Research on Assessment of Cyber Attack Risk Conduction in Distributed Photovoltaic Contained Distribution System

Shenjian Qiu, Zhipeng Shao, Qigui Yao, Yu Liu, Hui Cui and Jiaxuan Fei

October 21, 2024

Research on Assessment of Cyber Attack Risk Conduction in Distributed Photovoltaic Contained Distribution System

Shenjian Qiu*
China Electric Power Research Institute.
Nanjing, China
qiushenjian@epri.sgcc.com.cn

Zhipeng Shao
China Electric Power Research Institute.
Nanjing, China
shaozhipeng@epri.sgcc.com.cn

Qigui Yao
China Electric Power Research Institute.
Nanjing, China
yaoqigui@epri.sgcc.com.cn

Yu Liu
State Grid Jiangsu Electric Power Co.,Ltd.
Yangzhou Power Supply Branch
Yangzhou,China
28555203@qq.com

Hui Cui
State Grid Jiangsu Electric Power Co.,Ltd.
Yangzhou Power Supply Branch
Yangzhou,China
cuihui_haian@163.com

Jiaxuan Fei
China Electric Power Research Institute.
Nanjing, China
feijiaxuan@epri.sgcc.com.cn

***Abstract*—Cyber attacks can threaten the stable operation of distributed PV-containing distribution systems, so this paper proposes a cyber attack risk conduction assessment method. First,typical cyber-attack paths against distributed PV-containing distribution systems are described. Second,attack risk conduction probability of different paths using Petri nets are quantified, taking into account the security protection devices on the information side of the system. Finally, the network centrality theory is considered to assess the probability of an attack penetrating a specific topological location of a PV plant station, and the results show that the cyber attack paths and physical layer device topologies are important factors affecting the probability of success of the attack .**

Keywords—cyber attack,distributed photovoltaic,distribution system,risk assessment,risk conduction,network centrality.

I. Introduction

In recent years, access to a large number of control terminals and gateway interaction units has created additional vulnerabilities in the distribution system. The risk of cyber attacks to break through the information security protection of the power distribution system to reach the physical equipment layer is intensified[1].For example, the 2015 cyber attack on the Ukrainian power system and the 2016 cyber attack on Israeli power system posed severe threats to economic development[2][3].In addition, the access of a large number of distributed energy devices will reduce the transient stability and cyber security level of the power system[4].Cyber attacks targeting grid-connected PV will threaten stable operation of distribution grids[5].Therefore, the conduction paths and conduction risks of cyber attacks in distributed PV-containing distribution systems should be emphasized and researched.

Currently, many scholars at home and abroad have carried out research on modeling cyber attacks and risk transfer for power systems.Literature [6] constructed a behavioral model of power grid security risk propagation based on Petri net under the global perspective. Literature [7] proposes a practical false data injection attack model for state estimation of power distribution systems; several risk assessment methods are proposed on the basis of relatedmodeling approaches. Some of them adopt traditional probabilistic assessment methods. For example, reference [8] introduces an attack graph-based approach to assess the cyber risk of cyber-physical power systems. The work in reference [9], uses Bayesian networks to address CPS cyber-physical risks associated with system vulnerabilities. In reference [10], the authors use stochastic game theory to model the behavior of attackers and defenders to assess cyber security risk. Literature [11] proposes an attack detection algorithm for voltage regulation in PV integrated distribution networks. In addition, emerging learning-based approaches are becoming increasingly popular. For example, literature [12] proposes a rank algorithm based on a learning approach for real-time risk assessment of power systems. Literature [13] utilizes deep reinforcement learning to find the optimal network transition strategy from the attacker's perspective and assess the impact of potential attacks.

Considering the shortcomings of existing research, this paper proposes an attack risk conduction assessment method based on Petri nets and the physical layer network topology containing distributed photovoltaic power distribution systems, and quantitatively analyzes the risk of cyber-attack conduction with different attack paths and attack targets.

II. Cyber Attack Paths Targeting Distributed Pv-Containing Distribution Systems

A. Distributed PV Distribution System Architecture

The architecture of the distributed PV-containing distribution system is shown in Fig. 1. It is divided into master control layer, communication network layer and physical distribution layer. The interaction of data and commands and network communication are accomplished by the master server and network infrastructure equipment between layers. The corresponding network equipment includes IEDs (intelligent measurement and control terminals), routers, and interactive machines. Among them, the intelligent measurement and control terminal of distributed PV can upload real-time measurement data such as light intensity, PV active output power, etc., and control

This article is funded and supported by the science and technology project of State Grid Corporation of China: “Research on Techniques of Risk Identification and Attack Suppression for Distributed Photovoltaic System under Cyber-Physical Cross-Domain Attack”(project No.5700-202318304A-1-1-ZN)

PV on and off the grid according to the control commands issued by the master station.

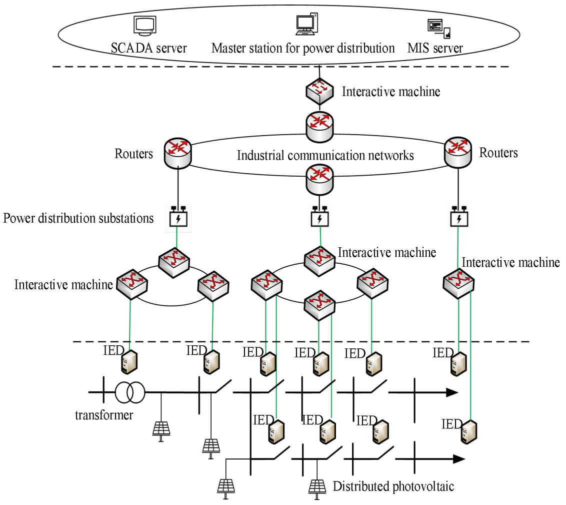

Fig.1.Distributed Photovoltaic Distribution System Architecture

Considering the impact of this business architecture as well as network security protection devices, two network attack path models targeting distributed PVs are proposed from the attacker's perspective.

B. *Modeling of Cyber Attack Paths Targeting Distributed Photovoltaics*

1) Denial-of-service Attack Path

As shown in Fig. 2, in the distributed PV distribution system, the attacker launches a denial of service attack by first attacking a router in the communication layer that interacts with the station control layer, so that it sends a large amount of useless information to the master station's pre-switching switch through the SDH/MSTP communication network, and the useless information arrives at the master station, so that its ability to deal with the business of scheduling and control of electric power resources is undermined, resulting in the blocking of communication commands, which further leads to global problems such as paralyzing the physical side PV output regulation capability and mismatching of PV consumption decisions. command blocking, which further leads to global problems such as paralyzed PV output regulation capability on the physical side and mismatch of PV consumption decisions.

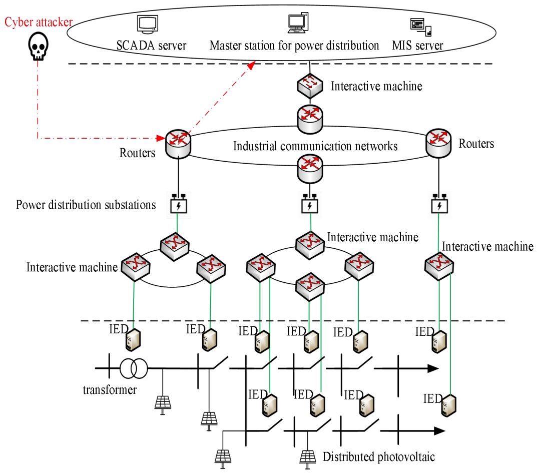

Fig.2.Denial of Service Attack Path Schematic

As shown in Fig. 3, the security protection devices in the denial-of-service attack path include intrusion prevention device detection, authentication of the access gateway at the master end, and the primary and backup firewalls.

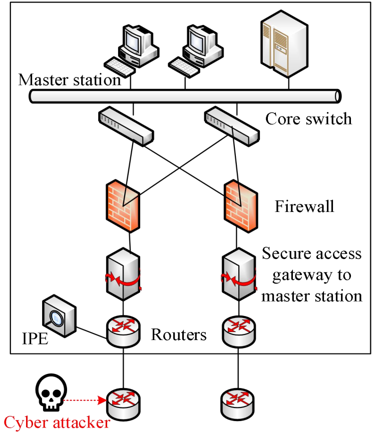

Fig.3.Denial of Service Attack Path Related Network Protection Devices

2) Data Tampering Attack Path

As shown in Fig. 4, when launching a data tampering attack on the PV, the attack initiator first steals the control instructions issued by the distribution master station to the distribution electronic station, which contain regulation and control data for the distributed PV. Subsequently, it injects the data of the attack instructions into the management interoperability machine of the attack-targeted PV array, and, finally, through the interoperability and by issuing the erroneous scheduling data to the PV scheduling unit, it change the PV output situation and cause the tidal state of the distribution system to vary.

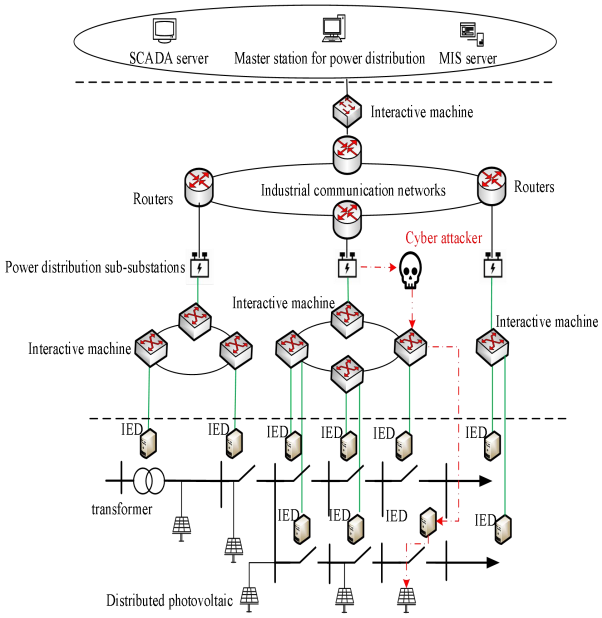

Fig.4.Data Tampering Attack Path Schematic

As shown in Fig. 5, the security protection devices in the data tampering attack path include the port management privileges of the interacting machines at each layer, the firewalls between the sub-station and terminal layers, and the security passwords of the vertical encryption devices.

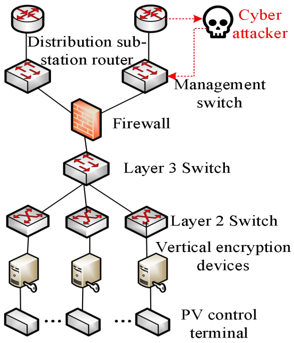

Fig.5.Data Tampering Attack Path Related Network Protection Devices

Based on the aforementioned network attack path and the network security protection equipment involved in the path, the network attack conduction process is described with the help of stochastic Petri nets to complete the probability quantification of the network attack breaking through the security protection conduction to the physical equipment layer.

III. Quantification Of Network Attack Conduction Probability Based On Stochastic Petri Nets

A. Data Tampering Attack Conduction Probability

As shown in Fig. 6, based on Petri net theory and Fig. 5, the attack path of *data tampering attack* is established.

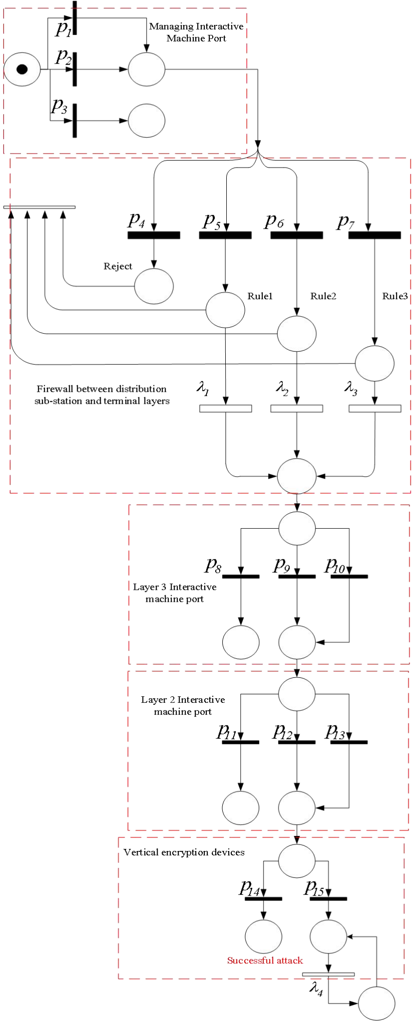
p_1
p_2
p_3
Managing Interactive Machine Port
p_4
p_5
p_6
p_7
Reject
Rule1
Rule2
Rule3
Firewall between distribution sub-station and terminal layers
λ_1
λ_2
λ_3
p_8
p_9
p_{10}
Layer 3 Interactive machine port
Layer 2 Interactive machine port
p_{11}
p_{12}
p_{13}
Vertical encryption devices
p_{14}
p_{15}
Successful attack
λ_4

Fig.6.Petri Net Model for Risk Conduction of Data Tampering Attack

The variable p_i (i=1,2,3...) and λ_i (i=1,2,3...) denote the value of the instantaneous change probability and the value of delay variation in the random Petri net respectively, which are set based on the log data of the network security protection device.

Based on the instantaneous variation and delay variation values of each security protection device under an attack event in the Petri net model of a cyber attack path, the probability of a cyber attack being transmitted to the physical side of the system can be quantified.

TABLE I. NUMBER OF CORRESPONDING EVENTS IN THE ATTACK SCENARIO

Attack scenario corresponding events	Events collected by Petri net terminals
Failure to pass management switch port	4036
Blocked by the firewall	4482
Failure to pass layer 3 Interactive machine port	164
Failure to pass layer 2 Interactive machine port	101
Blocked by vertical encryption devices	880
Successful invasion	307

As shown in TABLE I, The probability of success of the attack under 10,000 simulation experiments is 3.07%.

B. Denial of Service Attack Conduction Probability

As shown in Fig. 7, based on petri net theory and Fig. 3, the attack path of denial of service attack is established.

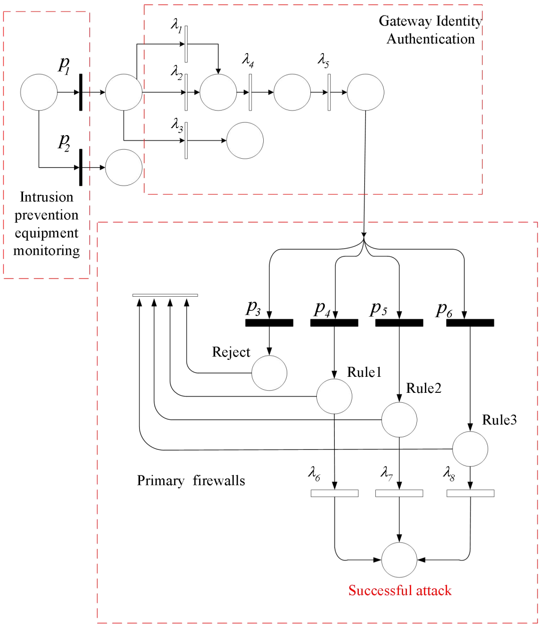

Fig.7.Petri Net Model for Risk Conduction of Denial-of-Service Attack

As shown in TABLE II,the probability of success of the attack under 10,000 simulation experiments is 1.43%.

TABLE II. NUMBER OF CORRESPONDING EVENTS IN THE ATTACK SCENARIO

Attack scenario corresponding events	Events collected by Petri net terminals
Intercepted by intrusion detection system	120
Failure to authenticate	135
Blocked by the firewall	9602
Successful invasion	143

IV. Risk Assessment Of Cyber Attack Conduction Against Photovoltaic Plant Stations

After the attack data flow is conducted to the physical device layer. From the attacker's point of view, the physical network topology location where different distributed PVs are located affects the selection of the attack object, so the network centrality evaluation index is used to describe the possibility of different PVs suffering from the attack.

The nodes topology network of the physical device layer of the distributed PV distribution system is shown in Fig.8.PV integration node numbers are 2, 8, 14, 18, 32.

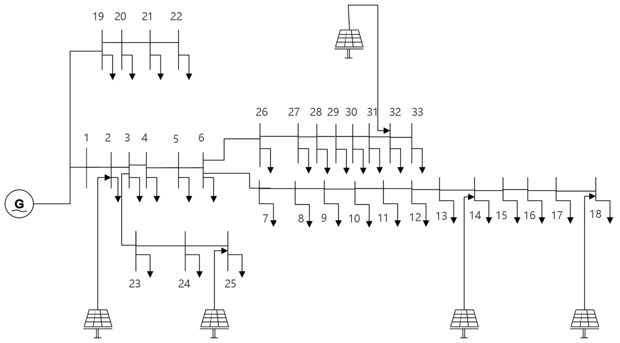

Fig.8. Nodes Topology Network of The Physical Device Layer of The Distributed PV Distribution System

Based on the network node topology graph in Fig. 8, the degree centrality, meson centrality, and proximity centrality of each distributed PV access node are calculated sequentially.

The degree centrality function is:

$$PV_{\mathrm{x}} = \frac{k_{\mathrm{i}}}{\mathrm{N}-1} \qquad (1)$$

where k_{i} is the number of edges directly connected to the PV access node and N-1 denotes the number of edges that start at the PV access node and end at the remaining nodes in the network graph.

The meson centrality function is:

$$PV_{\mathrm{y}} = \frac{2}{(\mathrm{N}-1)(\mathrm{N}-2)} \sum_{s\neq i\neq t} \frac{n_{\mathrm{st}}^{\mathrm{i}}}{g_{\mathrm{st}}} \qquad (2)$$

where n_{st}^{i} denotes the number of paths that pass through PV access node i and are shortest paths, and g_{st} denotes the number of shortest paths connecting any two non-PV access nodes in the network graph.

The proximity centrality function is:

$$PV_{\mathrm{z}} = \left(\frac{1}{\mathrm{N}-1}\sum_{\substack{j=1\\ j\neq \mathrm{i}}}^{\mathrm{N}} d_{\mathrm{ij}}\right)^{-1} \qquad (3)$$

d_{ij} denotes the distance from PV access node i to other nodes, and the reciprocal of the sum of the average distances is its proximity centrality.

The above parameters are averaged to form a comprehensive indicator of network centrality of distributed PV access node i. PV_{i} is used to measure the basis of attacker's selection of attack nodes.

$$PV_{\mathrm{i}} = \frac{PV_{\mathrm{x}} + PV_{\mathrm{y}} + PV_{\mathrm{z}}}{3} \qquad (4)$$

Remember the attack breakthrough to the physical layer as the total event space, the total number of PV nodes in the physical layer is N. the attacker successfully invades a total of n PV nodes as event A_{n}, and PV node i is attacked as event B_{i}.

If an attacker launches an attack on a combination of multiple PV nodes, on the one hand, the attacker prioritizes the nodes with high network centrality and launches an attack on each node in turn; on the other hand, considering the network security detection device deployed on the physical side, the probability that an attack launched on a node with high network centrality will be detected is greater than the probability that an attack launched on a node with low network centrality will be detected, and if the attack is successfully detected, then the attack stops; Denote the matrix

$$J = \begin{bmatrix} \mathrm{p}_{ii} & \mathrm{p}_{ij} \\ \mathrm{p}_{ji} & \mathrm{p}_{jj} \end{bmatrix} \qquad (5)$$

p_{ii} denotes the probability that the attack is not successfully detected under the condition that the currently selected attack target is the maximum network centrality node. The value is taken as 0.4.

p_{ij} denotes the probability that the attack is not successfully detected under the condition that the currently selected attack object is not the maximum network centrality node. The value is taken as 0.9.

p_{ji} denotes the probability that attack is successfully detected under the condition that the currently selected attack object is the maximum network centrality node. The value is taken as 0.6.

p_{jj} denotes the probability that an attack is successfully detected if the currently selected attack object is not the largest network centrality node The value is taken as 0.1.

$$Q = \begin{bmatrix} \mathrm{p}_{\mathrm{m}} \\ \mathrm{p}_{\mathrm{n}} \end{bmatrix} \qquad (6)$$

p_{m} indicates that the probability of selecting the maximum network centrality node among the remaining nodes as the attack object, which takes the value of 0.8.

p_{n} denotes the probability of selecting other nodes among the remaining nodes as the target of the attack, which takes the value of 0.2.

$$Z = JQ \qquad (7)$$

Then the probability that the total number of attacking nodes is n is

$$\mathrm{P}(\mathrm{A_n}) = \begin{cases} Z_{11}{}^{\mathrm{n}-1} Z_{21} & 1 \leq n \leq \mathrm{N-1} \\ 1 - \sum_{n=1}^{\mathrm{N}-1} \mathrm{P}(\mathrm{A}_n) & n{=}\mathrm{N} \end{cases} \qquad (8)$$

The quantitative results are shown in TABLE III below

TABLE III.PROBABILITY OF TOTAL NUMBERS OF PV NODES ATTACKED

Total number	1	2	3	4	5
P(A$_{\mathrm{n}}$)	0.500	0.125	0.125	0.0625	0.0625

Characterize the risk factor of a distributed PV access node i being compromised by an attack using the following equation

$$u_{PV_i} = \frac{PV_i}{PV_{\max}} \qquad (9)$$

The probability that a given PV node i will be the target of an attack in the space consisting of all attack events is quantified by the following equation:

$$\mathrm{P}(\mathrm{B}_i) = 1 - \mathrm{e}^{-u_{PV_i}} \tag{10}$$

The probability of each PV node being attacked is shown by Fig. 9.

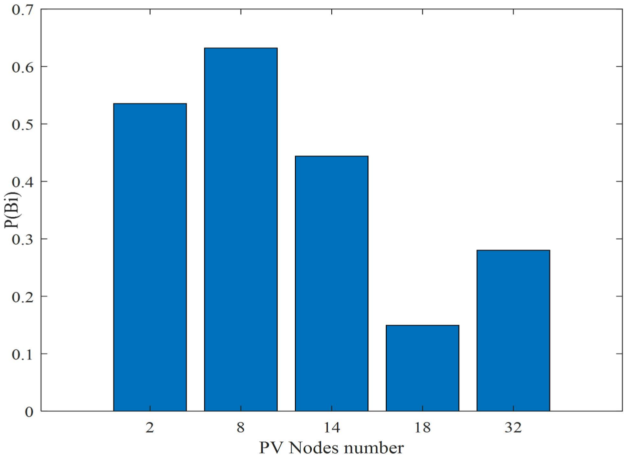

Fig.9.Probability of Each PV Node Being Attacked in All Attack Events

When the total number of intruding nodes is 1;The probability of different PV nodes being the target of an attack is positively correlated with the risk factor under the conditions of the event A_1. There is

$$\mathrm{P}(\mathrm{B}_i \mid \mathrm{A}_1) = \frac{u_{PV_i}}{\sum_{i=1}^{n} u_{PV_i}} \tag{11}$$

As a result, the probability of each node being attacked when the total number of intruding nodes is 1 is shown in TABLE IV below

TABLE IV. PROBABILITY OF EACH PV NODE BEING ATTACKED

PV node	PV_x	PV_y	PV_z	PV_i/probability
2	0.09375	0.2802	0.1429	0.1723/26.95%
8	0.0625	0.4435	0.1684	0.2248/35.16%
14	0.0625	0.2258	0.1074	0.1319/20.63%
18	0.03125	0	0.0780	0.0364/5.69%
32	0.0625	0.0625	0.0967	0.0739/11.57%

V. Conclusion

This paper proposes a conduction risk assessment method for cyber attacks against power distribution system , which quantifies the risk of cyber attacks breaking through the security protection equipment to reach a specific photovoltaic field station. Results show that the conduction path of cyber attacks and the topology of the physical layer of the distribution system affects the probability of the successful cyber attack, which provide a reference for the scheduling of cyber security defense resource allocation in the distribution system.

References

[1] Yohanandhan RV, Elavarasan RM, Pugazhendhi R, Manoharan P, Mihet-Popa L, Zhao J, et al. A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid. Int J Electr Power Energy Syst 2022; 136: 107720.

[2] G. Liang, S. Weller, J. Zhao, F. Luo, Z. Dong The 2015 Ukraine blackout: Implications for false data injection attacks IEEE Trans Power Syst, 32 (4) ,2016, pp. 3317-3318

[3] Z. Li, W. Tong, X. Jin Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel Automation Electric Power Syst, 40 (8) ,2016, pp. 147-151.

[4] Roy S， Pico H N V. Transient stability and active protection of power systems with grid-forming PV power plants[J]. IEEE Transactions on Power Systems，2022，38(1)，pp. 897-911.

[5] WU Yibei, LI Jun'e, LIU Quanying, etc. Large scale controllable loads are being suppressed Risk analysis of distribution network under the scenario of intentional control [J]. Power System Automation, 2018,42 (10): 30-37.Chinese

[6] HUMAYED A,LIN J,LI F, et al. Cyber-physical systems security survey[J].IEEE Internet of Things Journal,2017,4(6):1802-1831.

[7] Y. Zhang, L. Wang, Y. Xiang Power system reliability analysis with intrusion tolerance in SCADA systems IEEE Trans Smart Grid, 7 (2) ,2015, pp. 669-683.

[8] Semertzis, I.; Rajkumar, V.S.; S¸tefanov, A.; Fransen, F.; Palensky, P. Quantitative Risk Assessment of Cyber Attacks on Cyber Physical Systems using Attack Graphs. In Proceedings of the 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), Milan, Italy, 3 May 2022; pp. 1–6.

[9] Deng, S.; Zhang, J.; Wu, D.; He, Y.; Xie, X.; Wu, X. A Quantitative Risk Assessment Model for Distribution Cyber-Physical System Under Cyberattack. IEEE Trans. Ind. Inform. 2023, 19, 2899–2908. [CrossRef]

[10] He, X. Threat Assessment for Multistage Cyber Attacks in Smart Grid Communication Networks. Ph.D. Thesis, Universität Passau, Passau, Germany, 2017.

[11] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, et al. Takashi Onoda, Yasuhiro Hayashi. Detection of cyber attacks against voltage control in distribution power grids with PVs IEEE Trans Smart Grid, 7 (4) ,2015, pp. 1824-1835

[12] Lv, Z.; Han, Y.; Singh, A.K.; Manogaran, G.; Lv, H. Trustworthiness in Industrial IoT Systems Based on Artiffcial Intelligence. IEEE Trans. Ind. Inform. 2021, 17, 1496–1504.

[13] Liu, X.; Ospina, J.; Konstantinou, C. Deep Reinforcement Learning for Cybersecurity Assessment of Wind Integrated Power Systems. IEEE Access 2020, 8, 208378–208394.