Network Security Risk Assessment of CPS System in Distribution Network Based on Attack Graph

GONG Gangjun1, ZHANG Peng1, ZHOU Bo1, QIANG Ren1, SUN Yue2, CHEN Leran2, CHEN Wei2

1Beijing Engineering Research Center of Energy Electric Power Information Security, North China Electric Power University, 2 Beinong Street, Beijing 102206, China
2State Grid Jibei Electric Power Co. Ltd. Research Institute, North China Electric Power Research Institute Co. Ltd., Beijing 100045, China

*Corresponding author: 1182201232@ncepu.edu.cn

Abstract. With the development of advanced information and communication technology and intelligent control technology, the modern distribution network has gradually developed into a cyber-physical system of the distribution network, which also brings about the impact of information-side network security threats on the coupling failure of the physical-side power grid. In this context, a method for quantitative assessment of the network security risk of the distribution network CPS system suitable for the principle of power security protection is proposed. First of all, the physical architecture model of a typical distribution network information physical system was built; Secondly, for system network attacks, the attack path data stream related to device vulnerabilities is established, the attack behavior process is modeled based on the attack graph, and the "series-parallel model" is combined to calculate the success probability of attacking the target circuit breaker; Finally, the article takes the loss of load caused by the action of the attack circuit breaker as the physical consequence to quantify the risk value of the system and complete the network security risk assessment of the system.

1. Introduction

With the popularization and application of advanced sensor detection technology, intelligent control technology, new generation of information and communication technology and efficient data processing technology in the distribution network[1], the operation efficiency and intelligent automation level of the distribution network have greatly improved especially with the large-scale access of smart power distribution terminals, distributed power sources, and Internet of things terminal, the modern distribution network has gradually evolved into a cyber-physical system that incorporates communication networks, physical systems, control and computing systems[2]. At the same time, the degree of coupling between the power distribution system and the information system has gradually deepened, leading to the risk of network attack on the secondary information side of the power that may affect the primary power system through cross-space propagation, increasing the security operation risk of the cyber-physical system (CPS) of the distribution network[3], so it is necessary to study the quantitative assessment of the cyber-physical system network security risk of the distribution network under network attack.

At present, the research on the risk assessment of the distribution network CPS system under cyber attack is still in its infancy. Literature[4] uses the disturbance analysis idea of "information disturbance-information failure consequence form-grid fault form" to study the influence of different
types of information disturbance on the reliability of the distribution network; Literature[5] proposed a risk propagation mechanism for distribution network information space and physical space under information attack, and quantitatively evaluated the security operation risk of distribution network under information attack scenario. However, the above literature lacks modeling of the process of cyber attacks. Based on this, the literature[6] proposed a network attack behavior analysis model suitable for electronic distribution stations, and completed the quantitative assessment of the risk of the distribution network according to the consequences of the network attack; Literature[7] analyzed the behavior process of network false data attacking the distribution system and the security risks caused by it based on Bayesian graph theory. But in fact, because the current power CPS system strictly follows the principle of "safe partition" isolation of different business systems, it is difficult for the intelligent substation automation system to cross the horizontal boundary and affect the power distribution system after being attacked by the network, leading to security risks.

Therefore, this paper proposes a risk assessment method that considers the actual topological business structure of the distribution network CPS system. This article first establishes a distribution network CPS architecture model considering the safety protection principles of power monitoring systems; Secondly, it analyzes the potential information security risks of the system, and uses the circuit breaker as the target of network attacks to study the data flow path of potential attacks related to equipment vulnerabilities; Finally, the attack graph model is used to complete the analysis and modeling of the attack path and the calculation of the success probability of the attack, and establish the physical consequence index caused by the action of the circuit breaker to quantify the risk value of the system.

2. Cyber-physical system architecture of distribution network

At present, in accordance with the 16-character safety principle of "Safety Partitioning, Network Dedicated, Horizontal Isolation, and Vertical Authentication" in the "Power Monitoring System Security Protection Regulations" [8], the hierarchical structure model of the cyber-physical system of the distribution network under the principle of security protection is shown in Figure 1, which is divided into three levels: backbone layer, access layer, and physical layer.

The backbone layer includes the power distribution master station system and the optical fiber backbone communication network composed of optical fiber synchronous digital system (SDH) technology.

The power distribution access layer consists of a substation system and a communication access network. The substation system is divided into monitoring function substation and communication convergence substation, which completes the summary upload of the terminal collected data information and the distributed distribution of control instruction information from the master station, which is composed of computers, switches and other equipment; Wired communication access network. This article mainly considers the wired optical fiber private network composed of mainstream passive optical network (EPON) technology. The physical layer of the distribution network includes traditional power primary equipment and power distribution terminals. The primary equipment is composed of circuit breakers, section switches, and power distribution lines; The power distribution terminal is responsible for completing the functions of "remote measurement, remote signaling, remote control" three remotes or "remote measurement, remote signaling" two remotes, and realizes the upload of collected data and the control of switching actions. And when the terminal equipment uses the wireless public network for data communication, it is directly connected to the master station system after passing through the secure access area.
3. Security analysis of network attacks on distribution network cyber-physical systems

3.1. Security Risks of CPS System in Distribution Network

Under the conditions of network security protection of the existing distribution network CPS system, the master station system strictly follows the "sixteen-character" security policy to achieve physical isolation and closed operation. It is difficult for network attackers to illegally access the management information area through the external network and further bypass the forward and reverse isolation device to penetrate into the production control area, so as to affect the production operation of the distribution network and optimize dispatch control. At the same time, because electronic distribution stations are usually placed inside unsupervised substations or large switching stations [9], external physical isolation measures are relatively complete, and the cost of attack is relatively high, cyber attackers seldom choose it as an attack entry point.

With the intelligent development of the distribution network CPS system, a single master station of the distribution automation system may communicate with thousands of terminals at the same time. The vast majority of terminals are usually deployed outdoors, geographically dispersed, poor physical protection measures, and the risk of weak passwords. They are easily accessed illegally and become
the first choice for network attacks. And once the terminal is illegally accessed, experienced network attackers will use loopholes or take other measures to bypass firewalls and isolation devices, and through multi-level network attacks, gain control of the main station, front-end computer and other equipment, obtain the remote control authority of all power distribution switches or tamper with the information collected by the power distribution terminal and the position and status of the switches. It may cause the distribution network dispatching operation data to be disordered, and in severe cases, cause long-term power outages for important users of the distribution network, and large-scale power outages in the distribution network.

3.2. Data Flow Analysis of Attack Path of CPS System in Distribution Network

In order to maximize their own benefits and have the most serious impact on the distribution network under the condition of limited attack resources, network attackers often choose key power equipment in the distribution network as the ultimate target of the attack. Circuit breaker is an important control device of the distribution network. Once an attack causes its abnormal action, it will seriously affect the operation of the system. Therefore, this article aims to obtain "circuit breaker action authority" as the target of attack, and constructs a multi-level network attack data flow model based on the security vulnerabilities of CPS equipment in the distribution network, as shown in Figure 2 below.

![Figure 2. Attack path data flow analysis diagram.](image)

From the perspective of an attacker, the possible attack paths that exist are mainly divided into three categories. Among them, paths ① and ② penetrate through wired channels, and path ③ penetrates through wireless channels. They are:

(1) Attackers access the power distribution terminal unit through physical damage, brute force cracking authentication, etc., and use the terminal to allow port scanning vulnerabilities to scan the topology of the entire power distribution network CPS network, after obtaining the topology of the entire network, they use existing experience and knowledge to launch network attacks on the set targets; and illegally tamper with the super management password of the ONU device, and change the routing mode to bridge mode to access the Internet; Then they use the vulnerability of allowing remote login access to gain control of the OLT equipment of the sub-station, and inject PHP code into the front-end processor of the main station to achieve permission elevation; In the end, the attackers uploaded an extensible file, such as an exe file, to execute arbitrary codes on the central server of the power distribution master station, causing the circuit breaker of the distribution network to malfunction.

(2) With reference to path (1), after the attackers obtain the control right of the OLT device of the monitoring function slave station, they can obtain the control server's authority to execute arbitrary code by causing the trigger stack overflow of the slave station control server. Furthermore, the attackers maliciously tampered with the command information issued by the master station, causing the circuit breaker to malfunction.

(3) With reference to path (1), after the attackers illegally access the terminal, they use the injection vulnerability in the VPN gateway interface of the wireless terminal, and use this vulnerability by constructing special parameters to complete the privilege elevation; Then they use untrusted cookies in
openSSH to increase the authority of the public network front-end processor. Refer to path (1) to achieve the purpose of the attack.

Therefore, after a network attacker purposely exploits the different vulnerabilities of different devices, he can obtain the operation authority of the circuit breaker of the distribution network CPS system, and cause the target circuit breaker to malfunction by issuing wrong operation instructions. Under normal operating conditions of the distribution network, important users of the distribution network will be cut off, and when the distribution network fails, cascading failures may occur, resulting in a large-scale blackout. The forms and consequences of exploiting vulnerabilities in different devices are shown in Table 1.

Table 1. Device vulnerability detailed information table

| Device                        | Vulnerability name and serial number | Use form                  | Consequence                      |
|-------------------------------|--------------------------------------|---------------------------|----------------------------------|
| Power distribution terminal   | Allow port scanning CVE-2005-0315    | Port scan                | Network topology information leakage |
| ONU equipment                 | Weak password risk CVE-2007-5460     | Brute force              | Routing mode change              |
| OLT equipment                 | Allow remote login access control CVE-2017-5521 | Default open port access | Privilege escalation             |
| Wireless terminal             | The VPN gateway has an injection vulnerability CVE-2013-4984 | Special parameter construction | Privilege escalation             |
| Public network front-end processor | The operating system uses the OpenSSH protocol CVE-2007-4752 | Use of untrusted cookies | Privilege escalation             |
| Monitoring substation server  | Allow remote execution of arbitrary code CVE-2009-0241 | Trigger stack overflow | Arbitrary code execution permission acquisition |
| Configuration workstation      | Allow remote execution of arbitrary code CVE-2013-4465 | Upload of expandable files, such as .exe files | Arbitrary code execution permission acquisition |

4. Quantitative assessment of information security risk of cyber-physical system in distribution network

This paper draws on the risk assessment calculation model in the field of information security\cite{10}, and proposes the average power loss load value (\(E_r\)) as the security assessment risk value. The calculation formula is:

\[
E_r = C^{m(i)}_{total} \cdot P_{total}
\]  \(1\)

Among them, \(P_{total}\) is the probability value of successfully attacking the target, and \(C^{m(i)}_{total}\) is the physical consequence caused by the successful attack of the target node.

4.1. Probability calculation based on attack graph

The attack graph can characterize the attack path implemented by the attacker to complete the successful attack on the target. The vulnerability assessment of the system is completed by calculating the probability of successful attack under different paths\cite{11}. In this paper, the device is used as the state node of the attack graph. The directed edges between the devices represent an attack process,
and the directed edges use the related vulnerabilities of the device to complete the attack process infiltration.

The attack graph can be defined as $AG = (S, E, S_{\text{start}}, S_{\text{goal}}, R, P)$, where $S$ represents the set of attribute state nodes; $E$ represents the set of directed edges; $S_{\text{start}}$ represents the set of attack start state nodes; $S_{\text{goal}}$ represents the set of attack target nodes; $P$ is the set of success probability of form step attack, $P_i$ is the transition probability of state node $S_i$ to $S_{i+1}$; $R$ is the set of connection modes of the attack graph, including three types: series, parallel, and series-parallel composite, as shown in Figure 3 below.

Figure 3. Attack graph connection method.

(1) Series model
The total probability of a successful attack of the tandem structure is:

$$P_{\text{series}} = \prod_{i=1}^{n} P_i \hspace{1cm} (2)$$

(2) Parallel structure
The total probability of successful attack of the parallel structure is

$$P_{\text{parallel}} = 1 - \prod_{i=1}^{n} (1 - P_i) \hspace{1cm} (3)$$

(3) Series-parallel composite structure
The total number of attack paths traversing from the initial state node to the target state node is $m$, and each attack path is processed in a series structure. Assuming that the total probability of the attack path $i$ is $P_i$, the total probability of the series-parallel composite structure is:

$$P_{\text{parallel-series}} = \sum_{i=1}^{m} P_i \hspace{1cm} (4)$$

4.1.1. Calculation of attack entry probability. Power distribution terminals such as FTU, DTU, RTU, etc., are often chosen as attack portals for network attackers. Due to their different geographical environments and different functions, their physical protection measures are different, and the probability of being selected as an attack entry (physical access) by a network attacker is also different. According to actual research, under the same conditions, this article assumes that the physical protection of the "three remote" terminal equipment is better than the "two remote" terminal, DTU physical protection is better than TTU, and TTU physical protection is better than FTU. This article refers to the level assignment principle to assign the probability of attack entry selection, as shown in the following table 2-3:

| Probability assignment $P_{\text{equip}}$ | Description                                      |
|-----------------------------------------|-------------------------------------------------|
| 0.2                                     | The terminal is a "three remote" functional device |
| 0.8                                     | The terminal is a "two remote" functional equipment |
Table 3. Probability assignment of different terminal equipment.

| Probability assignment $P_{import}$ | Description       |
|--------------------------------------|-------------------|
| 0.2                                  | Terminal is DTU   |
| 0.3                                  | Terminal is TTU   |
| 0.5                                  | Terminal is FTU   |

Then the probability value $P_{import}^{total}$ of the terminal being used as the attack entry is:

$$P_{import}^{total} = P_{import}^{1} \cdot P_{import}^{2}$$

(5)

4.1.2. Calculation of success probability of state node vulnerability attack. A cyber attack is a process of offensive and defensive confrontation. The success of an attacker's single-step attack is not only related to the inherent characteristics of the state node vulnerability itself, but also closely related to the degree of ability the attacker has mastered. Then the probability that the vulnerability $i$ of the state node $S_i$ is successfully attacked is:

$$P_i = P_i^1 \cdot P_i^2$$

(6)

Among them, $P_i^1$ is the exploitability probability of the vulnerability, which characterizes how difficult the vulnerability itself is to be exploited. Refer to the Common Vulnerability Scoring System (CVSS)$^{[12]}$ to evaluate the probability of exploiting the vulnerability. The calculation formula is:

$$P_i^1 = AV_i \cdot w_1 + AC_i \cdot w_2 + AU_i \cdot w_3 + RL_i \cdot w_4 + EX_i \cdot w_5$$

(7)

$AV_i$, $AC_i$, and $AU_i$ are the index assignments of the access vector, access complexity, and authentication times of the base attribute group in the CVSS of the vulnerability of the state node, which respectively represent the static score of the vulnerability score; $RL_i$ is the index assignment of the patch repair degree of the temporal attribute group in the CVSS of the vulnerability $i$ of the state node $S_i$, and $EX_i$ is the time exposure degree of the vulnerability $i$, which respectively represents the dynamic score value of the vulnerability in the time dimension; $w_1$ - $w_5$ is the corresponding weight value. $EX_i$ can be calculated using the Pareto distribution, as in the following formula (7), $\alpha$ and $\beta$ are the Pareto distribution parameters, and $t_i$ is the release time of the vulnerability $i$:

$$EX_i = 1 - \left( \frac{\beta}{t_i} \right)^\alpha$$

(8)

$P_i^2$ characterizes the attacker’s ability to exploit the vulnerabilities of the target node. The calculation formula is:

$$P_i^2 = k \cdot \frac{1}{N_i \cdot 1 + e^{-\log_2(0.04(M_i+1)-5)}}$$

(9)

Among them, $k$ reflects the degree of knowledge the attacker has, and $k \in [0,1]$; $N_i$ is the total number of vulnerabilities in the state node $S_i$; $M_i$ is the number of times the attacker attacks the vulnerability $i$ of the state node $S_i$.

4.1.3. Calculation of attack success probability of attack target. In order to successfully attack the target node, by traversing each path in the attack graph, the total number of possible attack paths is obtained, and the series-parallel composite structure model is used for probability calculation to obtain the probability value of successfully attacking the target.

$$P_{total} = \sum_n \left( P_{import}^{total} \prod_{i=1}^n P_i \right)$$

(10)
Among them, \( n \) is the number of state nodes traversed under different path conditions.

### 4.2 Calculation of the consequences of cyber attacks

Cyber attackers influence the action of feeder circuit breakers, thereby causing power outages within a certain range, and even expanding the scope of power outages. This article considers the loss load caused by the circuit breaker to the power system from the two aspects of malfunction and refusal as the consequence index\(^{[13]}\), specifically:

\[
C_{\text{hi}}(i) = \sum_{n \in f[h(i)]} \alpha_n L_n
\]  

(11)

Among them, \( C_{\text{hi}}(i) \) is the total power loss load on the feeder terminal \( i \) considering the user level factor \( \alpha_i \); \( \alpha_n \) is the user level factor of user \( n \); \( L_n \) is the load of user \( n \); \( h(i) \) is the section where the fault occurs; \( f[h(i)] \) is the set of power load units that have failed on feeder \( i \).

The following figure 4 is an example to illustrate the physical consequences caused by the malfunction and refusal of the circuit breaker.

![Figure 4. Analysis diagram of circuit breaker action consequences.](image)

1) When the feeder is operating normally and the circuit breaker \( G_1 \) is disconnected by mistake, the feeder section 1-3 will lose power, and the load loss will be:

\[
C_{1} = \sum_{i=1}^{3} \left( \sum_{n \in f[h(i)]} \alpha_n L_n \right)
\]

(12)

Among them, \( C_1 \) is the total load loss caused by the malfunction of the circuit breaker.

2) When a fault occurs in the feeder section \( j(j \in \{1, 3\}) \), the distribution network adopts the fault handling method to locate and isolate the fault successfully, and the attack causes the circuit breaker \( G_i \) to refuse to operate, causing part of the feeder section to lose power. The load loss is:

\[
C_{2} = \theta \sum_{i=1}^{3} \left( \sum_{n \in f[h(i)]} \alpha_n L_n \right)
\]

(13)

\[
\theta = \begin{cases} 
0, & j = 1 \\
1, & j \neq 1 
\end{cases}
\]

(14)

Among them, \( C_2 \) is the total load loss caused by the circuit breaker’s refusal action; \( \theta \) is the parameter. In summary, the physical consequences of attacking breaker \( G_i \) are:

\[
C_{\text{total}} = C_{1} + C_{2}
\]

(15)

### 5. Conclusion

The quantitative assessment of the risk of the distribution network CPS system under the network attack scenario is the basis for guiding the future system construction of the network defense system. Therefore, this article establishes a distribution network CPS architecture model that follows the national level protection principle, using the distribution terminal as the entrance to the network attack, and the distribution network circuit breaker as the target of the attacking; According to the attack graph theory, this article analyzes the potential attack data flow path from the wired communication channel and wireless communication channel and calculate the probability of successful attack; Then
combined with the loss of load caused by attacking the circuit breaker of the system as a physical consequence, the risk quantitative assessment of the system is completed.

Acknowledgment
We would like to express our sincere gratitude to everyone who helped in this research work. This project is supported by the Science and Technology Project of State Grid Jibei Electric Power Co. Ltd. (52018K190024).

References
[1] Liu Wenxia, Gong Qi, Han Hui, Wang Zhiqiang and Wang Lingfeng 2018 IEEE Transactions on Power Systems. 7096-108
[2] Liang Ying, Wang Yaokun and Liu Kejian 2019 Power System Technology. 8
[3] Fu Rong, Huang Xiaojuan and Xue Yusheng 2019 Institute of Electrical and Electronics Engineers Access. 75616-628
[4] Chen Biyun, Lu Zhi and Li Bin 2019 Automation of Electric Power Systems. 103-13
[5] An Yu, Liu Dong and Chen Fei 2019 Power System Technology. 2345-52
[6] Zhang Yuhang, Ni Ming and Sun Yonghui 2019 Automation of Electric Power Systems. 12-30
[7] Huang Xiaojuan, Fu Rong and Wu Yingjun 2019 Electric Power Construction. 86-95
[8] Wang Shengfei, Hu Hua and Zhao Wenjie 2019 Electrical Engineering Technology. 47-49
[9] Han Guozheng and Xu Bingyin Automation of Electric Power Systems. 57-60, 69
[10] A. Alwi and K. A. Zainol Ariffin 2018 2018 Cyber Resilience Conference (CRC). 1-4
[11] Zou Zhenwan, Wang Di, Yang Huiting 2018 Electronic and Automation Control Conference (IAEAC). 2420-23
[12] Zhang Hua, Lou Fang, Fu Yunsheng and Tian Zhihong 2017 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen. 238-241
[13] Chen Biyun, Dai Qiaoling and Ccui Zhiwei 2017 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2). 1-4