Research on Risk Prevention Measures of Network Information Security in Power Systems

Ji Lai¹, Jia Wu¹, Yuchen Jiang²,*
¹State Grid Jibei Electric Power Co., Ltd, Hebei, China
²NARI Information & Communication Technology Co., Ltd, Nanjing, China
*Corresponding author e-mail: 16797174@qq.com

Abstract: The imperfect network information security technology restricts the development process of network informatization of power systems. This paper mainly studies the network information security of power systems, analyzes the risks faced by power system network operation, and puts forward some preventive measures for the network information security of power systems.

1. Risks Faced by the Power System Network Operation

1.1 Openness of Computer Network

The fundamental of the network is openness. While enjoying the openness and convenience of the network, any individual or enterprise needs to bear the security risks brought by the openness, and the power system can not be avoided, so the security risks should be reduced as far as possible. Generally, the network data transmission follows the TCP-IP protocol, and network data run directly in the network world when transmitted through the message, which poses a severe test to the security of data information. Therefore, it is particularly important to ensure the security of network transmission protocols.

1.2 Computer Virus

Computer viruses are the biggest threat to power systems, which are highly infectious, latent and destructive. It can directly destroy power data through port intrusion and mounting Trojan horse, which will affect the correctness and fairness of power data. “Worm.WbBoy.cw”, “Ransomware”, “CIH virus” and other viruses are all through illegal means to paralyze or restart users’ computers to achieve economic or other purposes.

1.3 The Insufficient Supervision of Network Information Security in Power Systems

The collected power data information has always been the core of power system operation. However, due to the acceleration of the network informatization process of power systems, these important power data information will be stored in the form of network data. Although this greatly facilitates the use and analysis of power data, once these data are destroyed or tampered with, serious losses will be caused to power enterprises. At present, the supervision means and intensity of power systems for these important data are seriously inadequate, which to a certain extent has caused serious network information security risks.

The specific process is shown in Fig.1.
1.4 Backward Computer Equipment

In the process of the network informatization of power systems, due to the neglect of power enterprises, insufficient capital investment of township power companies at all levels of power systems and backward network electronic equipment, the security risk of township power systems will be increased.

Considering the economic risk and system risk, this paper divides economic risk into equipment risk, personal and environmental risk and social risk, and its risk value is the superposition of these three items. The system risk is assessed by severity index, which is divided into power flow out-of-limit severity, voltage out-of-limit severity, voltage instability severity and cascading failure severity. Then, the sum of them is quantified economically and used as the final system risk value. Finally, the total risk value of the equipment is shown in the equation (1):

$$R(t) = P(t) \sum W_i C_i(t)$$  \hspace{1cm} (1)

Among them, \(R(t)\) is the total risk of equipment caused by failure; \(P(t)\) is the possibility of equipment failure; \(W_i\) is the weight coefficient of economic risk and system risk respectively; \(C_i(t)\) is the different consequences of equipment failure, which means economic risk and system risk, and \(t\) is a certain time.

Social risk is the loss caused by the loss of load after equipment failure. Based on previous research methods, an economical and effective ratio of output value to unit electric energy consumption (ROVTUE) method is used to calculate the social risk, as shown in equation (2):

$$R_s = P_G \times W_L \times T$$  \hspace{1cm} (2)

Among them, \(R_s\) refers to the social loss caused by equipment failure, \(P_G\) refers to the power generation ratio of a certain region, that is, the ratio of gross domestic product (GDP) to electricity consumption, \(W_L\) refers to the amount of load loss, and \(T\) refers to the time of power failure.

2. Security Precautions for the Network Informatization of Power Systems

2.1 Establishing Perfect Standards for Safety Information Prevention

The development of the network informatization of power systems makes managers realize the importance of information security prevention, however, most of the risk prevention measures only exist on the surface and in the meeting without clear rules and regulations. The first step to prevent the network informatization of power systems is to establish a perfect risk prevention system and formulate emergency plans to deal with potential safety risks. When the internal operation and maintenance personnel enter the power system network, they need to be strictly authenticated. When the collected power data are transmitted up and down, the transmitted message needs to be encrypted, such as digital signature and secret key technology. Power system developers can develop an internal identity authentication system and security encryption system, which will make it more difficult for illegal personnel to enter the power system and destroy data information.

2.2 Enhancing the Ability of Virus Detection and Prevention

For the emergence of computer viruses, power systems need to develop and use new firewall technologies and also need to increase the frequency of virus detection, and operation and maintenance personnel should establish a sense of virus prevention to fundamentally reduce virus intrusion. Network technologies update very quickly, so the update speed of the power system safety prevention must keep up with it. The power protection system should be updated in time, the latest virus prevention software should be updated, and when other software is installed in the network connected equipment inside the power system, these software should be scanned safely to minimize the chance of virus invasion.
2.3 Strengthening the Supervision and Doing a Good Job of Data Backup

Improving supervision can maintain the stable operation of the power system. Therefore, it is necessary to increase the supervision penalty, increase the pressure of supervisors, and maintain the morale of supervisors. For important power data, they need to be backed up several times every day. Data backup is a safe technology solution. When the power system or mechanical equipment unfortunately encounters disaster, these data can be restored quickly, so that the whole power system can be put back into normal operation in the shortest time.

2.4 Updating Computer Equipment

As the most basic subelement, the computing equipment in the power system is an important guarantee for the stable operation of the power system. The protection ability of township-level companies in the power system to the risk and safety of network informatization of the power system has always been the weakest. In the past, there have been many information security accidents. Therefore, in the safety prevention of power systems, it is necessary to strengthen the update and design of the computer equipment of the subordinate company, and try to use the same computer equipment as the superior company, which also reduces the information transmission barriers caused by equipment compatibility.

2.5 Paying Attention to Information Security Technological Means

The security technology means is the key to solve the network informatization security of power systems. Operation and maintenance personnel can solve the potential security problems through advanced technology means. In principle, the “advanced, applicable, innovative and developmental” means can be used, the advanced means of foreign counterparts can be carefully studied, and their advanced technical means can be integrated into the power system, such as firewall technology, intrusion detection technology, vulnerability scanning technology, isolation technology, VPN technology, security audit strategy, etc. Combined with the characteristics of the power system, the details can be shown in the following aspects.

1) Active defense: Starting from the information security system, taking the technical means as the breakthrough point, the principles of “partition, secure access, dynamic perception, and comprehensive protection” are adopted, and the event-driven passive defense is transformed into message-driven active defense.

2) Continuous tracking: The development trend and achievements of international informatization and information security should be continuously tracked, studied and applied to the information security protection of State Grid Corporation of China.

3) Advanced deployment: Based on the reality, the overall situation should be grasped, and the future development of technology should be considered. The frontier technology research and the application of basic achievements should be deployed in advance, such as big data, cloud computing and virtualization technology application.

3. Conclusions

The problem of information security is becoming more and more serious in the process of modernization of power systems. It is urgent to establish a perfect information security system for power systems. The power system must start with management, technology, equipment and thought, and increase various functions of various security defense systems, system level protection and emergency precautions. Among them, the internal equipment of the power system should be mainly “anti-attack, anti-leakage, and multi-backup”, and the external equipment should strengthen the internal control and external connection. Only the internal and external considerations of the power system can better maintain the stable operation of the power system and ensure the economic benefits of the power enterprises.
References

[1] J.R. Zhai, “Measures to Strengthen Information Security Management of Computer Network in Power System,” Heilongjiang Science and Technology Information, vol.35, no.29, 2013, pp. 172-176.

[2] Y.Z. Lan, “Analysis of Safety Protection Measures for Power System Information Network,” Wireless Internet Technology, vol.25, no.10, 2012, pp.23-24.

[3] Z.H. Yan, “Preliminary Analysis of Safety Preventive Measures of Power Information Network,” Computer CD Software and Applications, vol.12, no.21, 2014, pp.196-200.

[4] W.W. Li, W.X. You, X.P. Wang, “Survey of Cyber Security Research in Power System,” Power System Protection and Control, vol. 5, no.10, 2015, pp.140-147.

[5] Y. Hu, X.R. Xie, Y.D. Han, etc, “A Survey to Design Method of Security Architecture for Power Information Systems,” Power System Technology, vol.3, no.1, 2005, pp. 35-39.

[6] Li W, Mansour Y. “Application of Transmission Reliability Assessment in Probabilistic Planning of BC Hydro Vancouver South Metro System,” EEE Trans. on Power Systems, vol.10, no.2, 1995, pp. 964-970.