Information Hiding Technology in Power System Network Security

Jie Huang1,*, Jing Li1, Jie Wang2, Li Tian2

1State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430077
2Electric Power Research Institute of State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430070

*Corresponding author e-mail: gmq1988@126.com

Abstract. Since the beginning of the 21st century, with the popularization and application of electronic information technology in the power system, the power system information network security has begun to attract the attention of all walks of life, especially the power enterprises. To ensure the safety of electric power information network is not only the need to ensure the safety of industrial production and residents' daily electricity consumption, but also the internal demand to ensure the stability, development and prosperity of national economy. In the electric power industry, the information security of the electric power system is directly related to the production, operation, management and operation of the electric power enterprises. When these information data are illegally violated, it will bring adverse effects to the electric power enterprises. It can be seen from this paper that the network security of the telecommunications industry accounts for a large proportion of 18.7%. Therefore, information security is the important protection content of power enterprise network security. The emergence of information hiding technology, a good realization of the power network information security protection, this paper will be information hiding technology as the focus of research, analysis of its application in the power network security.

Keywords: Information Hiding, Power Network Security, Information Encryption, Power Informatization

1. Introduction
In recent years, China's power industry and enterprises to produce more confidential data information. At the same time, the development of big data and cloud computing has increased the severity of privacy leakage. Therefore, it is extremely important to protect confidential power data, which is also an important task in system network security management. Among them, information hiding technology, as a kind of "behavior security" technology, plays an important role in power information protection and has been focused on and applied.

The development of today's society proves that the network has become an important driving force for the development of various industries. Without the network, the development of the industry will
be seriously affected. The power system is a sign of the development level of a country and an important foundation for the country's economic development. The application of information networks to power systems to achieve the improvement and development of power systems is a new leap in the development of China's power system [1]. However, the inherent attributes of information network systems, such as sharing and connectivity, also make the application of the Internet a certain degree of insecurity. It is the responsibility of every power system staff to attach great importance to the safety of information systems in power systems and to effectively manage power. System information network security is the due meaning of power system development [2-3]. Today, the highly developed Internet has facilitated our lives, but at the same time has brought new crises to our lives, especially the information security crisis [4]. After the Internet is applied to the power system, the information management of the power system has become more convenient and concise, which has improved the working efficiency of the power system, and realized a full range of power system information management. However, the power system has not escaped the information network security Dilemma of the problem [5-6]. Compared with other industries, the importance of power system information network security is more obvious and prominent [7].

In the information age, science and technology is a double-edged sword. While it brings great convenience to human production and life, it also increases the danger and instability of the system it serves [8-9]. However, it is undeniable that the application and popularization of network information technology in the power system has indeed given endless power to the modernization of power [10]. However, due to the uncertainty and openness that network information technology cannot overcome, it also brings a lot of hidden dangers to the safe operation of power systems to some extent [11-12]. It is the purpose of this paper to actively explore the main problems in the current power system information network management work in China and propose reasonable precautions to solve these problems.

2. Method

2.1 It is Necessary to Increase Publicity, Deepen the Concept of Safety, and Effectively Strengthen the Power System

Information network security education has continuously improved the confidence of all employees in the power system to maintain internal information network security. The key support point for information network security lies in "people", especially the professional and technical personnel who directly or indirectly deal with the management of power system information networks within the enterprise. The Electricity Bureau where the author works has always attached great importance to the information network security education of employees within the unit. It is precisely under the intensity of publicity and education that the information network security management within the entire system has been continuously strengthened. Power supply safety has made outstanding contributions. Therefore, in order to improve the security and efficient operation of the information network, we must first strengthen publicity and education so that all members of the system can recognize, strictly observe, and actively participate in the management of the information network. Secondly, it is necessary to continuously strengthen the construction of power system information network hardware and software systems, continuously enhance its robustness, security, and ability to resist external risks, and actively prevent malicious intrusions from the outside. From a practical point of view, the current destructive power of the power network information system comes mainly from the outside, which requires the power system to continuously strengthen the management and maintenance of internal software and hardware systems. For example, it is necessary to timely find the vulnerabilities in the information network system, and when the vulnerabilities are found, the internal network system and the public service network are disconnected in time and the patches are updated in time, so as to prevent problems before they occur; the firewall and the Intrusion detection system, accurate detection and timely shielding of illegal intrusion and control from outside the system.
2.2 Digital Watermarking Technology
As for the digital watermarking technology, it mainly realizes the effect of embedding some identification information (digital watermarking) directly in the digital carrier (multimedia, document, software, etc.) to achieve the purpose of secret information hiding. This information hiding method will not have a negative impact on the use value of the original carrier, and it is difficult to be perceived and paid attention to by the perceptual system (visual system, auditory system, etc.). For spatial digital watermarking, the most typical algorithm is the least significant bit (LSB) algorithm. At this point, mainly relying on the modification of the color and the bit plane of the color component of the digital image, the adjustment of perceived unimportant pixels in the digital image is completed to express the watermark information and embed the information into the watermark to hide the confidential information.

2.3 Visual Cryptography
Compared with steganography and digital watermarking technology, visual cryptography was proposed and formed in a relatively short time. It was first proposed in 1994 and gradually improved with the passage of time. The realization principle of this function for visual cryptography is as follows: N pieces of film without any meaning are formed, and several of them are selected for superposition processing, which can not only restore the hidden information. Subsequently, the relevant researchers optimized the visual cryptography technology, and the specific improvement methods are as follows: the formation of N pieces of film with a certain significance to improve the deceptiveness of the film; The visual cipher sharing based on black and white image is extended to cover the visual secret sharing based on gray scale and color image.

3. Experiment
The realization of power system information network security structure is the key link of power system information network security management. At present, the most feasible and applied power system information network security structure mainly includes:

Firewall technology. The so-called firewall technology is to combine the network security domain and control the flow of information through a single exit. In this way, the resilience of the power system information network will be improved. Of course, the isolation of different locales can also reduce the mutual influence between locales, so as to protect the whole system.

Fingerprint authentication technology. The identification of identity is an important way to protect the security of a system. By the identification of identity, selectively allow some people to enter and refuse some people to enter, the invasion of dangerous factors can be avoided to a large extent. The key distribution center (KDC) stores the key and fingerprint characteristics of all users. IDEA
t algorithm is used to match the key and fingerprint in advance. When the user enters, the key will be authenticated by the fingerprint to find the appropriate key.

Network encryption technology. Encryption technology is a more traditional technology, widely used in a variety of industries, in the process of power system information network security management, information content can be encrypted into another code through encryption technology, through the encoding and decoding to protect the security of the information network.

4. Discuss

4.1 Analysis of Information Hiding Technology
As shown in Table 1 and Figure 1, the distribution of information security industry can be seen from the figure that the telecom industry accounts for 18.7%. Some enterprise employees and even enterprise managers of the information network security awareness is not strong, to effectively do the power information network security caused obstacles. Because the popularization of information technology in the power system is short and has not caused a huge impact on the safe operation of the power system in a short period of time, many employees fail to fully realize the importance of
ensuring the safety of the power information network. Awareness is not strong, it is difficult to ensure that the system security protection work of the unit, such as some employees login password setting is too simple, casually and the enterprise network link to share resources, these have brought hidden dangers to the power information network security. Once the information network of the power system is attacked by external criminals, it is bound to bring huge losses to the whole power enterprise.

Table 1. Customer service distribution statistics of information security industry

| Industry                      | Percentage |
|-------------------------------|------------|
| Financial                     | 17.90%     |
| Energy                        | 5.60%      |
| Transportation, logistics, transportation | 7.10%      |
| The government                | 22.70%     |
| Education                     | 6.70%      |
| Family                        | 4.10%      |
| Telecom                       | 18.70%     |
| Other                         | 17.20%     |

Figure 1. Customer service distribution in information security industry

Part of the power enterprise information network hardware system is backward and aging, causing inconvenience to the maintenance of information network security. Hardware system is the main carrier of information network operation. The backward and aging hardware system greatly increases the instability and vulnerability of information management and transmission. Compared with the traditional power management system, information network has obtained more and more enterprises, one of the most important factor is because of had by it automatic, intelligent, stabilization and strong sustainability characteristics, and the characteristics of information network, it is based on advanced network hardware system and stable, if cannot be sustained, stable to ensure network hardware management system to keep pace with The Times, it is difficult to ensure their safety. For example, the hardware failure caused by lightning, the information distortion caused by the transmission process, is related to the hardware system's backwardness and aging.

Power system information network security management and maintenance lack of systematic and normative. Compared with other public service enterprises, the power system pays more attention to its standardization and efficiency. The high efficiency of power system is based on the daily management and maintenance of standardized power information network security. After failing to establish the system, standardized, scientific and effective information network security management
and maintenance system, many enterprises in daily work can for network risk faced by power system to make timely, accurate, malicious invasion, occurring in recent years, such as network mischief and large area of the spread of the virus, has been to the safety of the power system operation caused a great loss.

4.2 Measures to Maintain the Security of Power System Information Network
To establish a systematic, standardized, scientific and effective information network security management and maintenance system, through different security measures for the power information network management, to maximize the maintenance of the power system information network security. The so-called systematization is to realize the systematic and overall management of the power information network, take it as the key work of the whole power system to coordinate, and mobilize all the forces that can be mobilized in the whole system; The so-called standardization and scientific, is to set out from the actual situation of the unit, the establishment of the actual, modern power information network management system, both

To ensure the standardization and scientific hardware system, but also to let professional personnel to the power system information network management and maintenance, so that the information network can be orderly and scientific operation; the so-called effectiveness is to gradually establish a perfect information technology supervision center and necessary emergency measures. Through the establishment of a relatively complete and unified supervision system, the power information network can be faced with a timely response in the face of a crisis, so as to avoid the loss of power information resources.

5. Conclusion
Therefore, the electric power enterprise network security is very important for the long-term stability of the electric power industry development of our country, the application of information hiding technology is scientific, reasonable, make its various advantages can fully play out, on the basis of the protection of data security, related to the trading behavior of the electric power enterprise, and help enterprises to protect their own rights, to avoid the real electricity market price leak problem, to provide effective support for the development of electric power industry in our country.

References
[1] X. Dai, K. Zhang. The Integral and Simplified Structural Model of Power System's Component Including Component's Controller (Part II): Model Construction of SVC, TCSC and HVDC[J]. Proceedings of the Csee, 2017, 37(15):4363-4371.
[2] Jinliang Xu, Yinshi Li, Jian Xie. Special Issue dedicated to the 1st International Conference on Supercritical CO2 Power System (ICSCPS 2018)[J]. Journal of Thermal Science, 2019, 28(3):393-393.
[3] Y. Wang, S. Liu, J. Liu. Resonance Mechanism Analysis of the Power System Involving Distributed Grid-connected Inverters[J]. Proceedings of the Csee, 2018, 38(9):2693-2706.
[4] B. Tang, B. Yang, Y. Ren. Optimal Design of the Power System of ABL Wind-Tunnel[J]. Journal of Xian Jiaotong University, 2017, 51(6):110-114.
[5] X. Lü, G. Liu, Y. Zhou. Research on combined unit commitment of wind power-hydro power-thermal power for the power system with pumped hydro storage[J]. Dianli Xitong Baohu Yu Kongzhi/power System Protection & Control, 2017, 45(12):35-43.
[6] E. S. Trunin, V. M. Tarakanov, S. P. Boikin. Torsional Oscillations in a Gas Turbine Unit and the Possibility of Collapse of an Isolated Power System[J]. Power Technology & Engineering, 2017, 51(2):211-215.
[7] X. Dai, K. Zhang. The Integral and Simplified Structural Model of Power System's Component Including Component's Controller (Part I): Modeling Method and Its Application in Generator Set[J]. Proceedings of the Csee, 2017, 37(14):3982-3992.
[8] S. Xu, W. Sun, H. Wang. Numerical and experimental study of the rim-driven marine current
power system[J]. Acta Energiae Solaris Sinica, 2017, 38(1):194-200.
[9] Fangxing Li, Yan Du. From AlphaGo to Power System AI: What Engineers Can Learn from Solving the Most Complex Board Game[J]. IEEE Power & Energy Magazine, 2018, 16(2):76-84.
[10] Jing Ma, Shangxing Wang, Jie Wu. Time-delay stability control strategy considering the jump characteristic of power system[J]. IET Generation Transmission & Distribution, 2017, 11(1):185-192.
[11] N. Tang, J.-X. Su, Y.-P. Wang. The Application of FFT Algorithm in Harmonic Analysis of Power System[J]. Journal of Beijing Institute of Clothing Technology, 2017, 37(4):83-88.
[12] Liangcheng Cai, Zhengyou He, Haitao Hu. A New Load Frequency Control Method of Multi-Area Power System via the Viewpoints of Port-Hamiltonian System and Cascade System[J]. IEEE Transactions on Power Systems, 2017, 32(3):1689-1700.