Research on Hybrid Networking Mode and Security Strategy for Intelligent Operation and Maintenance Scenario of Wind Farm

Jinhui Li*
China Telecom Research Institute, National Engineering Research Center of Cloud and Network Infrastructure Security, Shanghai, China
lijh37@chinatelecom.cn

Jinhua Wang
China Telecom Research Institute, National Engineering Research Center of Cloud and Network Infrastructure Security, Shanghai, China
wangjinh@chinatelecom.cn

Chengbin Huang
China Telecom Research Institute, National Engineering Research Center of Cloud and Network Infrastructure Security, Shanghai, China
huangchb@chinatelecom.cn

ABSTRACT

In recent years, the operation and maintenance (O&M) of wind farms has gradually developed towards intellectualization. However, due to the fact that most wind farms are built in remote areas with backward network infrastructure, the progress of intelligent O&M of wind farms is slow. Based on the current network situation of wind farms and the network requirements of intelligent O&M, this paper proposes a hybrid networking mode of 5G private network and traditional power communication network, and the networking mode integrates 5G on the basis of retaining the original production network of traditional wind farms private network. This networking mode not only ensures the safe access of intelligent inspection equipment and various sensors in the wind farm, but also provides customized network services such as large bandwidth and low latency. In addition, this networking mode combines the data analysis capabilities of the cloud platform to realize the unattended and unattended wind farm O&M mode, effectively reducing the cost of wind farm operation and maintenance and improving the power generation efficiency of the wind farm. Finally, this paper analyzes the risks of this networking mode, and proposes corresponding security strategies for terminal access and end-to-end (E2E) network channels to ensure the communication security of wind farm intelligent O&M scenarios.

KEYWORDS

5G private network, intelligent O&M, hybrid networking, security policy

ACM Reference Format:
Jinhui Li*, Jinhua Wang, and Chengbin Huang. 2022. Research on Hybrid Networking Mode and Security Strategy for Intelligent Operation and Maintenance Scenario of Wind Farm. In *2022 Asia Conference on Electrical, Power and Computer Engineering (EPCE 2022) (EPCE 2022), April 22–24, 2022, Shanghai, China.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3529299.3530211

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
EPCE 2022, April 22–24, 2022, Shanghai, China
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9612-7/22/04…$15.00
https://doi.org/10.1145/3529299.3530211

1 INTRODUCTION

The realization of intelligent O&M of wind farms faces many difficulties. First of all, wind farms are usually distributed in coastal or mountainous areas with harsh natural environment and climate, and various types of equipment in wind farms are scattered, which increases the difficulty of operation and maintenance. Secondly, the intelligent O&M of wind farms requires on-site equipment to be able to send back the collected sensor and multimedia data in real time for real-time calculation and analysis of the data. However, at present, wind farms are usually only equipped with optical fiber ring networks. For equipment that cannot be connected by wire, such as inspection robots, special sensors in wind turbine blades, etc., the collected data can only be stored in the local memory card of the equipment. Real-time data access to edge and cloud data processing platforms cannot be guaranteed. The introduction of 5G technology not only solves the problem of real-time data collection of complex equipment in wind farms, but also customizes bandwidth and latency according to the specific network requirements of wind farms to provide network services with the best cost-effectiveness. However, how to integrate the 5G network with the existing wind farm network and how to ensure the access security of 5G equipment will be the two major problems faced by the development of intelligent O&M of wind farms.

At present, there have been related researches on the application of 5G technology in the wind power industry such as [1], [3]. However, there is no research on the networking mode and security strategy of wind farm intelligent operation and maintenance scenarios. Starting from the network requirements of wind farm intelligent operation and maintenance services, and based on the current situation of wind farm network architecture, this paper studies a hybrid networking mode of 5G private network and traditional power communication network, which satisfies the wireless access, High bandwidth and low latency network requirements. At the same time, this paper analyzes the security risks of this private network mode, and proposes the corresponding wireless terminal access security strategy and E2E network channel security strategy, which can better meet the high security requirements of wind farm intelligent operation and maintenance.

2 HYBRID NETWORKING ARCHITECTURE DESIGN OF 5G PRIVATE NETWORK AND TRADITIONAL POWER COMMUNICATION NETWORK

Recently, the 5G industry chain and the smart device industry chain have developed rapidly, and a large number of smart O&M devices that support 5G access have entered people's field of vision, such as inspection robots, drones, and smart sensors. The emergence of these intelligent terminals can simplify the O&M of wind farms in many fields, making it possible to realize intelligent O&M of the entire wind farm [1-2]. However, there is currently no 5G signal coverage in wind farms, and most of the production control data and equipment collection data of traditional wind farms are transmitted through the optical fiber ring network. Therefore, most of the data of inspection equipment that cannot be accessed by wire is stored locally, which cannot meet the real-time data requirements of intelligent O&M of wind farms. Therefore, this paper integrates the networking requirements of wireless access, large bandwidth, low latency, and full coverage required for intelligent O&M of wind farms, as well as the networking situation of wind farms, designs a hybrid networking mode of 5G private network and traditional wind power production network. On the premise of ensuring the security of production network information, this networking mode realizes the beneficial blessing of the 5G private network to the intelligent O&M collection of wind farms.

2.1 Network requirements for wind farm O&M scenarios

With the development of intelligent robots and intelligent sensors, the O&M work of wind turbine tower detection, wind turbine blade damage repair, wind turbine cabin environment perception, and wind turbine blade fault monitoring can be completed by robots instead of manual work. However, the intelligent O&M of wind farms is not a simple superposition of various O&M tasks. It requires robots and sensors to operate autonomously and to complete the closed loop of the entire O&M process from data collection, data analysis to alarm and control. Therefore, the data of all robots, sensors and other equipment in the wind farm needs to be connected to the same network, and the 5G network can just meet this local coverage scenario. At the same time, the low latency and large bandwidth of the 5G network also satisfy the large data volume and high real-time access of these terminals.

Among them, in the scene of robot inspection of fan tower, due to the high fan tower and complex equipment in the tower, the inspection process is more difficult. The traditional fan tower inspection method is generally manual climbing inspection or inspection with the help of telescopes [1]. The inspection method of manual climbing is not only complex in process, but also has a high risk factor; the method of telescope inspection is easy to cause defect misjudgment due to the long distance and low clarity. The use of inspection robots to complete the tower inspection work can solve these problems. The inspection robot equipped with 5G module can send back 4K / 8K ultra-high definition video in real time through large bandwidth 5G slices. Then, inspectors can remotely control the inspection robot through video to clearly check every detail of the fan tower in real time, which greatly improves the work efficiency of inspection.

In the environment perception and monitoring scene inside the fan cabin, when the temperature and humidity reach a certain value, it will have an adverse impact on the operation of the equipment. Therefore, multiple temperature sensors and humidity sensors will be added at different positions in the cabin to monitor the temperature and humidity in real time. The camera and sensor equipped with 5G module can not only get rid of the limitation of the cable on the camera position, but also return video, temperature and humidity data in real time. The data platform will conduct real-time analysis on the data. Once the analysis results meet the alarm conditions, it can also automatically alarm the authorized O&M personnel through 5G slice, so as to facilitate the O&M personnel to find and deal with dangerous situations in time.

2.2 Design of hybrid networking mode of wind farm

The hybrid networking mode of the 5G private network and the traditional wind power production network designed in this paper requires the erection of next Generation Node B (gNB) in the wind farm, and the installation of 5G signal enhancement equipment in places with strong signal shielding such as wind power towers and computer rooms, so that 5G signals can cover the entire wind farm. Terminal devices such as inspection robots can access the edge cloud platform through the 5G private network, and the large bandwidth of 5G can ensure that they can transmit multimedia data in real time; Apps dedicated to O&M can also access the edge cloud platform through a specific slice of the 5G private network to obtain the required O&M information. At the same time, this networking method also needs to deploy an optical fiber ring network and safety isolation equipment on the device side to transmit supervisory control and data acquisition (SGADA) system data in the traditional production network to the edge cloud platform. After the edge cloud platform collects all the data, it calculates and analyzes the data, and sends the processing results to the O&M App and the center cloud platform. Wind farm O&M personnel and group O&M experts can jointly carry out O&M work through the O&M App and group cloud data to improve O&M efficiency. The network mode structure is shown in Figure 1

In this networking mode, the edge cloud platform can collect power grid production data, sensor data, video images and other data in real time through wired and wireless network. On the one hand, these data will be stored and backed up in the edge cloud, on the other hand, they will be mapped and calculated according to the physical model, and the calculation results will be sent to the group center cloud at a certain time interval. This can not only reduce the transmission bandwidth pressure between the edge cloud and the group cloud center, but also reduce the data computing and storage pressure of the group cloud center.

In addition, this networking mode can provide three key capabilities, namely, wireless data acquisition capability, low latency wireless data transmission capability and wireless data isolation capability. Wireless data acquisition capability mainly refers to that, compared with the traditional single optical fiber ring network, the terminal equipment can access the data acquisition platform

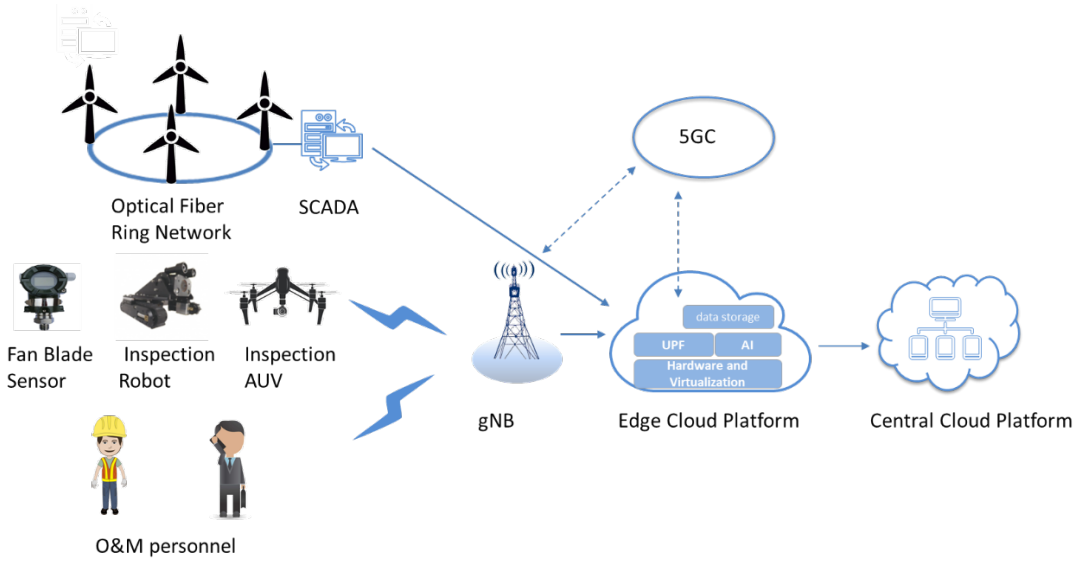

Figure 1: Networking model of 5G private network and traditional wind power production network combination

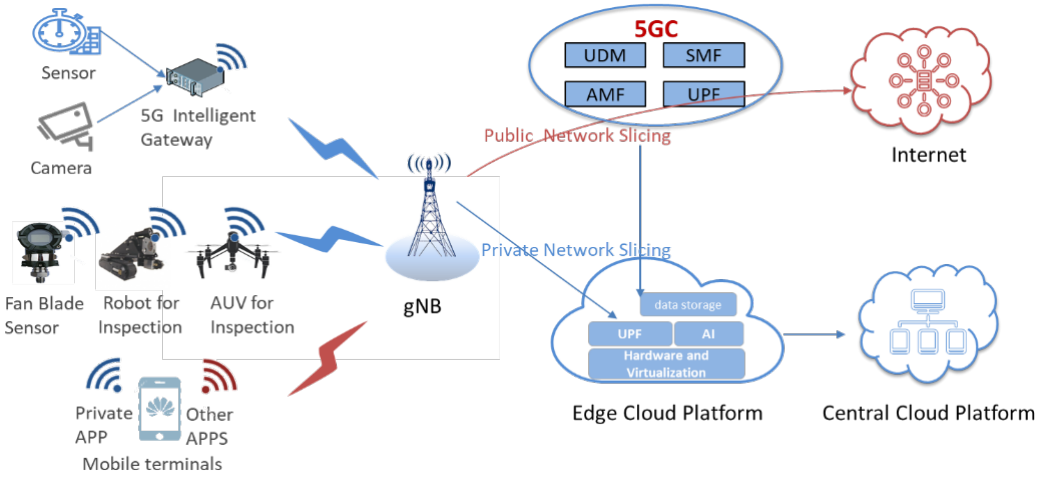

Figure 2: Data wireless acquisition and processing architecture diagram

through 5G private network. For example, in order to analyze the running state of the fan blade in real time, it is necessary to collect its vibration, speed and other data in real time. So we have to deploy relevant sensors on the fan blade. Since the fan blade rotates continuously during operation, it is not suitable to use wired mode for data acquisition. The sensors and other equipment on the blade can be connected to the data acquisition platform through 5G private network. Low latency wireless data transmission capability refers to the deployment of user plane function (UPF) to the edge of the network based on the Control and User Plane Separation (CUPS) architecture of 5G Core Network (5GC) in this paper, which reduces the transmission delay, realizes the local diversion of data traffic, and relieves the data transmission pressure of the core network, so as to improve the network data processing efficiency and meet the requirements of wind farm O&M for low latency, large bandwidth and security. Wireless data isolation capability means that in order to ensure the security of wireless data acquisition, 5G slicing technology is used to realize the data isolation between 5G private network and public network. For example, the mobile terminal App authorized for the wind farm O&M system can access the edge cloud platform through the 5G private network slice, while other mobile terminals or their Apps can only access the data network through the public network slice, so as to realize the isolation from the private network and the public network [7]. As shown in Figure 2

Table 1: Terminal access security policy table

Security risks	Security policy	attribute
Endpoint access security risks	Primary Authentication	Required
	Network Slice-Specific Authentication Power system secondary authentication	Choose one of the two
	Privacy protection of S-NSSAI	Required
	network access restrictions	Optional

3 RESEARCH ON SECURITY RISK AND PREVENTION STRATEGIES

The SGADA data in the existing wind farm is accessed to the edge cloud platform through the operator's private line. There are already many mature boundary protection methods, such as the deployment of one-way isolation gates, physical firewalls and other security isolation devices, which will not be repeated in this article. This paper focuses on 5G terminal access and E2E network channel security, and proposes security reinforcement strategies for wind farms.

3.1 Terminal access security risk and protection

The emergence of 5G network and intelligent terminal inevitably magnifies the threat of security vulnerabilities such as malicious programs and firmware vulnerabilities. Power industry data information is very sensitive to security, so when the terminal is accessed, the primary authentication, ciphering and integrity protection of 5G network defined by The 3rd Generation Partnership Project (3GPP) Standards Developing Organization are not enough. On the basis of the primary authentication when terminal access to 5G network, this paper provides safe access capabilities such as network slice-specific authentication, power system secondary authentication and network access restrictions, so as to meet the high security needs of the power industry. Terminals such as 5G intelligent gateways, intelligent inspection robots, and mobile Apps need to pass a multi-level certification system when accessing the wind power network, as shown in Table 1

1) Primary authentication: When the terminal accesses 5G network, it should carry out primary authentication based on the USIM/eSIM card, such as EAP-AKA, 5G AKA. Prevent illegal users from accessing the network.
2) Network slice-specific authentication: When the terminal is connected to the wind power private network, it needs to select the correct slice for the terminal through the terminal's single network slice selection assistance information(S-NSSAI) firstly. At the same time, slice specific authentication and authorization can be carried out to ensure that the legitimate terminal accesses the dedicated slice.
3) Privacy protection of S-NSSAI: In the process of accessing the wind power dedicated slice, the terminal needs to encrypt the S-NSSAI to prevent the leakage of S-NSSAI.
4) Power system secondary authentication: Wind power enterprises can choose to deploy authentication servers. After the wind power terminal / special App is connected to the special slice, if you need to access wind power business, you need to pass the secondary authentication of wind power.
5) network access restrictions: When the terminal accesses the wind power dedicated slice, it can restrict the location area of the access terminal through the closed access group (CAG). At the same time, it can also limit the terminal's access to the specific UPF according to the specific data network name (DNN).

3.2 E2E network channel security risk and protection

At present, network slices generally adopt the method of logical isolation, but if one network slice overload may cause other network slice resources in the same physical pipeline to be preempted. And the attacked network slice may also affect other network slices [9]. Therefore, this paper uses Flexible Ethernet (FlexE) technology to achieve hard pipe isolation between network slices. At the same time, communication is required between different network slices and between access network slices and core network slices. In order to prevent attackers from attacking the network slice interface and stealing user data, this paper uses E2E security encryption and isolation technology to ensure the security of wind power operation and maintenance data.

(1) E2E data encryption technology

At present, a gNB is usually configured with only one priority list of ciphering and integrity algorithms. AES algorithm is generally used as the first priority algorithm for public network slice. This paper proposes a security strategy to set the priority order table of different algorithms for different slices in gNB, that is, set the priority order table of different ciphering and integrity algorithms by identifying S-NSSAI. For wind power dedicated slice, ZUC algorithm is set as the first priority algorithm in gNB to distinguish the priority from public network slice security algorithm and prevent key business information from being eavesdropped and tampered on the air interface side. At the same time, an internet protocol security (IPSec) gateway is deployed at the interface between the 5G base station and the edge UPF, and between the UPF and edge cloud to construct a network security channel. For 5G terminals with high security requirements, security modules or security chips should be integrated, and corresponding password modules should be deployed on edge cloud platforms, to realize data encryption communication at the application layer between 5G terminals and edge cloud platforms and secure E2E data transmission security.

(2) Slice resource guarantee and isolation technology

In order to ensure the E2E resource guarantee and safety isolation of wind power dedicated slice, this paper proposes to reserve resource

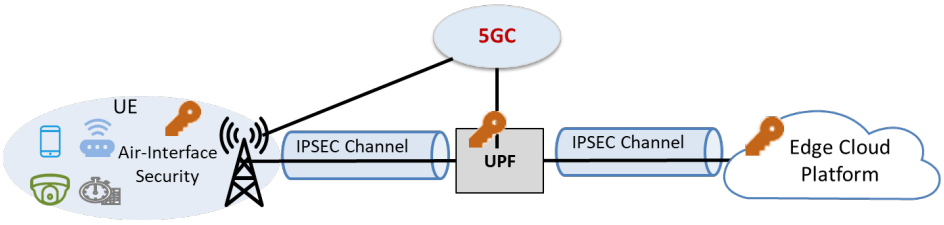

Figure 3: E2E data encryption security

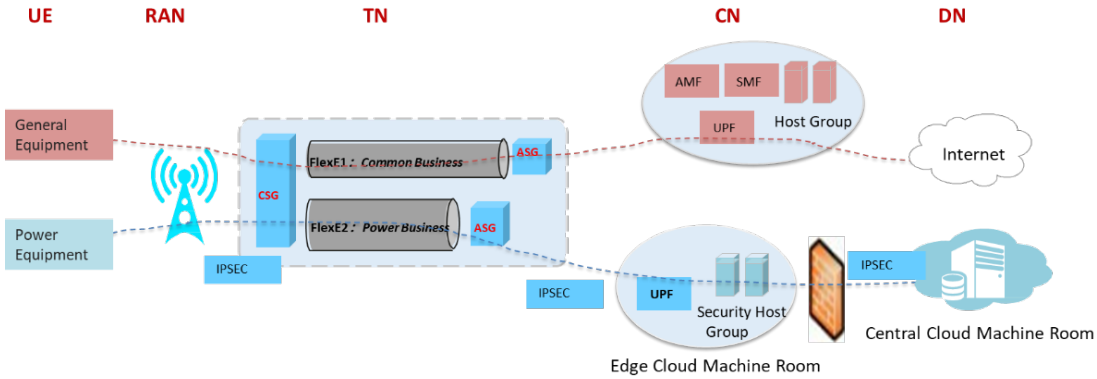

Figure 4: E2E slice isolation

Table 2: Network security policy table for different business types

Business	UE	RAN	TN	CN
Public data business	Primary Authentication	Do not do rate guarantee Default Ciphering and integrity guarantee	Common FlexE	Public UPF
Wind power business - intelligent inspection	Primary Authentication Slice authentication/ Power secondary authentication	RB reservation Upstream rate guarantee ZUC ciphering and integrity protection	Dedicated FlexE Fixed Bandwidth IPSEC Channel	Edge UPF Specific DNN
Wind power business - intelligent maintenance	Primary Authentication Slice authentication/ Power secondary authentication	Downlink rate guarantee ZUC ciphering and integrity protection	Dedicated FlexE Fixed Bandwidth IPSEC Channel	Edge UPF Specific DNN

block (RB) for wind power dedicated slice on the radio access network (RAN) to achieve slice-level spectrum isolation. Then, FlexE technology based on slot scheduling is adopted on the transport network (TN) to ensure fixed bandwidth allocation and isolation of wind power slice. Build a UPF based on dedicated security units at the edge, and use a Specific DNN in the core network (CN) to realize the flow of power service data to the edge UPF to achieve E2E resource guarantee and high-strength security isolation of user data, as shown in Figure 4. At the same time, this paper also designs different security strategies for different business types to ensure E2E security isolation and resource management of each business, as shown in Table 1

4 CONCLUSION

Based on the intelligent O&M scenario of wind farms, this paper proposes a hybrid networking mode of 5G private network and traditional power communication network and its security strategy. On the premise of not changing the existing architecture of wind farm production network, it applies 5G technology to wind farm intelligent O&M scenarios, and proposes corresponding security strategies. On the premise of meeting the high network security requirements of the power industry, the cost reduction and efficiency increase of wind farm O&M have been realized, and good practice has been made for the application of 5G in the intelligent application of various scenarios of wind farms in the future. However, due to the geographical location of wind farms, the construction of base stations is generally difficult and the initial investment is relatively

large. How to further reduce costs and improve efficiency requires further research. In addition, how to realize the intelligent control of production equipment in the wind farm production network under the premise of meeting the safety requirements and specifications of the wind power industry, and then realize the intelligence of the entire wind farm is also an important topic in the future.

REFERENCES

[1] Wang Yan, Tong Bo, Li Jiadong, Liu Mingjiang, Su Xinmin, Zhou Guodong, "Application Status and Prospect of 5GTechnology in Intelligent Operation and Maintenance of Offshore Wind Farms [J] " Ship Engineering, 2021, 43(S1): 130-133 .

[2] Li Kui, Yin Houfei, Yang Zhi, Wang Zhitao, Huang Sumin, Zhang Kangkang. Intelligentization and Application of Fan Blades [J]. Technology Innovation and Application, 2020(33):174-175.

[3] Yu Xiaoguang, Yu Yingxin, Yang Chen Jinjian, Xie Xiaoqing. Security Technology in 5G Smart Grids [J]. Journal of Information Security Research, 2021,7(09):815-821.

[4] J. Ye, Y. Gao and X. Su, "Smart Energy Management Cloud Platform Design Based on Offshore Wind Farm," 2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), 2019, pp. 130-133, doi: 10.1109/ICITBS.2019.00038.

[5] Yang Ruyi, Feng Shuchen, Wang Xianwen, Zhang Yue, Zhang Dongming, Yu Dapeng. Application Analysis of 5G Network Slicing in Intelligent Power Generation and Management of Thermal Power Plants [J]. Energy Science and Technology, 2021, 19(06): 49-54 .

[6] Zhang Xiping, Wu Zhiquan, Wu Chun, Feng Qiang. Data Collection,Analysis and Calculation Method of Intelligent Wind Farm Based on Edge Computing[J]. Electric Engineering,2021(10):54-57+79.

[7] Yang Yuan, Wang Shaoyong, Tan Jiangping, Chen Liang. The Intelligent Operation and Maintenance Management System for Offshore Wind Farms [J]. Southern Energy Construction, 2021, 8(01): 74-79

[8] Wang Tiantian, Yang Hongzhen, Mao Xiuwei, He Chen, Xu Yangzhou, Lu Shan, He Jiale, Shen Jiahui. The Typical Application Scenarios Based on 5G Power Virtual Private Network [J]. Electric Power Information and Communication Technology, 2021,19(09) :38-44.

[9] Zhang Xiaojian, Fei Jiaxuan, Jiang Haitao, Yao Qigui. Security Risk Analysis of Power 5G Hybrid Networking [J]. Telecommunications Science, 2022,38(01):132-139.

[10] Zhang Maatata. Application of 5G network slicing in power industry [J]. International Electronic Elements, 2021, 29(19): 103-106.

[11] Li Pifan, Liu Zhonghua, Cao Tongjie.Discussion on Smart Operation and Maintenance Solution of Offshore Wind Farm Based on 5G Private Network [J]. Designing Techniques of Posts and Telecommunications | Desig Techn Post Telecommun, 2021(07):51-54.