Systematic Application of Commercial Encryption Technology in New Energy Network Security Protection

Bo Wu[1, a], Qi Zong[2, b], Lei Chen[3, c*], Junping Zhou[4, d], Wuyi Zhang[5, e]

[1]Westone Information Industry INC., Chengdu City, Sichuan Province, China
[2]Westone Information Industry INC., Chengdu City, Sichuan Province, China
[3]Westone Information Industry INC., Chengdu City, Sichuan Province, China
[4]Westone Information Industry INC., Chengdu City, Sichuan Province, China
[5]Guodian Nanjing Automation Co., Ltd, Nanjing City, Jiangsu Province, China

[a]e-mail: 2725212515@qq.com
[b]e-mail: 2725212515@qq.com
*Corresponding author: [c]13581669627@163.com
[d]e-mail: 2725212515@qq.com
[e]e-mail: 14706253@qq.com

Abstract. China strives to achieve carbon peak by 2030 and carbon neutrality by 2060. The "double carbon" strategy advocates a green, environment-friendly and low-carbon lifestyle. In order to accelerate the pace of reducing carbon emissions, guide green technology innovation, and improve the global competitiveness of industry and economy, China continues to promote the adjustment of industrial structure and energy structure, vigorously develop renewable energy, accelerate the planning and continuous construction of new energy power generation bases such as wind power and photovoltaic, and strive to give consideration to economic development and green transformation simultaneously. At the same time, since 2017, the number of global cyber attacks against the energy sector has surged. Among them, the power grid and oil and gas infrastructure have become the "key areas" of cyber attacks, accounting for more than 50% of all cyber attacks. In this context, in order to ensure the safe and stable operation of new energy business production, based on the actual requirements of network security protection of typical business information systems and automatic control systems under the new energy scenario of electric power enterprises, this paper studies and proposes systematic encryption applications from encryption service to key management to encryption monitoring. Based on the unified key management and encryption monitoring platform, the technical architecture is jointly developed, combined with business processes; realize the design of encryption related applications and software and hardware monitoring. At the same time, according to the feasibility of technology realization and the characteristics of the new energy physical environment, we put forward suggestions on technology implementation, and finally form a practical application prototype suitable for the pilot construction, so as to realize the systematic application of commercial encryption s in the new energy network security protection, effectively improve the enterprise's network security capabilities

V. Escudero et al. (Eds.): BADS 2022, AHCS 11, pp. 383–390, 2023.
https://doi.org/10.2991/978-94-6463-102-9_41

and achieve the goal of standardized and safe use of encryption s, so as to ensure the safe and stable operation of new energy business.

Keywords: Electric power enterprises; Systematic application; Network security protection; Cryptography; Network security

1 Introduction

In 2021, the country defined the positioning of carbon peaking and carbon neutralization, and made a systematic plan and overall deployment for the major work of carbon peaking and carbon neutralization. Guided by relevant policies, China's new energy development, represented by wind power and photovoltaic power generation, and has achieved remarkable results, with the installed capacity ranking first in the world and the proportion of power generation rising steadily. The new energy business is mainly composed of information systems and industrial control systems. As the advanced technology and development space of information systems and industrial control systems continue to increase, network security vulnerabilities will also increase. With frequent network security incidents, new energy network security will face more severe challenges [1-2].

To sum up, in order to achieve the goal of reaching the total installed capacity of wind power and solar power to more than 1.2 billion kilowatts by 2030, and accelerate the construction of a clean, low-carbon, safe and efficient energy system, a strong network security protection framework is required as a business security guarantee. The safe, compliant use and construction of cryptographic technology can help to do a good job in the network security protection of new energy construction in carbon peak and carbon neutral work. To achieve this goal. This paper proposes the systematic application of commercial encryption s in new energy network security protection, and can be applied in new energy wind power generation [3-4].

2 Problems and needs

The operation and maintenance management of new energy power generation system is an important guarantee for the safe and smooth operation of new energy power generation. This paper takes the typical business system of new energy power generation - centralized control system as an example to study the business process, analyze the problems faced and business network security requirements. With the development of science and technology in recent years, the intelligent power management system has emerged as the times require, opening a new business model of “unattended and few people on duty” for power generation business. The centralized control system of new energy power generation provides the centralized management and control function of new energy business. Relying on the centralized control center of new energy, power generation enterprises can remotely monitor all new energy stations in the centralized control center, and realize the remote observation, adjustment

It can be controlled to reduce the human resource cost of power generation enterprises, integrate all operation data of enterprises, help managers intuitively understand the operation status and existing problems of all stations and equipment, and provide scientific basis for enterprise decision-making. In view of its business model and business process characteristics, relevant analysis was carried out and the following problems were found:

- Unattended and few people on duty business model has strict management requirements, and management loopholes and weak physical security may lead to unauthorized operation or destruction of illegal personnel;
- The new energy business process flows from the new energy centralized control center to the new energy station, and finally to the new energy power generation site. It involves three physical regions vertically and different regions in the typical power network partition horizontally. It is complex and interlaced. If there is no systematic security protection construction, there may be security protection omissions in the multi-level business development, Production problems and network security problems that cause internal operation errors and external attacks, mainly in the security protection of business data.

In view of the above problems, it can be seen that the centralized control business of the new energy power generation system has the following security requirements:

- In the face of massive, wide area, automated and unattended new energy scenarios, it is necessary to solve the problem of personnel identification in physical security based on the application of encryption technology, ensure that the identity of personnel entering the computer room and other important areas is legal, and ensure that the identity of the users of important host equipment deployed by the business system is legal;
- In the face of the network situation involving multi zones, multi domains and multiple physical locations involved in the new energy business data flow, it is necessary to use cryptographic technology to design business protection based on the attributes of business data, and protect the confidentiality, integrity and non repudiation of business instructions;
- At the same time, according to the basic requirements of the encryption application of the information system, in addition to the technical requirements, the relevant compliance design requirements for the encryption application's own management system, personnel management, construction and operation, and emergency response should be carried out.

3 Cryptographic system application design

In the business of the new energy centralized control system, the control command is issued by the centralized control center (centralized control side) to the power plant station (station side), and then issued by the power plant station (station side) to the on-site fan or photovoltaic (site side); Similarly, the collected data is sent from the

field side to the station side and finally to the centralized control side. The business and its associated systems are deployed in different business partitions according to business attributes.

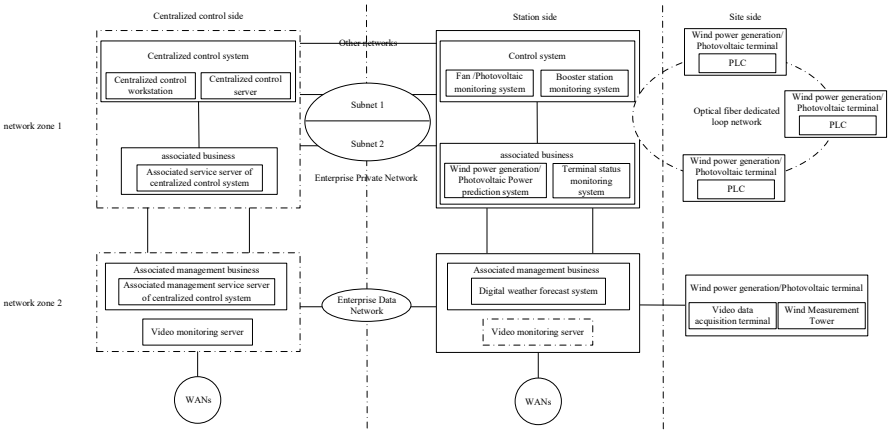

Fig. 1. Schematic Diagram of New Energy Business.

According to the technical requirements of GBT39786-2021 Information Security Technology - Basic Requirements for Cryptographic Application of Information Systems [5], the design of cryptographic application technology is carried out from the following aspects [6]:

1) Physical and environmental security. The physical and environmental security of the centralized control side and the station side is designed with the business system room as the dimension. The systems of each business area are deployed in the same machine room. The encryption application is mainly in the access control system and video monitoring system of the machine room. For the important areas on the site, the encryption is mainly used in the access control system at the entrance of the fan tower and the control area of the photovoltaic power generation unit, as well as in the video monitoring system of important areas.

The access control system is uniformly managed by the centralized control side, and the access control terminals at the centralized control side, the machine room at the station side, and the important areas at the site side can adopt the same encryption application protection design. There are many encryption applications for the access control system. The key dispersion technology based on SM4 algorithm can be used to achieve one card and one encryption for the non-contact access control card, and the symmetric algorithm is used to encrypt the random number. Through the comparison of the operation results, the identity of the cardholder can be authenticated; At the same time, fingerprint, face and other biometrics and electronic encryption s are used to complete the information input between the entry personnel and the access control recognition terminal. The technology based on SM2, 3 and 4 algorithms is used between the access control recognition terminal and the access control terminal for identity authentication and identification information protection.

The access control record information of the machine room at the centralized control side, the station side and the important area at the site side is managed and stored uniformly at the centralized control side; The video monitoring audio and video recording data of the computer room at the station side and the important area at the site side are viewed and stored in real time at the station side under their jurisdiction, and then transmitted from the station side to the centralized control side under their jurisdiction for storage. The camera terminals in each region use the signature verification technology of SM2 algorithm to conduct two-way authentication and protect the authenticity and integrity of video data with the control terminal. The symmetric encryption technology of SM4 algorithm is used to protect the confidentiality of video data.

For the unified storage of electronic access control data and video surveillance audio and video recording data on the centralized control side, the H-MAC technology based on SM3 algorithm is used for integrity protection. When log data is used, integrity verification is performed to ensure that the data has not been tampered with.

2) Network and communication security. According to the network topology, the service data transmission network between the centralized control side and the station side, and between the station side and the site side, based on the SM2 algorithm, the communication entities of both sides of the communication are mutually identified to ensure the authenticity of the communication entity identity; SM3 algorithm is used to protect data integrity during communication; SM4 algorithm is used to protect the confidentiality of data in the communication process.

3) Equipment and computing security. For important hosts of centralized control business, including servers and workstations, SM2 algorithm is used to authenticate the identity of the person who logs in to the host operating system to ensure the authenticity of the identity of the user who logs in to the host. For the key system files of the centralized control system program, the integrity protection is carried out based on SM3 algorithm. Before each startup, the key system files are verified. If the verification is passed, the program is started normally, and no error is reported through the program.

When remotely managing the equipment on the centralized control side, a secure channel is established based on SM2, 3, and 4 algorithms and SSL security protocol technology to establish a secure channel for the transmission of remote management instructions and data.

4) Application and data security. For business applications, SM2 based signature verification technology is used to verify the identity of users of business applications to ensure the authenticity of the identity of users using the application system; For the important instruction data transmitted, the signature verification technology based on SM2 protects the data non repudiation, the HASH technology based on SM3 protects the data integrity, and the encryption and decryption technology based on SM4 protects the data confidentiality. For other important data transmitted, the HASH technology based on SM3 protects the integrity of the data, and the encryption and decryption technology based on SM4 protects the confidentiality of the data. For the important data stored [7], the integrity of the data is protected by the HASH technology based on SM3, and the confidentiality of the data is protected by the encryption and decryption technology based on SM4.

In addition to encryption application technology, it is designed from the perspective of management to form a systematic application of encryption s, including encryption monitoring and key management. Encryption monitoring refers to the monitoring, statistics and analysis of encryption devices, encryption applications and key management related to encryption applications. Key management mainly refers to the management of key life cycle, mainly in key generation, distribution, storage, use, update, archiving, cancellation, backup, recovery and destruction [8]. The management design is as follows:

1) Encryption monitoring. It mainly monitors the status and information related to the encryption application, including the status of the encryption device, such as the memory usage rate and CPU usage rate of the encryption device, and the network traffic, port and IP status of the device; Key information, such as the number of keys and the key used; Business call information, including the number of encryption device connections, business transactions, and the status of business encryption applications.

2) Key Management. Through the construction of cryptographic infrastructure, complete the life-cycle management of keys and digital certificates related to cryptographic applications. Multi level management and key certificate application can be carried out according to the actual needs of the business.

4 Suggestions on implementation of encryption application

According to the actual scenario of new energy power generation, the following suggestions are made for the implementation of encryption application:

- After the business security is protected by encryption, it should meet the delay requirements of the business, and at the same time, it should not change the business operation habits in a large area. In actual operation, the operator should try to use the encryption without feeling;
- Meet the site environmental conditions, and consider the equipment form and function realized on the ground. If the physical space of the site environment is tight, the form of encryption application products/systems and the integration of multiple security functions need to be considered for implementation;
- The implementation of encryption applications for application and data security needs to consider other security requirements of each business partition, and choose different methods for different types of clients, scenarios and network conditions. For example, when the client accesses the business system, if the B/S mode is used, the national security browser is used to establish an SSL channel with the server, during which the client's identity authentication is achieved; If the C/S mode is adopted, the client uses the smart encryption key, encryption card and other encryption modules, and the server calls the encryption device/system to achieve SM2 based identity authentication. The encryption service for the business server can also be implemented by selecting a encryption device or a encryption service

platform based on the cloud micro service architecture according to the scenario, network, business system quantity, architecture and other factors;
- In order to avoid repeated construction and waste, it is necessary to formulate the relevant encryption application specification system according to the actual implementation situation to achieve unified planning, unified construction and unified management of encryption applications.

5 Conclusions

The cryptographic technology mentioned in this paper provides important support for identification, secure channel, information encryption, integrity protection and non repudiation of the new energy business system. As the underlying technology of network security, the use of encryption technology is the foundation, legal and compliant use and regulatory encryptions are the baseline, and encryption construction combined with business characteristics is the implementation principle of encryption applications. Systematical application of encryption technology can not only ensure business production security, avoid new security risks caused by security equipment vulnerabilities, but also monitor whether the protection means are correct and effective in real time, the key is managed throughout its life cycle. The systematic application of encryptions is applicable to a variety of new energy power generation scenarios, providing strong and reliable network protection for the development of new energy business.

Acknowledgment

This paper was supported by Westone Information Industry INC., and Guodian Nanjing Automation Co., Ltd.

References

1. LIU B, LI L, LIU J, et al, (2021)Analysis of Weak Links in Network Security of Power Monitoring System in New Energy Fields. Electric Engineering, 18. 78-80.
2. GAO P, CHEN ZY, YAN LC, et al, (2021) A New Generation of Power Data Security Protection Technology for Zero-trust Environment, Electric Power Information and Communication Technology, 19: 7-14.
3. GE W, (2020) Applied analysis of Electricity Information Acquisition System in Electricity Marketing, Computer Products and Circulation, 4:104.
4. JIA JF, YI HM, XIA XY, et al, (2017) Distributed energy power system access new metering system, Power System Protection and Control, 45:118-124.
5. GB/T39786, (2021) Information security technology-Baseline for information system cryptography application.
6. ZHAO YQ, (2019) Application of secondary safety protection system in photovoltaic power station, Information Technology and Informatization, 10.

7. WANG J, SONG Y, HAN S, (2018) Encryption of CARS data-link communication based on SM4 algorithm, Journal of Civi Aviation Universrry of China, 36(1): 6-10.
8. LIU X, (2021) Research on cryptography application in computer network security, China Broadband, 3: 25.