Research on Information Security Strategy and Risk Management for Smart Grid

Rui Wang
China Electric Power Research Institute
No. 15 QingheXiaoying East Road,HaidianDistrict,Beijing,China.

Abstract
Firstly,analyzes the characteristics of the smart grid network, this paper expounds the importance of information network security in the safe operation of smart grid.Based on the analysis of power information security protection framework,pointing out the importance of establishing the information safety monitoringsystem for smart grid. Secondly, according to the mainfunctions and characteristics of the smart grid information new elements are analyzed.Various risks as well as malicious attack scenarios to the intelligent power network are analyzed from the aspect of information security,ranging from the information co llection,transmission,management and interaction. Finally, some feasible countermeasures and the improvement measures based on modern power system developments are given to enhance the information security of the intelligent power system in key technologies,standards,and policies.
Keywords: Smart grid, Electric power information, information security, risk management

Introduction

The smart grid is mainly based on the physical network, the new grid will be highly combined the sensor technology, communicatio n technology, information technology,computer technology and control technology with the physical network. Among them, the information is the important premiss for realization of smart grid. With the advance penetration of information technology in the electric power system infrastructure and the advanced application, the interdependence of power network and the information network will become an important part of the future smart grids.

With the development of smart grid construction, to the power enterprises, the depth of information leads to higher production efficiency and the management level for enterprises; to the power users, the popularization of information technology means more economic experienc e with electrical and better users'experience. However, the development and popularization of the informationization brings many favorable for the electric power enterprises and users, at the same time,also to the safe operation of the smart grid brings many hidden dangers. On the one hand, the development of information technology is very rapid, left manysecurity vulnerabilities in the process of technological development has not been effectively resolved, even some not identified security risks; on the other hand, the purpose of the mechanism and the role of information network and power network interaction front is not deep. The vulnerability of the malicious attack is likely to cause large-scale chain blackout. Therefore, it is necessary to analyze the information security of smart grid operation process, in-depth study of information security impact on the survival of power system.

This paper first introduces the network security features of smart grid under the condition of informatization, analyzes the security problems under the background of information in smart grid, and points out the importance of establishing the information safety monitoring system for smart grid. To further explore the impact of information network security on the existence of power system. Finally, discussed to improve information security level of smart grid strategy.

2. The characteristics of information security of smart grid

In general, a complex network of smart grid can be regarded as composed mainly of the two interdependent network, information network and the power network . The nodes in power network is simplified as the source nodes and load nodes , the two nodes are connected by a transmission line. The information node in the network is simplified to information acquisition / executes instructions node and information processing / instruction generation node ,the infor mation nodes in the network connect through the optical fiber and wireless network.

The interdependence of power network and the information network is mainly reflected in two aspects,the normal operation of network information node needs power node adjacent power network to provide working power supply,the worksafety, reliabili ty, economic operation of power network depends on the information node in the network.

Electric power network and the information network are complex ultra large scale network . In some cases,the complex network operation safety risk greater than the single complex network . From this point of view, the smart grid security can't be ignored. Among them, the security of information network is the priority among priorities. The main reasons are as follows:

From the maturity of network development , the hidden safety danger information network are relatively too much. Even in today's highly developed information technology, information in the network still has many known security vulnerabilities have not yet been resolved, and there will be more new loophole, it provides many possible channels for the attack. In contrast, an attack to the power grid often need to resort to physical means, attack cost is relatively higher ,and restricted and affected by weather and geographical conditions.

From the interdependence in the operation process , the normal operation of the power network more depends on the information network . Power output adjustment and load node in power network switching operations are based on the information network to realize. If the information network error or crash, power network is generally difficult to maintain the normal operation . On the other hand, although the operation of power information network need power network support, but the important information network are usually equipped with uninterruptible power supply systems, power outages and will not cause a big impact on the information network..

From the propagation characteristics of network fault, fault information network more easily caused widespread power outages. Because of the information floware cost far less than the cost of energy flow, which makes the information network interconnection is stronger than the power network, and information flow can frequently interact in a large range. Therefore, the scope of information network faults' affect will be more widely.

Thesmart grid structure determines the operation risk comes from power network, a lso derived from the information network.Among them,the information network security and the power grid operation risk bring by information network , to which much attention should be paid.

Analysis of the smart power grid information system security risk

Information system is based on the computer and data communication network and the application system to realize information collection, storage, processing,analysis and transmission. Grid system according to different application fields can be divided into three categories: production control system, administrative management system and marketing system.

The production control system service for the electric power production, mainly including SCADA/ EMS, substation automation system, distribution network automation system, microcomputer protectio n and automatic safety devices,need higher reliability and high real-time requirement, communication platform using the electric power dispatching communication network. The power of modern production control from local control to control stage of based on the industrial ne twork. Production control system has taken the anti electromagnetic interference, redundancy and other measures in terms of reliability, but in the high-frequency, microwave communication links still exist, tampering, theft, posing as receiving replay types of cyber threats, seriously affect the power production information's integrity, authenticity and consistency. Administrative management system service for electric power enterprise daily business management ,such as, typical financial management system, personnel management systems, materials management system, office automation system and ERP (EnterpriseResource Plan) system. The administrative system of indirect service to power production, need to obtain the power production information from the production control system, so that the communication is also used for electric power data network. Compared to the production control system, administrative system relatively open, many users through U disk type, could disclose the information . The system adopts various types operating system such as UNIX and Windows, system flaw is more, if not timely patching will result in system instability and paralysis. In addition, the system also has network threats and programming flaws, but overall,the information security important level lower than the production control system.

The marketing system is the connection of electric power enterprises ,the power users and the power material supplier, the typical system include the mark eting system, electricity market operation system, the bidding system etc.. Because need exchange with

the outside electric power enterprise entity for information, so the system must have access to the Internet. The marketing system is more open, the attackers should destroy information confidentiality, information integrity, consistency, non repudiation, a uthentication, access control in the physical, networ k, system, application and other aspects.Due to the need for data exchange and collaborative work, all kinds of electric power information system to realize the interconnection, to format the open electric power interconnection information system. The electric power information system access spots, all threats that contains the three kinds of electric power information system, there is interdependence and threats, to the interconnection of electric power information system attacks diversification.

The main feature of the smart grid information can be divided into two aspects,one is the traditional electric power, transmission, distribution, with high information links of electricity, two is to promote the "sale" and "power" of the parties involved in th e information interaction. Informationization brings many problems for the safe operation of the smart grid of the future.

Safety of information acquisition. In the smart grid, all kinds of advanced sensors and intelligent measuring meters will be widely used for monitoring the electric power system and the user state. Cost considerations, the intelligent meter is generally not adding complexity to the encryption technology, which leads to intelligent meter is easy to crack and control. Once these devices are controlled,the attacker can use its power to provide false electricity information, affecting the power supply, and the unreasonable price informatio n is provided to the user,and effects the user side 's using power mode.

Safety of information transmission . The establishment of communication system of high-speed, two-way, real-time, integration is the foundation for the realization of smart grid. In order to realize the comprehensive and real-timemonitoring, low cost wireless communication network and the widely distributed public Internet will play more and more density in the communication system in smart grid. The multi channel redundant communication network can easily construct through the wireless network and the public Internet , so as to achieve reliable communication. However, a lot of access to public network in power system to provide more entrance malicious attacks, the security of information transmission remains to be further improved.

The safety of intelligent control. From the grid side, intelligent control system can use to collect all kinds of information analysis, diagnosis and prediction of power grid state, and promptly take appropriate measures to adjust the power grid operation state, made it run in safe, reliable and economical state. From the user side to see, home appliances embedded intelligent control technology according to the power state, can automatically adjust the power plan, so as to obtain tangible economic benefits. However, if the lack of security informa tion interaction between intelligent appliances, i t is likely to be exploited by attackers, not only the electrical can not work normally, probably because of a lot of electrical control by the attacker used to form a larger impact on the power grid load.The safety of grid and users interactive environment. A n important feature of the smart grid is to encourage users to participate, realizes the interaction between grid and users. Professional attackers can use interactive process caused greater damage to the power system. For example, through the information network to the user side to release low price information, make a large number of intelligent load all enable cause the system overload,at the same time, through the control of sensor submitted network low load inform ation forged to grid side makes the grid to reduce power supply, thus the stability of power system and electricity security caused great harm.

Impact of information security on network security

From the macroscopic ,The future smart grid will evolve into a complex interaction networks by the information network and the network as the main body . In the event of failure, the internal system of malicious attacks and natural disasters, are likely to lead to collapse, triggering a large area blackout. Therefore, in order to ensure safe operation of power system, not only to control and eliminate the safety hidden danger information elements in power system,then the research from the system integrity system in the perspective of local failure or attack the whole system survivability.

The impact of information security on network security mainly in the following two aspects.

Strong coupling between the network function. On the one hand, the widely distributed information networks need electric power network supply power for its. On the

other hand, realization of power network in almost all functions are needed with the help of information network service. The strong coupling of power network and information network,made the blackout happened more easily. For example,through attack the key nodes of information network, the key electric power network in the corresponding shutdown or important transmission line overload, can cause power node corresponding to the information node failure.

The spread of network fault. In the network of interdependent of the smart grid and the information network, fault propagation form has more possibilities. For the interdependence of two networks, when a node of one network is failure, will cause the failure of other related nodes in a network. With this process occurs in two networks alternately, number of faulty nodes will increase quickly, large-scale network failure, eventually led to the collapse. The concern is, the future smart grid network provides a good platform for the dissemination of fault, the information network is a scale-free network, the power network is a small world network, once the information network of cascading failure, more likely to cause the collapse.

The establishment of information security monitoring system of power network

The smart grid security not only in the physical security of the system, but also includes the security of information system. Because of the importance of information security, more and more domestic and foreign enterprises and organizations began to establish information security monitoring system or information safety monitoring center, the goal is to comprehensively improve information security level. Its main function is to achieve the online monitoring function operation condition information equipment and information system. Based on the on-line monitoring , realize the safety management of information equipment and information system, raise the level of safety information system. Can realize the following functions:

1)Equipment safety management

Information security management equipment, monitoring equipment's state , and carries on the effective management. The basic functions are: ① real-time monitor the running state control information device; the device management tree classification; ● the expression way of equipment management geographic information system; information equipment configuration, maintenance and upgrade management.

2)Real time operation safety management

Real time operation safety management, to monitor the running of the information system, timely response to incident. Basic function: ● operation information to the network nodes as the unit of information acquisition system; ② running state of real-time classification and display systems and network; ③ the timely response to security incidents, the triggering event mechanism security response; ● storage and management of the security event information.

3) Off-line operation safety analysis

Support by the history security information,determining the anticipated security event queue, to develop security measures,security level evaluation. Including the following contents: ● the retrieval and management of safety data; ● analysis of the safety data calculation: determine the safety of the event queue, to develop security measures, the formation of security mechanism, evaluation system safety; ● safety analysis report form.

4) Information safety inspection, certification and evaluation management

The superior power of information security monitoring center has a safety check on information security, lower power enterprises certification and evaluation of power.

5)Daily management

Daily management consists of the following contents: ① user management; ● thesystem configuration management; ● the system log management; ● the safetymanagement system.

The strategy response to information security risk

1)To strengthen the research of information security technology. Information security of smart grid needs from information collection, transmission,processing and exchange to strengthen the protection. Research for the instrument data acquisition and storage intelligent in data encryption storage and transmission.The research on security protocol in wireless network and wired network firewall and security authentication technology.Improve the network and information security early warning, reporting, monitoring and emergency response platform, the formation

of safety protection syst

em effectively.

2)To make the information safety standard system. In the research of foreign relevant safety standards and draw lessons from the advanced research results .At the same time, it should be combined with China's actual situation, the scientific planning of the information security standard system of our country,for guide the development of information security standards system. At the same time, the rea sonable deployment will promote information safety standards in the industry and the implementation .

3)Improve the relevant policies and regulations.The construction of smart grid involve the government, users, power companies, IT companies , equipment manufacturers and other participants. The government needs according to the parties involved in the smart grid in the role to play reasonable policy. Through the policies and regulations, the introduction of the parties should bear the responsibility and obligation , and to formulate appropriate laws and regulations to regulate the behavior of the participating parties, the effective protection of critical information user privacy and the electric power enterprise's safety, the construction and operation of smart grid and orderly, more scientific.

4)The establishment of information security knowl edge. For most of the power user, the awareness of information security is still in the fuzzy state, and as the most number one involved in smart grid, the security awareness will directly affect the overall level of safety operation of smart grid. Therefore,the popularization of the perfect information security knowledge is an important guarantee for improving smart grid information security.

5)To strengthen the study of interdependent n etwork theory. As mentioned before, to grasp the behavior of interdependent networks is the premise to prevent blackouts of future smart grid, so we need to study and solve many key scientific problems. Such as the interdependence of static and dynamic characteristics of the network model,interdependence theory and analysis methods of network fault propagation, interdepend ent network vulnerability,reliability evaluation index system, and combined with the actual situation of modeling and analysis.

References

[1] HU Yan, DONG Ming-chui, HAN Ying-duo. Consideration of information security for electric power industry[J]. Automation of Electric Power Systems, 2002, 26(7):1-4, 12.

[2] LI Wen-wu, WANG Xian-pei, MENG Bo, et al. Theearly study of information security architecture of electric power industry[J]. Electric Power, 2002, 35(5):76-79.

[3] JIA Jing, CHEN Yuan, WANG Li-na. Security andsecrecy for information system[M]. Beijing:TsinghuaUniversity Press, 1999.

[4] DUAN Bin, LIU Nian, WANG Jian, et al. Accesssecurity management of substation automation systemsbased on PKI/PMI[J]. Automation of Electric PowerSystems, 2005, 29(23):58-63.

[5] DUAN Bin, WANG Jian. A security authenticationsystem of substation automation information exchange[J].Automation of Electric Power Systems, 2005, 29(9):55-59.

[6] LIAO Jian-rong, DUAN Bin, TAN Bu-xue, et al.Authentication of substation automation data andcommunication security based on password[J].Automation of Electric Power Systems, 2007, 31(10):1-5.

[7] Taylor C, Krings A, Alves-Foss J. Risk analysis andprobabilistic survivability assessment(RAPSA) : anassessment approach for power substation hardening[C].//ACM Workshop on Scientific Aspects of CyberTerrorism, 2002:1-9.

[8] Oman P, Schweitzer E, Frincke D. Concerns aboutintrusions into remotely accessible substation controllersand SCADA systems[C]. //27th Annual WesternProtective Relay Conference, 2000(4):73-96.[9] Oman P, Schweitzer E, Roberts J. Safeguarding IEDs, substations , and SCADA systems against electronicintrusions[C]. // Proceedings of the 2001 Western PowerDelivery Automation Conference, 2001(1):86-96.

[10] Oman P, Roberts J. Barriers to a wide-area trustednetwork early warning system for electric powerdisturbances[C]. //Hawaii International Conference onSystem Sciences, 2002(1):12-19.

Author's brief introduction and contact information:Rui Wang (1981-), Male, Shanxi province Linfen, graduate students, engineers, electric power quality,power safety and electricity power measurement technology.