https://doi.org/10.1051/e3sconf/202124802055

Research on risk assessment method of distribution network based on information physical fusion

Wei Wei Xu [1,2,*], Feng Chen [2], Bao Zhang[2], Jun Hao Huang[1], and Tao Yang[2]

[1] Hangzhou E. Energy Technology Co., Ltd., Hangzhou 310000, China
[2] State Grid Zhejiang Electric Power Research Institute, Hangzhou 310000, China

Abstract. With the improvement of information level, the information attack will cross the boundary of power grid information space and cause the disturbance of power grid physical system, which will form a cross-space chain fault and affect the safe operation of power grid. Based on this, this paper proposes a distribution network node risk assessment method based on information physical fusion. Firstly, the overall structure of the distribution network and the information physical coupling characteristics of the information physical fusion are studied. Then, the cross-space chain failure scenario of distribution network with information physical fusion is analyzed. Based on this, the risk assessment method is proposed. Finally, the effectiveness of the method is verified by a numerical example.

1 Introduction

In recent years, with the development of information technology, the interaction between information layer and physical layer in Cyber-Physical System (CPS) is more and more frequent. Indirect destruction of power physical system by information attackers by attacking power information system will become a common means of power network attackers. An information attack could cause cascading failures throughout the power grid, eventually leading to catastrophic blackouts. Therefore, it is of great significance to evaluate the security risk of distribution network with physical information fusion due to information attack. In the early studies, some scholars tried to establish the correlation between information attack and power system failure. Literature [1] discussed the hazards of delay, interruption, error code, jitter and other factors in power communication network to the operation of power system. In a recent study, more and more scholars begin to pay close attention to the dangers of cascading failure assessment across space, such as the literature [2-3] USES improved attack graph, complex networks, such as game theory method to measure the cascading failure across space the harm to power system operation, literature [4] put forward based on improved physical attack graph of power information system cascading failure risk assessment across space, literature [5] put forward information energy system, a comprehensive safety assessment of literature [6] proposed large-scale controllable load is malicious control scenario risk analysis of the distribution network. But the above research results still exist the following limitations: attack, only to static analysis method to establish the information of electric power secondary fault, parts of power between a disturbance events such as the causal logic.

In order to reveal the dynamic evolution process and impact of cross-space chain faults taking into account information attacks, and to quantitatively evaluate their harmfulness, a distribution network node risk assessment method based on information physical fusion is proposed. Firstly, the overall structure of distribution network and the coupling characteristics of information physics are studied. Furthermore, the cross-space chain failure scenarios of distribution network with information physical fusion are analyzed. On this basis, the risk assessment method of distribution network nodes based on information physical fusion is proposed. Finally, the effectiveness of the method is verified by a numerical example.

2 Cross-space chain fault analysis of distribution network based on information physical fusion

Different from the traditional power system faults, the cross-space chain faults involving information attacks originate from the power grid information space and develop and evolve within the CPS according to the attacker's intention, and their harm involves the power grid information space and the power grid physical system. Therefore, it is necessary to fully consider the attacker factor and explore the fault root in the information space to analyze the evolution process of this kind of fault.

Phase 1, the information the attackers choose target and set the expected consequences, through information scanning and detection technology, such as network topology scanning, packet intercepted and parsing, etc.) to

[*] Corresponding author: zhoudan@zjut.edu.cn

learn the identity of the target information system in marking and business functions such as information, try to infer information systems business functions and the communication network topology.

Phase 2, the use of information risk, vulnerability and vulnerability factors such as information, information system and control the whole/part of communication network and the target of system operating history data, try on the basis of information system and electric power secondary equipment business functions to deduce the identity of the electric power secondary equipment marking and business functions, implementation of target information space limited substantial control. If the starting point of the attack is the network in which the information system and the power secondary equipment coexist, such as the station control layer network in the smart substation, then the identity identification, service function and network topology of the information system and the power secondary equipment can be directly inferred in the first stage.

Stage 3, information attack caused part of the power secondary fault, on the basis of business knowledge and exploratory operation that electric power secondary equipment and power a device connection relationship, combined with a known power grid topology based target limited information - physical topology and the business logic function connection, and then on the basis of the information against part of the real-time system operation data obtained to estimate target local system running status, grasp necessary to trigger a cascading failure across space resources, realize the target of considerable limited local controllable, perhaps even with the help of social engineering and multiple data acquisition and monitoring control system, the wide-area monitoring system, The real-time data and data correlation of devices/systems such as synchronous phasor measurement units infer the global system status of the attack target.

In the fourth stage, the partial power secondary fault causes the partial power primary disturbance to form the power system N-1 fault. For example, malicious control of a large number of controllable loads causes load side failure due to collective abnormal start. If the above single fault fails to reach the expected target, several other such faults can be triggered and the space-time cooperative attack against the attack target can be formed to achieve the expected attack consequences.

3 Risk assessment of distribution network based on information physical fusion

3.1 Risk assessment method of information nodes

Based on the risk assessment framework of distribution network, a complete risk assessment model of distribution network based on information physical fusion is constructed after fully considering the influencing factors of information network attack. Under the threat of information network attack, the risk assessment method of distribution network based on information physical fusion is shown in Equation (1) :

$$R = P^A P^D L \qquad (1)$$

Among them, P^A is the probability of success of network attack; P^D is the probability of failure of the component under attack; L is the actual loss caused by component failure; R is the risk of distribution network system with information physical fusion; This method is used for risk assessment of distribution network system with information physical fusion.

3.2 Probability of success of intrusion information node

Division according to the safety of the electric power communication network, information of electronic security boundary nodes (electronic security perimeter (ESP)) breakthrough said information node has been a successful invasion. Assume that for every information attack, the ESP defense device has two states of success and failure.

Among them, ESP is the electronic security boundary, S_i represents the status of the ESP defense device of the attacked node *i*, Let q_i represent the state of the ESP defense device of the node *i* under attack , $f(q_i)$ represent the defense effect of the ESP defense device of the attacked node *i*. For the attack effect $h(x_i)$ of an information attack, x_i represents the information attack degree of node i, the state of the ESP defense device is as in (2):

$$S_i = \begin{cases} 0 & if \ \ 0 \le h(x_i) \le f(q_i) \\ 1 & if \ \ \ \ \ h(x_i) > f(q_i) \end{cases} \qquad (2)$$

The security status of the information node is related to the security status of the ESP defense device configured by the node. Only when all ESP defense devices are successfully attacked can the ESP of the information node be broken through, that is, the information node is successfully invaded.

According to the defense resources allocated by nodes, the defense equipment used and its corresponding defense effect function are determined, the defense effectiveness $f(q_i)$ of ESP defense equipment is as in (3):

$$f(q_i) = 1 - e^{-\lambda(q-\mu)} \qquad (3)$$

λ / μ -empirical coefficient, the better the function of defense equipment is , the higher the λ/μ value; q represents a resource for defense; assuming that the attack effect of information attack conforms to the uniform distribution of [0,1], calculating the probability that the effect of information attack is greater than that of equipment defense, and get p^A , as in (4):

$$P^A = 1 - f(q_i) \qquad (4)$$

https://doi.org/10.1051/e3sconf/202124802055

3.3 Probability of physical nodes being destroyed after successfully invading information nodes

Assume that defense resources are allocated only to ESP. Once the information attack breaks through the ESP defense, the information node will be successfully invaded. Because the physical equipment of the physical system node has certain anti-jamming ability, if the attacker tries to influence the physical system through the information attack, it must adopt the attack with enough damage intensity (that is, the intensity is greater than the critical damage intensity of physical security) , otherwise the information attack can not affect the physical system.

In this paper, p^D is used to express the possibility of physical system damage caused by information attack. Because the topological connection and anti-jamming ability of physical system nodes are not necessarily the same, the probability of the corresponding physical nodes being destroyed after different information nodes are successfully invaded is not necessarily the same, and can be analyzed and counted through simulation.

3.4 Actual loss caused by physical node destruction

After the successful attack of information domain node, the impact on the physical domain may be many aspects, such as active load loss, voltage/frequency deviation, etc. Active load loss is used as the evaluation standard of physical domain impact after the information domain node is successfully invaded, and the importance of different physical nodes is distinguished by comparing the difference of active load loss value of the whole system after the destruction of different physical nodes.

4 Example analysis

4.1 Risk simulation of distribution network based on information physical fusion

A co-simulation platform composed of OPNET,RTLAB and master control station is used to simulate the 22-node distribution network and its corresponding communication network. This paper analyzes the influence of DDoS attack on the security of physical power system, and calculates the risk value of network attack on each node in the system.

1)Probability of information node being successfully invaded

In this example, it is assumed that the various ESP defense devices distribute defense resources equally. According to the defense requirements of the communication system, the probability of successful intrusion of each information node is calculated through Equations (3) and (4), that is, 36%.

2) Probability of physical nodes being destroyed

In OPNET, every simulated node is attacked by DDoS, and the intensity of DDoS attack increases gradually. Test the maximum attack intensity of a DDoS attack without causing damage to the power system and record it as the critical damage intensity for physical safety. Due to the different topological connection and anti-jamming ability of each node in the physical system, the physical safety critical failure intensity of different nodes is different.

Assuming that the DDoS attack intensity conforms to the uniform distribution in the interval [0,1], the calculation formula of the failure probability of the corresponding physical node after the information node is successfully invaded can be simplified as (5):

$$p^D=1\text{-}power_p \qquad (5)$$

In this example, the physical safety critical failure strength of each node is calculated through repeated tests. The results are shown in Table 1:

TABLE 1. Security Critical Failure Strength Of Information Nodes

Node NO.	**1**	**2**	**3**	**4**	**5**	**6**
Powerp (%)	65	72	77	65	85	75
Node NO.	**7**	**8**	**9**	**10**	**11**	**12**
Powerp **(%)**	82	85	88	85	86	88
Node NO.	**13**	**14**	**15**	**16**	**17**	**18**
Powerp **(%)**	87	86	85	84	76	70
Node NO.	**19**	**20**	**21**	**22**		
Powerp **(%)**	75	88	85	82		

3) Active power loss of physical nodes

After the physical nodes are destroyed, the control platform will issue instructions to adjust the output of distributed generation and maintain the system operation. In RT-Lab, the active power loss of the system is calculated when the physical nodes are destroyed. The results are shown in Table 2:

TABLE 2. Active Power Loss Of Physical Nodes

Node NO.	**1**	**2**	**3**	**4**	**5**	**6**
L （kW）	1764	1764	1764	1884	1884	1660
Node NO.	**7**	**8**	**9**	**10**	**11**	**12**
***L* (kW)**	850	790	730	610	410	260
Node NO.	**13**	**14**	**15**	**16**	**17**	**18**
***L* (kw)**	60	750	330	120	124	124
Node NO.	**19**	**20**	**21**	**22**		
***L* (kW)**	24	60	60	60		

4) Risk value of each node

According to (3), the risk value of each node losing load under network attack is calculated. The results are shown in Table 3:

TABLE 3. The Risk Value Of Physical Nodes

Node NO.	1	**2**	**3**	**4**	**5**	**6**
***R* (kw)**	222.3	177.8	146.1	237.4	101.7	149.4
Node NO.	**7**	**8**	**9**	**10**	**11**	**12**
***R* (kw)**	55.1	42.7	31.5	32.9	20.7	11.2
Node NO.	**13**	**14**	**15**	**16**	**17**	**18**
***R* (kw)**	2.81	37.8	17.8	6.9	10.7	13.4
Node NO.	**19**	**20**	**21**	**22**		
***R* (kw)**	2.1	2.6	3.2	3.8		

Through the results, we can directly see the risk of each node losing load under network attack. In the simulation results of this example, the risk value of node 4 is the highest, because when the information node 4 is attacked, the probability of physical node being destroyed is higher, and when the physical node is destroyed, the loss value of the whole system is the largest. The load level of each node and the topological structure of physical layer and information layer are important factors affecting the information physical system. The simulation results can provide assistant decision-making for the allocation of communication security defense resources in power grid.

5 Conclusion

Information of physical fusion power distribution network in the information network under the attack of quantitative risk assessment is the foundation of the system safety protection work, this paper established the physical information fusion, the framework of the distribution network, secondly analyzes the information chain of physical fusion across space distribution network fault scenarios and its influence, on the basis of the risk assessment method is put forward. Through the calculation example, we can draw the following conclusions:

1) In the modern information system and the physical distribution network under the background of the depth of the coupling system, information the attackers may attack the key measurement based on the distribution network nodes, to influence the scheduling system for judging the current state of the physical network operation, to control the physical device issued the wrong instruction, resulting in the information in the transfer of risk to the physical space, eventually forming the faults of power distribution network system, causing unnecessary economic losses.

2) The method proposed in this paper can provide technical support for the theoretical and applied research of information physical fusion.

Reference

1. Cai Ye，Cao Yijia，Li Yong，et al. Cascading failure analysis considering interaction between power grids and communication networks[J]. IEEE Transactions on Smart Grid，2016，**7(1)**：530-538.
2. Cee man Vella ithurai，Anurag Srivastava，Saman Zonouz，et al. CPIndex：cyber-physical vulnerability assessment for power-grid infrastructures[J]. IEEE Transactions on Smart Grid，2015，**6(2)**：566-575.
3. Yang Xiang，Minh Truong. Acquisition of causal models for local distributions in Bayesian networks[J]. IEEE Transactions on Cybernetics，2014，**44(9)**：1591-1604.
4. 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]. Proceedings of CSEE，2016，**36(6)**：1490-1499.
5. Guo Qinglai，Xin Shujun，Wang Jianhui，et al. Comprehensive security assessment for a cyber physical energy system：a lesson from Ukraine’s blackout[J]. Automation of Electric Power Systems，2016，**40(5)**：145-147.
6. Wu Yibei，Li June，Chen Xiong，et al. Risk analysis of distribution network with large-scale controllable loads with attacks [J]. Automation of Electric Power Systems，2018，**42(10)**：30-37.