \\ \vdots \\ y_N^{(k)} \end{bmatrix} = \begin{bmatrix} \beta_{1,1}^B & \beta_{2,1}^B & \cdots & \beta_{M,N}^B \\ \beta_{1,2}^B & \beta_{2,2}^B & \cdots & \beta_{M,2}^B \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{1,N}^B & \beta_{2,N}^B & \cdots & \beta_{M,N}^B \end{bmatrix} \begin{bmatrix} x_1^{(k)} \\ x_2^{(k)} \\ \vdots \\ x_M^{(k)} \end{bmatrix} \tag{11}$$

According to Equations (10) and (11), the smart substation is modeled as a multi-variable discrete-time linear time-invariant system.

$$\boldsymbol{x}^{(k+1)} = \boldsymbol{\alpha} + A\boldsymbol{x}^{(k)} \tag{12}$$

$$\boldsymbol{y}^{(k)} = B\boldsymbol{x}^{(k)} \tag{13}$$

The vector $\boldsymbol{x}$ is iteratively updated in the process of calculation, which means the equipment turns to a new state after physical equipment actions, information transmission, and data sampling. Each iteration is the update cycle of device status, which is related to sampling action time and path length. The TVPHAG proposed in this paper considers the heterogeneity of various equipment and the asynchrony of action response, so the dynamic matrix of state update is time-varying, and its establishment method is introduced in Section 2.3. Analysis of the spread of faults. Based on the original model, it is further modeled as a multi-variable discrete-time linear time-varying system:

$$\boldsymbol{x}^{(k+1)} = \boldsymbol{\alpha} + A^{(k)}\boldsymbol{x}^{(k)} \tag{14}$$

$$\boldsymbol{y}^{(k)} = B^{(k)}\boldsymbol{x}^{(k)} \tag{15}$$

With the iterative calculation, vector $\boldsymbol{x}$ is continuously updated until it is of convergence. This paper gives the condition of convergence without proof [44]: the spectral radius $\rho\left(A^{(k)}\right) = max\{|\lambda_i|\} < 1$, where λ_i is the eigenvalue of the matrix $A^{(k)}$.

In terms of physical attacks or cyberattacks on the substation, which cause an abnormal state of the equipment, the elements of the attack vector $\boldsymbol{u}^{(k)} = [u_1^{(k)}\ u_2^{(k)} \cdots u_m^{(k)}]$ are formed with the attack strength, where $u_i^{(k)} \in [0,1]$ represents the probability of the attack causing an abnormal state of the equipment at time k. For the physical attack, the energy intensity applied or caused by attacks is used to evaluate the failure probability. Considering the voltage level of the equipment, the current determines the hazard levels. The current caused by the direct lightning strike can reach 40 kA, and the current caused by short-circuit of the line can reach 1 kA. It is believed that the direct lightning will cause a failure, then $u_i^{(k)} = 1/40$ at the situation of short-circuit. Cyberattacks are divided into three categories according to the purpose, i.e., destroying availability, integrity, and confidentiality of information. The value of $u_i^{(k)}$ is determined by the type and intensity of the cyberattack. In particular, $u_i^{(k)} = 1$ represents that the attack will definitely cause an abnormal state of the equipment v_i^e, while $u_i^{(k)} = 0$ represents no attack.

The matrix $C^{(k)}$ is established by the wiring of the substation, the load of the incoming and outgoing lines, and the operation mode. Finally, the multi-variable discrete-time linear time-invariant model of the smart substation is established in Figure 2 and Equation (16).

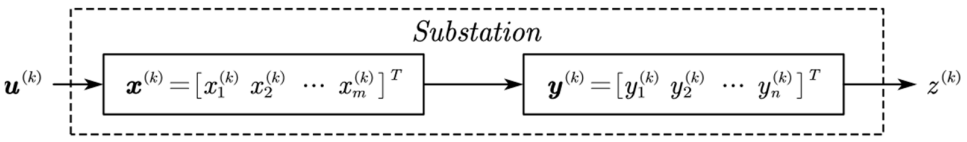

Figure 2. Multi-variable discrete-time linear time-invariant model of smart substation.

$$\begin{cases} \boldsymbol{x}^{(k+1)} = A^{(k)}\boldsymbol{x}^{(k)} + \boldsymbol{\alpha} + \boldsymbol{u}^{(k)} \\ \boldsymbol{y}^{(k)} = B^{(k)}\boldsymbol{x}^{(k)} \\ z^{(k)} = C^{(k)}\boldsymbol{y}^{(k)} \end{cases} \tag{16}$$

where $\boldsymbol{x}^{(k)} \in \mathbb{R}^m$ represents the vector of failure probability; $\boldsymbol{y}^{(k)} \in \mathbb{R}^n$ represents the vector of consequences of bays; $z^{(k)}$ represents the reliability of substations, i.e., LOLP; $\boldsymbol{u}^{(k)} \in \mathbb{R}^m$ represents the cyber-physical attack on the substation, and matrices A, B, C are dynamic matrices.

3. Results and Case Study of TVPHAG

The D2-1 smart substations in IEC 61,850 presently have been built more, including transformer bays, bus bays, and feeder bays. The primary equipment includes primary power equipment such as buses, transformers, circuit breakers (CB), disconnect switches (DS), and electronic voltage current transformers (VCTs). The secondary equipment includes the merging unit (MU), the intelligent electronic device (IED), the protection device (PD) and the measurement and control device (MD), switches, Network Control Center Server (NCCS), and other equipment [45]. The secondary system can be divided into three levels, viz., station level, bay level, and process level. This paper takes the D2-1 110 kV smart substation as an example. It has 2 SSZ10—40,000/110 main transformers with a total capacity of 2 × 40 MVA, with 110 kV sectionalized configuration, 2 incoming and outgoing lines, etc. Its topology is shown in Figure 3, where A and B are transformer bays, C is a bus bay, D and E are feeder bays, and the same type of bays has the same structures and configurations.

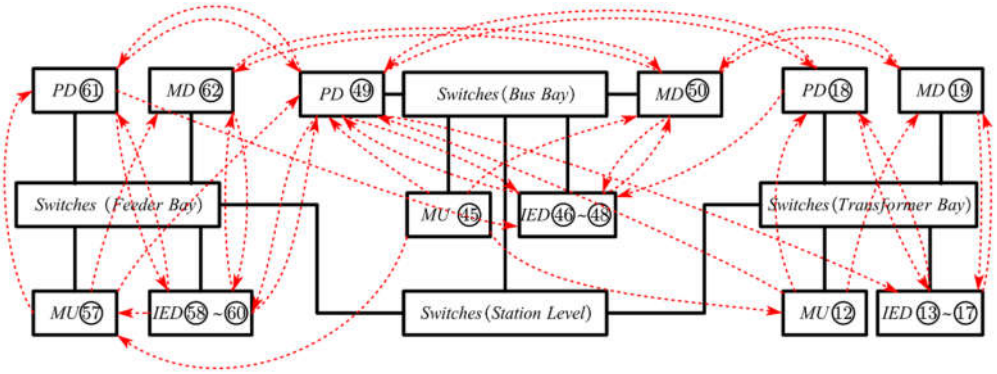

Figure 3. The message flow of smart substation.

TVPHAG is established according to the above analyses of the primary and secondary equipment of the smart substation. Figures 3 and 4 show the corresponding equipment of some vertices, and the other equipment can be expanded by their consistency. The vertices of the equipment and consequences of TVPHAG are distinguished by circles and squares in Figure 5. The description of vertices in Figure 5 is shown in Table 3.

Table 3. The description of vertices in Figure 5.

Category	Label	Correspondence
Vertices of Consequence	A, B	Transformer bay
	C	Bus bay
	D, E	Feeder bay
Vertices of Equipment	1–4,20–23,39–41,51–53,63–65	C/VT
	5,24,	Bus
	6,25,	Transformer
	7–9,26–28,43,44,54,55,66,67	DS
	10,11,29,30,42,56,68	CB
	12,31,45,57,69	MU
	13–17,32–36,46–48,58–60,70–72	IED
	18,37,49	PD

	19,38,50	MD
	75	Telecontrol NCCS
	76	Communication NCCS

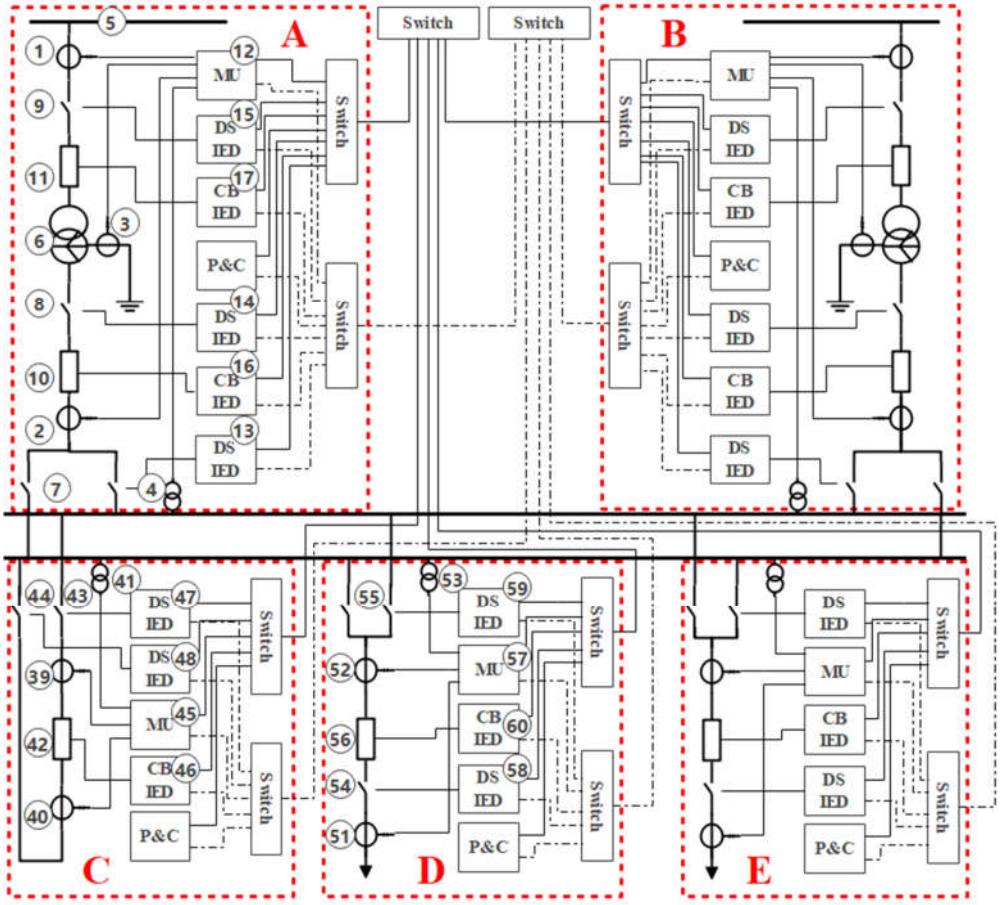

Figure 4. Topology of D2-1 smart substation.

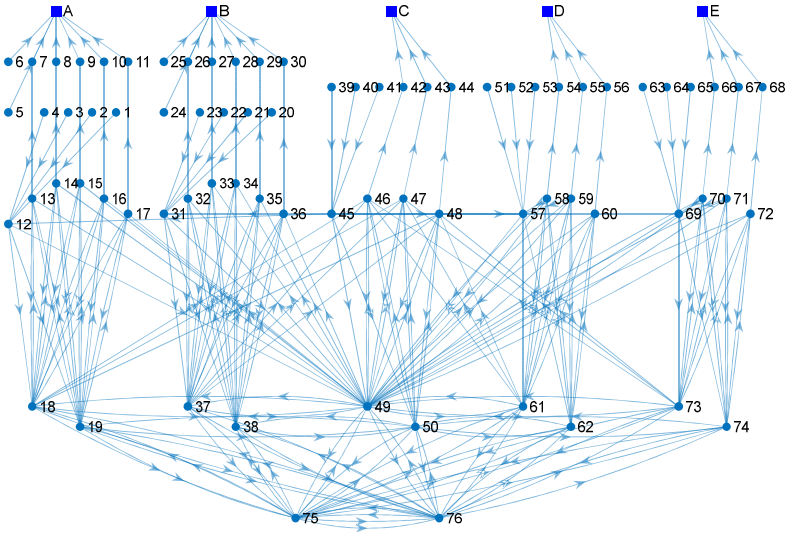

Figure 5. TVPHAG of D2-1 smart substation.

The self-triggering probability α_i is defined as MTTF λ, and shown in Table 4 [46,47]:

Table 4. Reliability data of equipment.

Equipment		$\lambda(year^{-1})$
PD		0.0067
MD		0.0067
IED		0.0050
MU		0.0200
NCCS		0.0699
Transformer	300 kVA–10 MVA	0.0059
	>10 MVA	0.0153
CB	0–600 V	0.0042
	>600 V	0.0096
Bus		0.0012
DS		0.0061
C/VT		0.0049

This paper firstly discusses the influence of β. According to the spectral radius of the matrix $A(k)$, the convergence condition of the established model is calculated, that is, $\beta < 0.135$. Moreover, the result is shown in Figure 6.

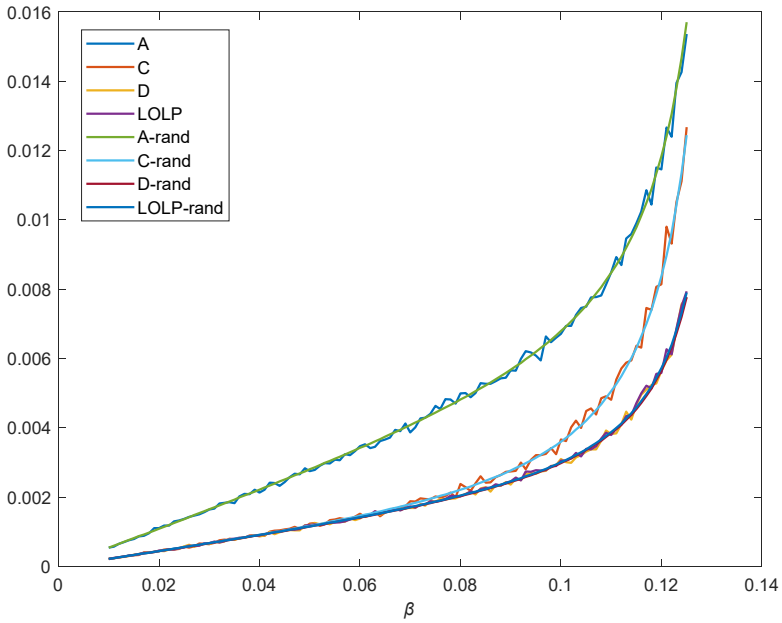

Figure 6. The failure probability as the increase in β

According to the coupling and wiring of each bay of the substation, the formula of LOLP is shown as:

$$P_{Loss} = \sum_{i\in\{A,B\}} y_i \times y_C \times 0.5 \times 1(p.u.) + \sum_{i\in\{C,D\}} y_i \times 0.5\,(p.u.) \quad (17)$$

In Equation (17), the function $y_A \times y_C \times 0.5 \times 1$ represents that the bay of A and bay of bus get failures, and the probability of working on any one of the buses is equal. In this case, all loads are lost, which can be changed in accordance with the actual operations of

the substation. The function $y_C \times 0.5$ represent the bay of C that gets failures, and the load of any one of the feeder bays is equal.

The probability of failure increases with the increase in β. The simulation is shown in Figure 6. Two cases are simulated in this paper. One case is that β is a constant value, and the other is that β is evenly distributed around the constant value. The failure probability of the system increases exponentially and rapidly when $\beta > 0.12$. Therefore, the situation that $\beta > 0.12$ should be avoided. In practical engineering, β is related to the degree of connection relationships between equipment. In this study, $\beta = 0.12$ is selected for the particularity.

- Static features:

To get a clearer picture of the impact of physical conditions, it is assumed that the primary equipment on bays E and D with a loading rate of 80%, and the other conditions are reference values. According to Equations (9) and (10), the correction coefficient $F = 2.9437$, that is, the MTTF of vertex $v_{20} \sim v_{29}. v_{63} \sim v_{68}$ is $\lambda' = 2.9437 \times \lambda$.

According to Tables 2 and 3, in the case of this paper, the delay of processes includes 1 ms, 3 ms, 10 ms, 20 ms, 25 ms, 100 ms, 500 ms, and 1000 ms. According to the delay of switching on states, eight attack graphs are established on the same time scale. These graphs are all subgraphs of the TVPHAG established above.

Comparing the two situations where the loading is at a reference and over 80% of it, the result of primary equipment in bay E and bay D is shown in Figure 7. The darker bar represents the situation of reference. In contrast, the lighter bar represents the situation where the loading exceeds reference.

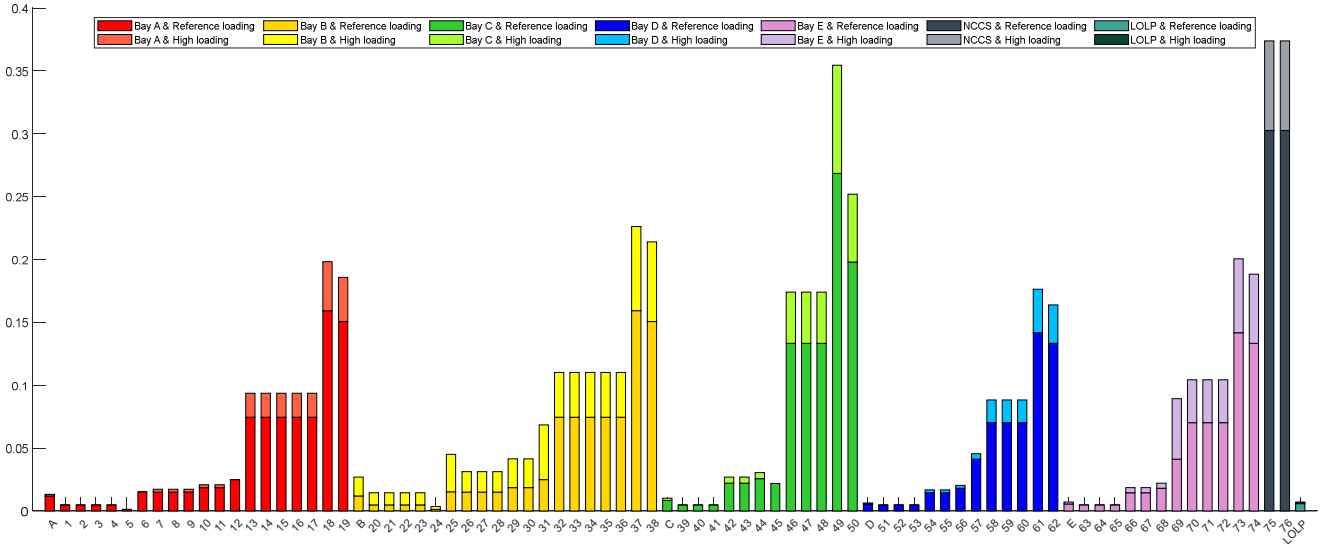

Figure 7. Failure probability under high and low loading rates.

The comparison is shown in Figure 7. Under the high load of primary equipment with only interval E and interval D, the failure probability of the bay whose equipment is in a harsh condition increases a lot, and other bays also see relatively small increases. The cause is that the anomalous data obtained by sampling is injected into other bays, which may lead to anomalies. The improvement in the E bay is much smaller than that of the B bay because the B bay has more primary equipment and is connected in series. From the above results in Figure 7, operating conditions of physical equipment have a greater impact on this bay. The impact on other bays is relatively limited.

The LOLP under different physical conditions is recorded in Table 5. Considering that the physical conditions of substations do not change drastically, the factors are set to deviate from the reference value by 10% and 20%. The impact of precipitation is relatively

small; the high temperature promotes a more rapid increase in hazards. LOLP increases proportionally with the increase in loading rates and operating years. The result verifies the correctness of the model.

Table 5. LOLP on different physical conditions.

Deviation	Temperature	Age	Precipitation	Load
−20%	0.562%	0.524%	0.551%	0.520%
−10%	0.570%	0.548%	0.568%	0.547%
0		0.575%		
10%	0.585%	0.605%	0.582%	0.603%
20%	0.627%	0.638%	0.590%	0.630%

- Dynamic features

The vertex 75 of TVPHAG is attacked from t = 50 ms to t = 6000 ms by simulation. The results of bay A, bay B, bay C, PD, MD, and NCCS are shown in Figure 8. The failure probability increases rapidly within 2s after the attacks' arrival. The response of each device has a delay after the attack is applied or removed because the transition between the normal state and the abnormal state requires time to transfer and process.

The failure probability reaches more than 80% of the increased value within 2 s after the vertex is attacked, while it takes 4 s to drop to 20% of the increased value after the attack is removed. The simulation is in line with the phenomenon that is easy to damage while hard to recover.

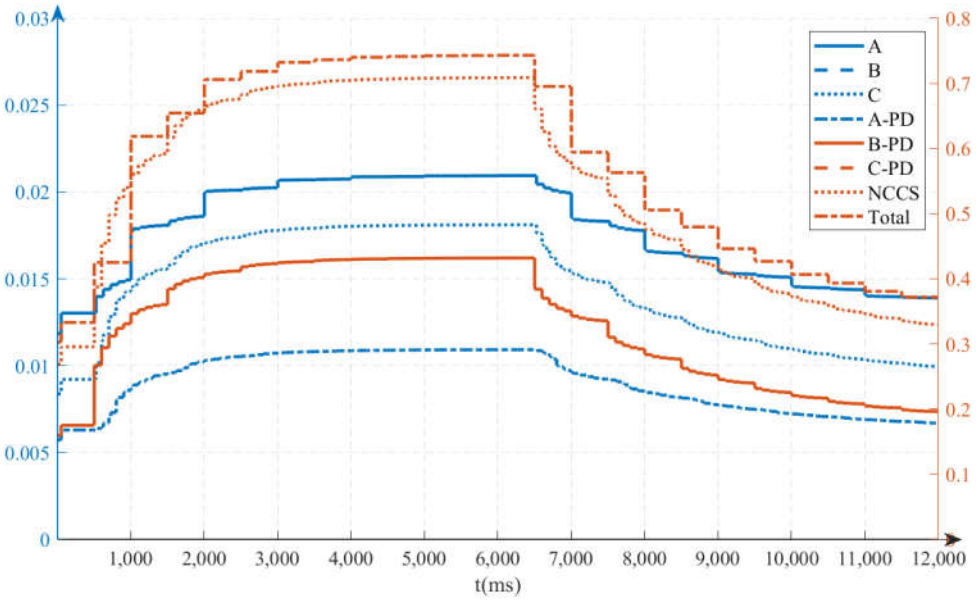

Figure 8. Dynamic change of failure probability after the attack.

During the followed simulation of TVPHAG, continuous physical attacks, cyberattacks, and cyber-physical attacks are respectively applied and analyzed. The main equipment and bays viz., bay A, bay B, bay C, PD, MD, and NCCS, are observed and analyzed.

Figure 9 shows the failure probability of the simulation that attacks arrive at t = 50 ms. Various delays such as sampling and transmission of processing, actions of equipment, etc.

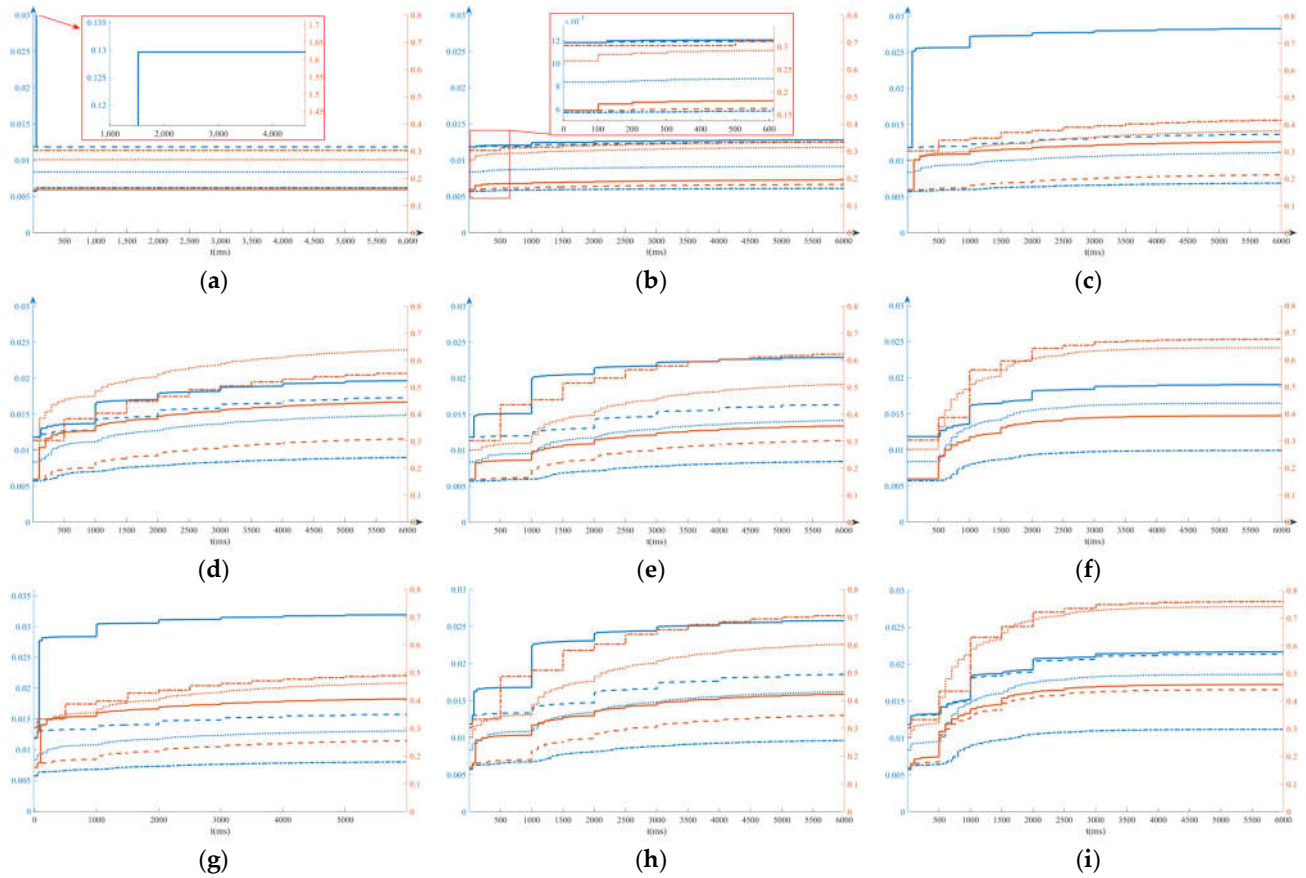

Figure 9. Dynamic diagram of failure probability of multi-type attack. (**a**) CB (bay A) is attacked, (**b**) transformer (bay A) is attacked, (**c**) CB-IED (bay A) is attacked, (**d**) MU (bay A) is attacked, (**e**) MD (bay A) is attacked, (**f**) NCCS is attacked, (**g**) transformer (bay A) and CB-IED (bay A) are attacked, (**h**) transformer (bay A) and MD (bay A) are attacked, (**i**) transformer (bay A) and NCCS are attacked.

Several main indexes are selected in this paper as indicators, including the failure probability of the bay where the attack is located, the mean failure probability of other bays, and LOLP. The critical time is selected to indicate corollary, that is, 50 ms (initial state), 500 ms, 1000 ms (rise rapidly), and 6000 ms (stable). The result is shown in Table 6.

Table 6. Record table of critical time probability of multi-type attacks (unit: %).

Time(ms) / Case	The Bay Attacked				Average of Other Bays				LOLP			
	50	500	1000	6000	50	500	1000	6000	50	500	1000	6000
A		12.96	12.96	12.96		0.788	0.788	0.788		0.622	0.622	0.622
B		1.205	1.207	1.28		0.802	0.807	0.844		0.582	0.588	0.612
C		2.566	2.567	2.829		0.817	0.828	0.953		0.585	0.6	0.689
D		1.358	1.37	1.965		0.903	0.943	1.244		0.655	0.702	0.898
E	1.184	1.508	1.51	2.289	0.788	0.821	0.833	1.174	0.572	0.582	0.598	0.844
F		-	-	-		0.867	1.109	1.479		0.572	0.779	0.992
G		2.834	2.836	3.191		0.914	0.932	1.108		0.656	0.678	0.800
H		1.674	1.679	2.578		0.917	0.936	1.338		0.651	0.674	0.963
I		1.326	1.518	2.167		0.882	1.173	1.547		0.640	0.875	1.118

As for the physical attacks, the attack on the measuring equipment, such as a C/VT, has the characteristics of small influence range, fast action, and little hazard. The attack

on important primary equipment such as CB will cause direct failures of this bay and greatly increase LOLP while having little impact on other bays.

Compared with physical attacks, the transmission of cyberattacks on substations is more complicated, causing larger hazards both on range and time. The failure probability of the secondary equipment is significantly improved, which can also spread across bays. At the same time, it has the possibility of affecting the servers in the station and spreading to other power stations. Compared with the attack on the bay layer, the attack on the access layer mainly affects the primary and secondary equipment of the bay while threatening the cyber system of the whole station less. Compared with attacks on the station layer, the attack on the bay layer is more harmful to this bay and less threatening to other bays, so abnormal states often appear on this line.

The cyber-physical attack has the characteristics of both physical attacks and cyberattacks. Due to the complex transmission of the TVPHAG, the abnormality of one device may cause an abnormality in other equipment. Therefore, under cyber-physical attack, the failure probability is mutually coupled and superimposed. The TVPHAG can reveal the relationship between system risks and attacks and its dynamic trends.

4. Discussion

This paper proposes the TVPHAG, which discretizes the state of the system. The model constructs a one-to-one mapping between the availability of the equipment/bay and nodes of TVPHAG. Based on the internal correlation of the system, the subgraphs of TVPHAG are established by the time scale of equipment transmission. The model solves the problem of asynchrony in the cyber-physical system and the phenomenon of confounding caused by heterogeneity and dynamically evaluates the reliability of the system.

The contribution of this paper exists in the following aspects: on the one hand, a smart substation is a complex network with cyber and physical equipment, including complex data flows and connection of the equipment, facing threats of cyber-physical attacks. By expressing uncertainty in probabilities, TVPHAG adapts to this complex network and simulates the cascade propagation process. On the other hand, due to the delay of state transfer, time-varying state equations in topology and cuts in algebra are introduced to TVPHAG. Combined with graph theory and algebra, it overcomes the insufficiency caused by only analyzing static networks in current research and helps to analyze the state of complex systems over time. In addition, being different from diagnosis, TVPHAG does not require information after the occurrence of faults, while it can evaluate the reliability of the system by using the basic information of the system's equipment and professional data in the field. On this basis, the research's conclusions on substation reliability can provide a reference for future substation construction and upgrade planning and designing.

There are several aspects worth studying in the future. (1) The method deals with systems as linear dynamics. Many device processes are linear or can be linearized, while some cannot be handled by linearization. Designing nonlinearity is a direction for future work. (2) The method deals with the association relationship based on messages. In actual production, the message has more characteristics due to different objects and types. Establishing more specific characteristics for more types of equipment and messages is one direction to improve reliability. (3) The failure transmission probability data needs to be supported by many experiments or big data, and this aspect is still thin at present.

Author Contributions: Conceptualization, W.W. and Z.L.; methodology, W.W. and Z.L.; software, W.W.; validation, W.X.; formal analysis, W.W.; investigation, R.D.; resources, Z.L.; data curation, R.D.; writing—original draft preparation, W.W.; writing—review and editing, W.W.; visualization, R.D. and W.X.; supervision, Z.L.; project administration, W.W.; funding acquisition, Z.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Fundamental Research Funds for the Central Universities of Central South University.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: Thanks are due to Sijie Shao, of Central South University, for the help in testing.

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

References

1. Adamiak, M.; Baigent, D.; Mackiewicz, R. *IEC 61850 Communication Networks and Systems in Substations: An Overview for Users*; University of Illinois at Urbana: Champaign, IL, USA, 2009.
2. Ahmad, T.; Senroy, N. An Information Theoretic Approach to Power-Substation Level Dynamic State Estimation with Non-Gaussian Noise. *IEEE Trans. Power Syst.* **2020**, *35*, 1642–1645. https://doi.org/10.1109/TPWRS.2020.2965795.
3. Bagen, B.; Huang, D.G.; Fattal, K. Enhanced probabilistic approach for substation reliability assessment. *IET Gener. Transm. Distrib.* **2019**, *13*, 2488–2495. https://doi.org/10.1049/iet-gtd.2019.0133.
4. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. https://doi.org/10.1038/nature08932.
5. Cai, B.P.; Kong, X.D.; Liu, Y.H.; Lin, J.; Yuan, X.B.; Xu, H.Q.; Ji, R.J. Application of Bayesian Networks in Reliability Evaluation. *IEEE Trans. Ind. Inform.* **2019**, *15*, 2146–2157. https://doi.org/10.1109/TII.2018.2858281.
6. Dai, Q.S.; Shi, L.B.; Ni, Y.X. Risk Assessment for Cyberattack in Active Distribution Systems Considering the Role of Feeder Automation. *IEEE Trans. Power Syst.* **2019**, *34*, 3230–3240. https://doi.org/10.1109/TPWRS.2019.2899983.
7. Duan, D.; Wu, X.; Deng, H. Reliability Evaluation in Substations Considering Operating Conditions and Failure Modes. *IEEE Trans. Power Deliv.* **2012**, *27*, 309–316. https://doi.org/10.1109/TPWRD.2011.2173807.
8. Falodiya, K.; Das, M.L. Security Vulnerability Analysis using Ontology-based Attack Graphs. In Proceedings of the 2017 14th IEEE India Council International Conference (INDICON), Roorkee, India, 15–17 December 2017; pp. 1–5. https://doi.org/10.1109/INDICON.2017.8488002.
9. Al Ghazo, A.T.; Ibrahim, M.; Ren; H.; Kumar, R. A2G2V: Automatic Attack Graph Generation and Visualization and Its Applications to Computer and SCADA Networks. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *50*, 3488–3498. https://doi.org/10.1109/TSMC.2019.2915940.
10. Hawrylak, P.J.; Haney, M.; Papa, M.; Hale, J. Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid. In Proceedings of the 2012 5th International Symposium on Resilient Control Systems, Salt Lake City, UT, USA, 14–16 August 2012; pp. 161–164. https://doi.org/10.1109/ISRCS.2012.6309311.
11. Holm, H.; Ekstedt, M.; Andersson, D. Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks. *IEEE Trans. Dependable Secur. Comput.* **2012**, *9*, 825–837. https://doi.org/10.1109/TDSC.2012.66.
12. Huang, K.; Zhou, C.; Qin, Y.; Tu, W. A Game-Theoretic Approach to Cross-Layer Security Decision-Making in Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Electron.* **2020**, *67*, 2371–2379. https://doi.org/10.1109/TIE.2019.2907451.
13. Huang, K.; Zhou, C.; Tian, Y.C.; Yang, S.; Qin, Y. Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Electron.* **2018**, *65*, 8153–8162. https://doi.org/10.1109/TIE.2018.2798605.
14. James, K.R. Convergence of matrix iterations subject to diagonal dominance. *SIAM J. Numer. Anal.* **1986**, *10*, 117–132. https://doi.org/10.1137/0710042.
15. Kirrmann, H.; Dzung, D. Selecting a Standard Redundancy Method for Highly Available Industrial Networks. In Proceedings of the IEEE International Workshop on Factory Communication Systems, Turin, Italy, 28–30 June 2006; pp. 386–390. https://doi.org/10.1109/WFCS.2006.1704184.
16. Lanotte, R.; Merro, M.; Munteanu, A.; Vigano, L. A Formal Approach to Physics-based Attacks in Cyber-physical Systems. *ACM Trans. Priv. Secur.* **2020**, *23*, 1–41. https://doi.org/10.1145/3373270.
17. Law, Y.W.; Alpcan, T.; Palaniswami, M. Security Games for Risk Minimization in Automatic Generation Control. *IEEE Trans. Power Syst.* **2015**, *30*, 223–232. https://doi.org/10.1109/TPWRS.2014.2326403.
18. Lei, H.; Singh, C.; Sprintson, A. Reliability Modeling and Analysis of IEC 61850 Based Substation Protection Systems. *IEEE Trans. Smart Grid* **2014**, *5*, 2194–2202. https://doi.org/10.1109/TSG.2014.2314616.
19. Li, C.; Qing, G.; Li, P.; Yin, T. Operational Risk Assessment of Distribution Network Equipment Based on Rough Set and D-S Evidence Theory. *J. Appl. Math.* **2013**, *2013*, 263905. https://doi.org/10.1155/2013/263905.
20. Mabunda, N.; Bokoro, P.; Nicolae, D. Statistical analysis of operating times of high voltage SF6 circuit breakers. In Proceedings of the 2016 IEEE 16th International Conference on Environment & Electrical Engineering, Florence, Italy, 7–10 June 2016. https://doi.org/10.1109/EEEIC.2016.7555528.
21. Meyur, R. A Bayesian Attack Tree Based Approach to Assess Cyber-Physical Security of Power System. In Proceedings of the 2020 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 6–7 February 2020; pp. 1–6. https://doi.org/10.1109/TPEC48276.2020.9042529.
22. Obychaiko, D.S.; Shikhin, V.A.; Chrysostomou, G. Reliability Analysis of Cyber-Physical Systems. In Proceedings of the 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Moscow, Russia, 15–18 May 2018; pp. 1–6. https://doi.org/10.1109/ICIEAM.2018.8728609.

23. Oyewole, P.A.; Jayaweera, D. Power System Security with Cyber-Physical Power System Operation. *IEEE Access* **2020**, *8*, 179970–179982. https://doi.org/10.1109/ACCESS.2020.3028222.
24. Peng, R. Reliability of Interdependent Networks with Cascading Failures. *Eksploat. Niezawodn. Maint. Reliab.* **2018**, *20*, 273–277. https://doi.org/10.1109/TR.2016.2606125.
25. Sahu, A.; Davis, K. Structural Learning Techniques for Bayesian Attack Graphs in Cyber Physical Power Systems. In Proceedings of the 2021 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2–5 February 2021; pp. 1–6. https://doi.org/10.1109/TPEC51183.2021.9384933.
26. Shi, X.; Li, Y.; Cao, Y.; Tan, Y. Cyber-physical electrical energy systems: Challenges and issues. *CSEE J. Power Energy Syst.* **2015**, *1*, 36–42. https://doi.org/10.17775/CSEEJPES.2015.00017.
27. Da Silva, A.M.L.; Violin, A.; Ferreira, C.; Machado, Z.S. Probabilistic Evaluation of Substation Criticality Based on Static and Dynamic System Performances. *IEEE Trans. Power Syst.* **2014**, *29*, 1410–1418. https://doi.org/10.1109/TPWRS.2013.2293626.
28. Soltan, S.; Mittal, P.; Poor, H.V. Line Failure Detection After a Cyber-Physical Attack on the Grid Using Bayesian Regression. *IEEE Trans. Power Syst.* **2019**, *34*, 3758–3768. https://doi.org/10.1109/TPWRS.2019.2910396.
29. Soltan, S.; Yannakakis, M.; Zussman, G. React to Cyber Attacks on Power Grids. *IEEE Trans. Netw. Sci. Eng.* **2019**, *6*, 459–473. https://doi.org/10.1109/TNSE.2018.2837894.
30. Sundararajan, A.; Khan, T.; Moghadasi, A.; Sarwat, A.I. Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies. *J. Mod. Power Syst. Clean Energy* **2019**, *7*, 449–467. https://doi.org/10.1007/s40565-018-0473-6.
31. Wisniewski, R. Design of Petri Net-Based Cyber-Physical Systems Oriented on the Implementation in Field Programmable Gate Arrays. *Energies* **2021**, *14*, 7054. https://doi.org/10.3390/en14217054.
32. Yin, X.; Li, L.; Liu, Q. A Study on the Vulnerability Cascade Propagation of Integrated Energy Systems in the Transportation Industry Based on the Petri Network. *Energies* **2022**, *15*, 4320. https://doi.org/10.3390/en15124320.
33. Gong, L.; Ma, R.; Yang, H.J.; He, Y. The substation fault diagnosis method based on the time constraint probability Petri net. In Proceedings of the 2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), Changsha, China, 26–29 November 2015; pp. 1142–1146. https://doi.org/10.1109/DRPT.2015.7432404.
34. Vellaithurai, C.; Srivastava, A.; Zonouz, S.; Berthier, R. CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures. *IEEE Trans. Smart Grid* **2015**, *6*, 566–575. https://doi.org/10.1109/TSG.2014.2372315.
35. Wang, H.; Chen, Z.; Zhao, J.; Di, X.; Liu, D. A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow. *IEEE Access* **2018**, *6*, 8599–8609. https://doi.org/10.1109/ACCESS.2018.2805690.
36. Wang, L.; Qu, Z.; Li, Y.; Hu, K.; Sun, J.; Xue, K.; Cui, M. Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal–Topological Correlation. *IEEE Access* **2020**, *8*, 57260–57272. https://doi.org/10.1109/ACCESS.2020.2982057.
37. Xiang, Y.; Wang, L.; Liu, N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electr. Power Syst. Res.* **2017**, *149*, 156–168. https://doi.org/10.1016/j.epsr.2017.04.023.
38. Yang, J.; Guo, Y.; Guo, C.; Chen, Z.; Wang, S. Cross-Space Risk Assessment of Cyber-Physical Distribution System Under Integrated Attack. *IEEE Access* **2021**, *9*, 149859–149869. https://doi.org/10.1109/ACCESS.2021.3101896.
39. Zhao, D.; Wang, Y.; Song, Y. Petri Net Based Intelligent Substation Fault Diagnosis. In Proceedings of the 2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2), Changsha, China, 8–10 November 2019; pp. 794–799. https://doi.org/10.1109/EI247390.2019.9062127.
40. Zeng, Z.G.; Zio, E. Dynamic Risk Assessment Based on Statistical Failure Data and Condition-Monitoring Degradation Data. *IEEE Trans. Reliab.* **2018**, *67*, 609–622. https://doi.org/10.1109/TR.2017.2778804.
41. Hao, S.; Zhang, J.; Liu, S.; Wang, D.; Huang, C. Power equipment reliability evaluation based on data mining. In Proceedings of the 2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), Changsha, China, 26–29 November 2015; pp. 699–703. https://doi.org/10.1109/DRPT.2015.7432325.
42. Zhang, Y.; Wang, L.; Sun, W. Trust System Design Optimization in Smart Grid Network Infrastructure. *IEEE Trans. Smart Grid* **2013**, *4*, 184–195. https://doi.org/10.1109/TSG.2012.2224390.
43. Zhao-Yang, Q.; Ya-Ying, L.; Peng, L. A network security situation evaluation method based on D-S evidence theory. In Proceedings of the 2010 The 2nd Conference on Environmental Science and Information Application Technology, Wuhan, China, 17–18 July 2010; pp. 496–499. https://doi.org/10.1109/ESIAT.2010.5567380.
44. Zhao, Y.; Huang, L.; Smidts, C.; Zhu, Q. Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants. *Reliab. Eng. Syst. Saf.* **2020**, *201*, 106878. https://doi.org/10.1016/j.ress.2020.106878.
45. Zhou, X.; Yang, Z.; Ni, M.; Lin, H.; Li, M.; Tang Y. Analysis of the Impact of Combined Information-Physical-Failure on Distribution Network CPS. *IEEE Access* **2020**, *8*, 44140–44152. https://doi.org/10.1109/ACCESS.2020.2978113.
46. Lee, J.C.; McCormick, N.J. Appendix C: Some Failure Rate Data. In *Risk and Safety Analysis of Nuclear Systems*; John Wiley & Sons: Hoboken, NJ, USA, 2011. https://doi.org/10.1002/9781118043462.app3.
47. Hajian-Hoseinabadi, H. Reliability and component importance analysis of substation automation systems. *Int. J. Electr. Power Energy Syst.* **2013**, *49*, 455–463. https://doi.org/https://doi.org/10.1016/j.ijepes.2010.06.012.