A security Assessment of Distribution Network CPS Based on Association Matrix Modeling Analysis

Zhou Yang¹, Xia Zhou¹, Ming Ni², Manli Li³, Husheng Lin¹

¹Nanjing University of Posts and Telecommunications, Nanjing 210023, China
²NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China

yang_zhou0207@163.com

Abstract. The addition of the information system has improved the operation of the distribution network CPS, but it also brings certain risks and impacts to the safety of the distribution network CPS operation. Therefore, the distribution network CPS security assessment needs to consider the impact of information systems. This paper proposes a security Assessment of Distribution Network CPS Based on Association Matrix Modeling Analysis. The research framework of information physical fault impact is proposed, and the correlation and impact of information physical failures are analyzed. The CPS model of distribution network based on association matrix is established, and the safety evaluation index and evaluation method are proposed. Case study shows the rationality and effectiveness of the proposed method.

1. Introduction
With the advancement of smart grid and energy Internet strategies, the high coupling of information and physics has become a key feature of smart distribution networks [1]. The addition of information systems brings convenience to information collection, information transmission and optimization control. At the same time, it also increases the security risk of distribution network CPS, which leads to an increased possibility of attack on CPS of distribution network [2]. The physical coupling mechanism leads to cascading failures, causing the entire distribution network CPS to even threaten the safe operation of the large power grid. In the distribution network CPS, the degree of influence of information on the physical system depends mainly on the role of information functions in power grid fault handling and recovery [3]. When the physical system fails, the simultaneous failure of the information will affect the fault handling process and deteriorate the system state. If the system fails, the feeder circuit breaker control function failure will cause the cascade fault to occur [4].

At present, the research on distribution network CPS has been improved from the initial architecture, modeling [5-7], to reliability [8-10], to risk assessment [11-12], to the impact analysis of information attacks [13]. However, there is less research on the impact of research information-physical prediction failure on the safety of distribution network CPS. In the actual operation of the distribution network CPS, most of the safety problems are caused by the failure of internal functions, such as the failure of the information acquisition equipment, the rejection or misoperation of the control operation of the secondary equipment, and the interruption or extension of the transmission of the information channel. Time. The failure of the functions of these information systems will induce the formation of combined
faults in the failure of the CPS physical system of the distribution network, which will affect the recovery of the CPS faults in the distribution network and bring secondary losses to the distribution network CPS.

This paper focuses on the impact of information system failures on the security of power systems. Firstly, the basic framework of fault research on distribution network CPS is proposed. According to the physical coupling characteristics of the information, a model based on the correlation matrix is established. A method for evaluating the safety of the distribution network CPS considering the influence of information is proposed. Finally, it was verified in the example system.

2. Analysis of the impact of information physical failure

2.1. Distribution network CPS hierarchy

Modern power distribution network is a typical information physical fusion system, which is divided into three hierarchical structures: distribution network backbone layer, access layer and terminal layer. As shown in Figure 1. The main layer includes the power distribution master station system, SCADA server, etc., and uses SDH technology to connect the power distribution main station and each of the distribution stations. The access layer uses EPON technology to connect the distribution station and each distribution terminal to realize real-time communication between the distribution terminal and the distribution station. The terminal layer contains feeders, circuit breakers, segment switches, and FRTUs, etc. The framework is divided into hierarchical layers, including the information center layer, the information physical coupling layer, and the physical entity layer. As shown in Figure 2.

![Figure 1. Structure of Distribution Network](image)

![Figure 2. Framework of Hierarchical Layers](image)

2.2. Information System Failure Impact Research Framework

2.2.1. Failure correlation analysis. The correlation between information failure and physical failure is divided into direct correlation and indirect correlation. Direct correlation: The functions completed by the information system directly affect the primary equipment of the power. This type of information failure will directly cause the primary equipment to fail to work properly and cause physical failure. Indirect correlation: The functions performed by the information system do not directly affect the primary equipment of the power, but will affect its performance. At the same time as physical faults occur, the simultaneous occurrence of information faults will affect the process of fault recovery and deteriorate the system state. The impact of physical faults on information faults is primarily a direct impact. The primary device of the physical system provides power for the communication device in the information system. However, in practice, most of the CPS information systems of the distribution network have an uninterruptible power supply, so the physical failure has less impact on the information failure.
2.2.2. Analysis of Impact of Information Failure on Physical System. The impact of the communication network on the physical system is mainly reflected in the delay, error and interruption generated during the information transmission. The function of the secondary equipment network is to realize the collection and transmission of information and transmission, and on the other hand, the real-time analysis and processing of the corresponding data [14]. Its influence on the physical system mainly manifests as the effect of information processing (such as the accuracy of fault identification, the accuracy of signal acquisition) and the delays and errors generated during the information processing. Therefore, the influence of the information system on the physical system can be expressed by equation (1).

\[ F = f[R(c_i), R(s_j), R(l_j)] \]  

In the formula, \( f \) is evaluation function for the state of the distribution network power business after its execution; \( R(c_i), R(s_j), R(l_j) \) is execution results of related power services after considering the status of the communication node or link, secondary device node or channel, information node.

3. A security assessment Method for Distribution network CPS

This paper proposes a correlation method based on the correlation matrix model for the assessment of the safety of the distribution network CPS, in accordance with the "fault analysis - model establishment - indicator evaluation" approach.

3.1. Distribution Network CPS Association Matrix Modeling

Firstly, the fusion information and physical distribution network CPS system should be modeled and analyzed. The correlation matrix model can accurately describe the topological relationship (structure) and logical association (control logic) between layers [15]. The modeling process is as follows.

3.1.1. Network modelling. Take power network modeling as an example. Other networks will adopt the same method. Physical layer model \( P \): According to the distribution network topology, the logical relationship between the physical layer is represented by two logical elements of "0" and "1". For a distribution network with \( m \) power nodes, establish an \( m \)-square matrix.

\[
P = \begin{bmatrix}
p_{i1} & \cdots & p_{ij} & \cdots & p_{im} \\
\vdots & & \vdots & & \vdots \\
p_{p1} & \cdots & p_{pj} & \cdots & p_{pm} \\
\vdots & & \vdots & & \vdots \\
p_{mi} & \cdots & p_{mj} & \cdots & p_{mm}
\end{bmatrix}
\]

In the formula, \( p_{ij} \) represents the nodes and lines of the physical entity layer; When \( p_{ij} \) is equal to 0, it means no connection; When \( p_{ij} \) is equal to 1, it means that there is a connection.

3.1.2. Association modelling. The association matrix describes the relationship between the layers of the distribution network CPS. The following is an example. Secondary equipment-communication association model: For the distribution network CPS network including \( k \) secondary device nodes and \( m \) communication nodes, the secondary device node-communication node association characteristic matrix is used to describe the information uploading and delivery process. In the next formula, \( s-c_{ij} = [s-c_{T,ij}, s-c_{PB,ij}] \) is used to describe the relationship between the communication node and the secondary device node. \( s-c_{T,ij}, s-c_{PB,ij} \) represents the delay and interruption of the communication node \( i \) and the secondary device \( j \) node respectively.
3.2. Security assessment index of distribution network CPS

In the distribution network CPS, the load loss caused after the physical failure occurs may include two parts: load loss of the fault section and load loss of the non-fault section. The former is fixed, which is caused by the isolation of the fault after the fault occurs; the latter is not fixed, due to the radiation network structure of the distribution network, which causes the downlink power supply area to lose power after the fault isolation. Load loss can be recovered by grid-connected and off-grid: grid-connected recovery refers to the use of alternate tie lines for adjacent feeder load transfer; off-grid recovery refers to the use of non-faulty segments for distributed The power supply is supplied. In the CPS fault recovery process of the distribution network, the information system plays a pivotal role. If information failure occurs again, it will once again affect the safety of the distribution network CPS. Based on this, this paper proposes the post-fault loss level indicator and the resilience index as the CPS safety assessment index of the distribution network.

3.2.1. System loss degree index after failure. The post-fault loss indicator includes two parts: the degree of load loss and the degree of user loss.

The degree of load loss is the ratio between the sum of the load reduction of the fault section after the failure of the distribution network and the load reduction of the non-fault section and the total load of the distribution network.

\[
\rho_l = \frac{\sum_{i \in M} \mu_i P_i + \sum_{i \in N} \mu_i P_i}{\sum_{i \in S} \mu_i P_i}
\]

In the formula, \(\mu_i\) is level weight of the node \(i\); \(P_i\) is active power load of node \(i\); \(M, N, S\) is load node sets of the fault zone, the non-fault zone and all.

The degree of user loss is reflected in the degree of impact on the user side after the failure of the distribution network CPS, including the proportion of power outages and the proportion of user power outage losses.

\[
\rho_u = (\sigma_1 \frac{X}{Y} + \sigma_2 \sum_{j \in X} \frac{W_j}{Y})
\]

In the formula, \(\sigma_1, \sigma_2\) are the weighting factors for the proportion of power outages and the proportion of user power outage losses. \(W_j\) is the rating factor of user \(j\). \(X, Y\) are the number of all lost users and the total number of users of the system after the failure.

3.2.2. System recovery capability index after failure. The timely recovery of the distribution network after the failure of the distribution network CPS is an important basis for maintaining the safe and stable operation of the distribution network. It is mainly evaluated from the two aspects of failure recovery rate and failure recovery speed.
Failure recovery rate: The power restoration process after the CPS failure of the distribution network generally starts from the failure, and continues until the fault is completely cleared and the normal power supply of the entire network is restored. Therefore, during this period of time, the recovery of the load should be considered in consideration of the load importance level.

\[
\rho_r = \frac{\sum_{t=1}^{T} \sum_{i \in M \cup N} \sigma_i P_{i,t} \Delta t}{\sum_{t=1}^{T} \sum_{i \in M \cup N} \sigma_i L_{i,t} \Delta t}
\]

In the formula, \( P_{i,t} \) is the actual recovery power of the load \( i \); \( L_{i,t} \) is the original power demand of the load \( i \) at the moment; \( \sigma_i \) is the rank weight of the node load \( i \); \( \Delta t \) is the duration of the fault; \( M, N \) are load node sets of the fault zone and the non-fault zone.

Fault recovery speed: In order to reduce the load loss and shorten the power outage time of the user, the distribution network requires timely power restoration for the non-faulty section after the fault occurs, and quick repair of the fault section.

\[
T_f = T_1 + T_2
\]

In the formula, \( T_1, T_2 \) are fault zone positioning time and fault isolation and non-fault zone recovery time.

3.3. Security assessment method based on expected fault set

The safety of the distribution network CPS refers to any time section in the continuous operation of the system. For a set of physical or communication expected faults, it can keep the distribution network CPS system running continuously to maintain the power supply capacity to the load. This paper proposes a CPS security assessment method based on the expected fault set. The flow is shown in Figure 3.

*Figure 3. Security Assessment Process for Distribution Network Cyber Physical System*
4. Case analysis

Figure 4 is a structural diagram of the distribution network 3 feeder system and its corresponding information system. In the figure, the distribution physical system has a total of 8 distributed power supplies to support the island operation, and a communication switch between the feeder 2 and the feeder 3 is provided for load exclusive supply. In order to make the calculation convenient, the 33 load nodes are divided into 11 sections, corresponding to 11 kinds of physical expected faults, and the sections are provided with isolating switches to ensure the isolation of faulty sections and non-faulty sections.

![Figure 4. Structure of Case](image)

4.1. Result analysis

In this paper, the security of the distribution network CPS is studied under the normal and fault scenarios of the information system.

4.1.1. The information system is normal. When the information system is normal, the communication and control functions between the communication device and the secondary device and the physical node are normal, and the load, switch, and the like in the physical system of the distribution network can be monitored and controlled. On this basis, the fault prediction is carried out, and the self-regulating ability of the distribution network CPS is used for recovery, and the calculation safety index is shown in Table 1. In Table 1, after the occurrence of the failure SEC11, the load and user loss are the lowest and the failure recovery rate is the highest. This is because the load level of the section is low and the number of users is small, and the load transfer can be quickly realized through the feeder transfer. It is expected that the load and user loss will be higher after the occurrence of the fault SEC5. This is because the load of the section is more important and the fault recovery rate is lower because it can only be restored by the power supply of the island.

| Predictive fault set | Safety indicator calculation result | $T / s$ |
|----------------------|-----------------------------------|--------|
| SEC1                 | $\rho_l / \%$ | $\rho_u / \%$ | $\rho_i / \%$ |        |
| SEC1                 | 2.34     | 2.40     | 96.14     | 120    |
| SEC2                 | 7.17     | 4.79     | 88.16     | 120    |
| SEC3                 | 15.51    | 16.94    | 74.38     | 120    |
| SEC4                 | 9.24     | 11.98    | 94.92     | 40     |
| SEC5                 | 35.87    | 19.55    | 80.26     | 40     |

Table 1. Calculation Result (Normal Information System).
4.1.2. Fault information upload failure. The uploading of CPS fault information of the distribution network is mainly the two parts of the monitoring equipment collecting fault information and the communication network transmission fault information. This article addresses the expected failures occurring at SEC1, setting information to monitor for error faults. The physical expectation fault occurs between the load nodes P2-P3, but because the information monitoring equipment of the load node P3 fails, the fault information cannot be transmitted, and the monitoring information of the load node P4 is successfully transmitted, the fault section is located at SEC1 and SEC2. Therefore, the security indicators for the expected fault SEC1 in different scenarios are shown in Table 2 below.

| Fault information upload status | Safety indicator calculation result |
|-------------------------------|----------------------------------|
|                              | \( \rho_{\text{fail}} \) /% | \( \rho_{\text{rec}} \) /% | \( \rho_{\text{recomm}} \) /% | \( T \) |
| Normal                        | 2.34                            | 2.40 | 96.14 | 120s |
| Malfunction                   | 10.51                           | 4.79 | 88.16 | 120s |
| Manual positioning            | 2.34                            | 2.40 | 90.51 | 30min|

It can be seen from Table 2 that the fault location range becomes larger due to the failure of the fault information uploading. If the decision control center does not find this information fault, the non-faulty section SEC2 is also isolated, resulting in load loss and user loss increase; If this information failure is discovered in time, manual fault location will be taken, which increases the time for failure recovery.

4.1.3. Control command issued failure. The fault information is uploaded to the information center, and after the decision is made, a control command is sent to the fault isolation switch and the load transfer switch. If the interrupt is generated by the control command, the above recovery operation cannot be completed in time. When the expected fault occurs in the feeder 2 and the feeder 3, the fault occurs during the issuance of the control command, the contact switch R cannot be closed, and the load transfer failure between the feeders fails, and the non-faulty section cannot be restored in time. The safety indicators are shown in Table 3 below.

| Predictive fault set | Safety indicator calculation result |
|----------------------|----------------------------------|
|                      | \( \rho_{\text{fail}} \) /% | \( \rho_{\text{rec}} \) /% | \( \rho_{\text{recomm}} \) /% | \( T \) / s |
| SEC1                 | 2.34                            | 2.40 | 96.14 | 120s |
| SEC2                 | 7.17                            | 4.79 | 88.16 | 120s |
| SEC3                 | 15.51                           | 16.94 | 74.38 | 120s |
| SEC4                 | 9.24                            | 11.98 | 94.92 | 40s |
| SEC5                 | 35.87                           | 19.55 | 80.26 | 40s |
| SEC6                 | 12.91                           | 21.38 | 88.06 | 60min|
| SEC7                 | 10.57                           | 18.98 | 91.27 | 60min|
| SEC8                 | 7.55                            | 11.98 | 95.43 | 40s |
| SEC9                 | 2.34                            | 2.40 | 96.59 | 120s |
| SEC10                | 16.35                           | 18.98 | 81.43 | 120s |
| SEC11                | 0.47                            | 1.60 | 99.74 | 40s |
Comparing the results of Table 1 and Table 3 can be seen: Since there is no load transfer between the feeder 1 and the feeder 2/3 through the tie switch $R$, each expected fault on the feeder has no effect on various indicators. By comparing the expected fault SEC6, due to the failure of the node control device, after the expected fault occurs, the fault isolation is performed. For the downlink SEC7 and SEC8 segments, the load transfer cannot be completed in time, thus causing the non-faulty segment to be powered off, so the load and The degree of user loss is greatly affected, and the failure recovery rate is also reduced. Compared with the expected SEC9-11, the contact switch is faulty, but since the feeder can also be powered by the distributed power supply, the impact is small, but it is turned into the island power supply through the contact switch. And the speed of failure recovery has an impact.

Acknowledgments
This work is supported by National key research and development plan projects(Security analysis and assessment method of cyber physical system (CPS) for distribution network attack .2017YFB090300); State Key Laboratory of Smart Grid Protection and Operation Control(SGNR0000GZJS1808074); National Natural Science Foundation of China(Research on Cyber Physical Security Theory and Active Defense Technology for Cyber Attacks, 61833008).

References
[1] MA Zhao, ZHOU Xiaoxin, SHANG Yuwei, et al. Form and development trend of future distribution system[J]. Pro-ceedings of the CSEE, 2015, 35(6): 1289-1298.
[2] WANG Yufei, GAO Kunlun, ZHAO Ting, et al. Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph[J].Proce- dings of the CSEE, 2016, 36 (6) : 1490-1499.
[3] LIU Wenxia, GONG Qi, GUO Jing, et al. Reliability Simulation of ADN Cyber-Physical System Based on Hybrid Communication Network[J]. Proceedings of the CSEE, 2018, 38(06): 1706-1718+1907.
[4] Zhao Ting, Wang Dong, Lu Dongxu, et al. A risk assessment method for cascading failure caused by electric cyber-physical system(ECPS)[C]/Proceedings of the 2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT). Changsha, China: IEEE, 2015: 787-791.
[5] LI Peikai, CAO Yong, XIN Huanhai, et al. Discussion on Cooperative Control Architecture of Cyber-physical Distribution Network System[J]. Electric Power Automation Equipment, 2017, 37(12):2-7+15.
[6] GONG Gangjun, LUO Anqin, CHEN Zhimin, et al. Cyber Physical System of Active Distribution Network Based on Edge Computing[J]. Power System Technology, 2018,42(10):3128-3135.
[7] CHEN Bin, HUANG Jianye, ZHANG Gonglin, et al. Typical Characteristics and Joint Test Verification of Cyber Physical System in Distribution Network[J]. Electric Power Construction, 2017, 38 (05):46-51.
[8] JIANG Zhuzhen, LIU Junyong, XIANG Yue. Key Technologies for Reliability Assessment of Distribution Network Cyber Physical System[J]. Electric Power Automation Equipment, 2017, 37(12): 30-42.
[9] LIU Wenxia, GONG Qi, GUO Jing, SHAN Xiaodong, WANG Zhiqiang. Reliability Simulation of ADN Cyber-Physical System Based on Hybrid Communication Network[J]. Proceedings of the CSEE, 2018, 38(06): 1706-1718+1907.
[10] WANG Bingjia, DAN Shuheng, XIA Xin. Reliability Evaluation of Distribution Network CPS Considering EPON[J/OL]. Proceedings of the CAU-EPSA:1-7.
[11] WANG Zibo, MU Yunfei, WANG Yufei, et al. Cyber Physical System Risk Assessment of Distribution Network Considering Communication Failure of Multi-agent System for Power Restoration[J]. Automation of Electric Power Systems, 2016,40(17):51-58.
[12] AN Yu, LIU Dong, CHEN Fei, XU Weiwei. Risk Analysis of Physical Distribution Network
Operation Considering Cyber Attack[J/OL]. Power System Technology: 1-8 [2019-05-07].

[13] ZHANG Li, LIU Junyong, LIU Youbo. Static security risk assessment of power system considering wind speed correlation[J]. Electric Power Automation Equipment, 2015, 35(04):84-89.

[14] TANG Yi, LI Feng, WANG Qi, NI Ming. Quantitative evaluation of communication system fault effect on real-time load control of power system[J]. Electric Power Automation Equipment, 2017, 37(02): 90-96.

[15] XUE Yusheng, LI Manli, LUO Jianbo, et al. Modeling Method for Coupling Relations in Cyber Physical Power Systems Based on Correlation Characteristic Matrix[J]. Automation of Electric Power Systems, 2018, 42(02): 11-19.