Cyber risk analysis and attack verification of key equipment in power grid

Fei Jiaxuan, Shi Congcong, Zhang Rui, Huang Xiuli,
Zhang Xiaojian, Chen Wei and Yang Yi

December 3, 2018

Cyber risk analysis and attack verification of key equipment in power grid

Fei Jiaxuan[1], Shi Congcong[1], Zhang Rui[1], Huang xiuli[1], Zhang Xiaojian[1], Chen Wei, and Yang Yi[2]
1 Global Energy Interconnection Research Institute co. Ltd. State Grid Key Laboratory of Information & Network Security, Nanjing 210003, Jiangsu Province, China.
2 State Grid Jiangsu Electric Power Research Institute, Nanjing 211103, Jiangsu Province, China;
zhangrui@geiri.sgcc.com.cn

Abstract

The normal operation of key equipment in power grid (KEPG) is of great significance for safe and stable operation of power grid. Firstly, this paper gives a systematic overview of KEPG. Secondly, the cyber security risks of KEPG on the main-station / sub-station side, channel side and terminal side are analyzed and the related vulnerabilities are discovered. Thirdly, according to the risk analysis results, three major cyber attack scenarios for key equipment on each side of the grid are proposed, which provides the test process and attack ideas for the subsequent KEPG-related attack penetration. Finally, the simulation environment of penetration test is built, and a series of attack tests are carried out on the terminal key equipment based on the cyber attack scenario proposed in this paper. The correctness of the risk analysis and the effectiveness of the attack process construction technology are verified. The cyber risk and attack scenarios analyzed in this paper are of great significance to enhance the cyber security defense capability of key equipment of power grid.

1 Introduction

With the deepening of the application of advanced information and communication technologies in smart grids [1], the cyber security threats faced by power grids are gradually increasing. The safe and stable operation of the Key Equipment of Power Grid (KEPG) is the key of the safe and stable operation of the power grid [2]. Many large blackouts occur at home and abroad show that the grid still has shortcomings in cyber security protection [3], [4]. In particular, KEPG's ability to resist

[*] the Project of State Grid Corporation of China SGRIXTKJ [2017] 117 (the Identification Method of Malicious Attack on the Power Grid and Active Defense Method on the Power Grid Side）

cyber-attacks is not high enough, and it is urgent to improve cyber security protection [5], [6] to ensure safe and stable operation of the power grid [7].

In recent years, scholars have done a lot of work in the field of grid cyber attacks research. Paper [8] gives the Ukrainian event attack process. The attacker sends the mail containing the malicious macro file to the target host. The macro in file is run and the host is infected by the Trojan horse program, which provides the attacker with a back door, and the attacker uses the back door to attack. The key equipment attack methods in the neighborhood network are studied by paper [9]. These types of attacks use the domain network gateway to attack the sub-station and the power distribution center. The DoS attack is analyzed by paper [10]. The attack mainly exploits the flaws of the protocol vulnerability or software. After the equipment is intruded, it sends a large number of useless requests, occupies resources to block the channel, hinders the information transmission, and affects the normal operation of the power grid. Paper [11] introduced the false data injection attack, which mainly caused the power grid misjudgment by injecting erroneous data, and caused power outage accidents. The above-mentioned research on grid cyber attacks has certain promotion effect of grid cyber security defense. However, the above methods do not systematically mine the vulnerabilities of KEPG, and do not fundamentally analyze the cyber security threats.

In view of the above problems, this paper gives a systematic overview of KEPG, respectively, the main-station / sub-station side, communication side and terminal side of the KEPG risk analysis, and excavated the relevant vulnerabilities. Based on the results of risk analysis, three major attack scenarios of KEPG are analyzed. Based on the risk analysis results and attack scenarios, an attack verification environment is set up to simulate the terminal critical equipment, which verifies the existence of terminal vulnerabilities and the correctness of risk analysis. This study provides a solid foundation for subsequent attack simulation and attack theory research.

2 Overview of KEPG

The key measurement equipment is the equipment that performs data measurement on the vulnerability of the grid measurement configuration. The key to the measurement of vulnerability is that the loss or tampering of the information of the vulnerable point will lead to the loss of availability, integrity and confidentiality of the power system, resulting in voltage collapse or misjudgment of the power grid, endangering the safe and stable operation of the power grid. Cyber risk analysis and attack testing of critical measurement equipment helps to assess the robustness of the measurement system and resist the measurement loss, and finds the vulnerability of the measurement configuration, so as to improve the configuration in a targeted manner. On the other hand, it can guarantee the integrity and authenticity of the measured data and prevent the system from misjudgment.

Critical control equipment generally needs to be identified through a series of evaluation procedures, usually taking equipment with high risk. This paper mainly refers to control equipment that have large cyber security risks, are vulnerable to cyber attacks, and have a significant impact on the safe and stable operation of the power grid. Through cyber risk assessment and testing of key control equipment, it is helpful to discover cyber security vulnerabilities in key control equipment, ensure the normal operation of critical control equipment, and provide strong guarantee for safe and stable operation of large power grids.

KEPG plays an important role in the power grid. The safety and stability of such equipment in the power grid directly affects the security and stability of the whole cyber of the power grid or local power grid. This type of equipment is very easy to become the target of an attacker. It is of great significance to conduct cyber security risk analysis on this type of equipment, exploit its potential vulnerabilities, remediate in time, and improve the resistance of cyber security attacks.

3 Cyber Security Risk Analysis of KEPG

3.1 Main-station / sub-station side risk of KEPG

The main-station / sub-station KEPG mostly uses Linux and embedded operating systems, using MySQL, Oracle data, etc. These operating systems and databases have a certain number of known and unknown vulnerabilities. Once exploited by attackers, it will pose a great threat to the safe and stable operation of the power grid. The risks that these vulnerabilities bring to the main-station / sub-station KEPG are: the risk of illegal exploitation of the operating system; secondly, the risk of the system being injected into Trojans or malware; the risk of illegal exploitation of the database.

Once the equipment operating system vulnerabilities are exploited by the attacker, the sub-station server may be subjected to an overflow attack, and then be privileged, and the Telnet port of the server is illegally exploited, giving the remote workstation trust privileges. There is a risk of tampering in the measurement data of power grid.

In the process of system maintenance or testing, there is a risk that the key equipment of the main-station / sub-station will be injected into Trojan horse program or malicious control software. Once the main-station / sub-station equipment is injected into Trojan horse program or malicious control software, the main-station / sub-station will face the risk of being attacked at any run time.

3.2 Communication side risk of KEPG

There are a large number of measurement equipment on the communication side of the power grid, such as switches and routers, and the switch has more idle ports, and there is a risk of being bypassed. During the system maintenance or testing process, the communication side switch is also the object of maintenance. Once the switch is bypassed, the following risks will occur: the communication message is monitored / cracked; the switch is attacked by DDos.

Once a communication message is listened, the message will face the risk of being parsed. An attacker can obtain the encrypted message, uploaded measurement data and control instructions. Uploading measurement data and forgery control instructions will be faced with the risk of malicious tampering and forgery.

The principle of DDos attack is that attackers use multiple switches to send a large number of useless requests, occupy network channel resources and block channels. As a result, the normal measurement data can’t be uploaded, so that the main station can’t make a correct prediction of the network operation situation risk. In addition, DDos attacks will also lead to the main station, sub-station control instructions can’t be issued in time, the terminal can’t respond to the risk of power grid control strategy in time.

3.3 Terminal side risk of KEPG

The terminal side KEPG generally uses VxWorks operating system, similar to the main KEPG, there are also operating system vulnerabilities. There are mainly the following risks: the risk of malicious attack on equipment functions; the risk of malicious control of communication; the risk of illegal use of ports.

By exploiting key equipment vulnerabilities, an attacker can attack some of the operating functions of the equipment from within the operating system, resulting in abnormal operation of the equipment, such as restarting the equipment when the critical equipment is running normally, resulting in the risk that the equipment can’t run normally.

Using the terminal KEPG operating system vulnerability, the attacker shuts off the communication port of KEPG from the operating system, interrupts the communication between KEPG and the key equipment, sub-station and main station, resulting in abnormal communication transmission. There is a risk of malicious control in communication.

By using the port of the key equipment, the attacker can obtain the related files of the system memory, and then obtain the key memory data, code, equipment parameters, operation strategy of the system, etc. The memory file has the risk of tampered.

4 Scenario Analysis of KEPG Attack

1) Analysis of side attack scenarios at main-station / sub-station

At the main-station side, the attacker tampers with the data uploaded by the KEPG of the main-station / sub-station by exploiting the operating system vulnerabilities, database vulnerabilities and Trojan horse malware injection risks, which results in misjudgment of the power system. Forgery of control instructions will interfere with the normal decision-making of the system, affect the efficiency of system fault self-healing, and expand the scope of the accident. Hijacking the conversation and hijacking the communication between the main station and the terminal will affect the normal decision of the main-station / sub-station.

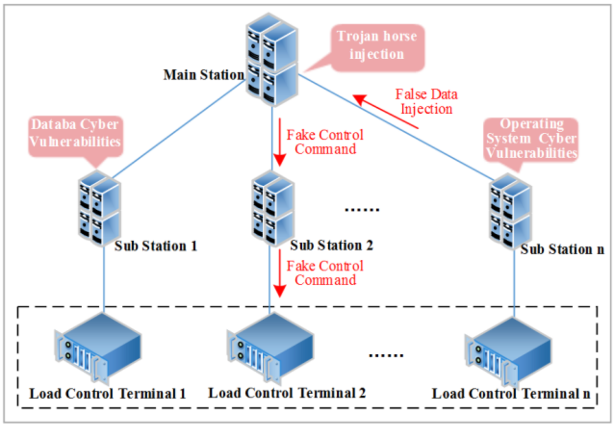


Figure1: Attack scenario of main-station / sub-station side

2) Communication side attack scenario analysis

On the channel side, the attacker listens to / cracks the message of the switch, then tampers with the uplink measurement data, forges the downlink control instructions, and makes the system misjudge and affects the normal decision of the system. By-pass at the switch, DDos attacks are launched to block communication with the main station, resulting in communication interruption, so that the terminal can’t respond to the decision-making of the main station in time, affecting the system failure self-healing efficiency, and expanding the scope of the accident.

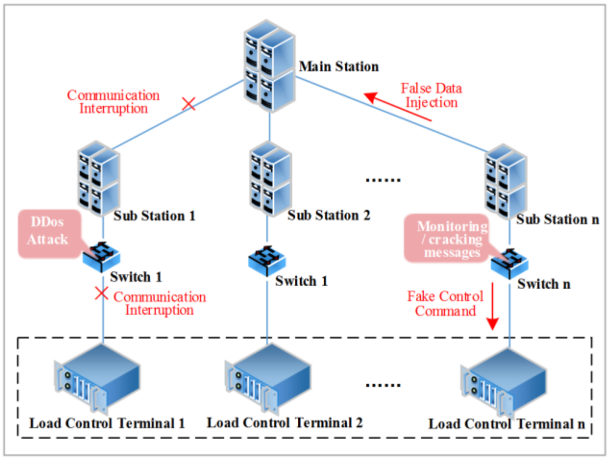


Figure 2: Attack scenario of communication side

3) Terminal side attack scenario analysis

On the terminal side, the vulnerability module of the operating system is exploited to attack the normal operation of the equipment, such as making the equipment cycle restart, locking the main screen, etc. By exploiting the internal vulnerabilities of the operating system, the communication module of the equipment is attacked from the inside of the system, and the communication is turned off from the inside of the operating system, which makes it unable to respond to the power grid decision in time. By exploiting the vulnerability module inside the operating system, we can attack the network memory, modify the memory configuration parameters, configuration strategies and so on, so that the system can't work properly and can't correctly respond to the decision of the main station.

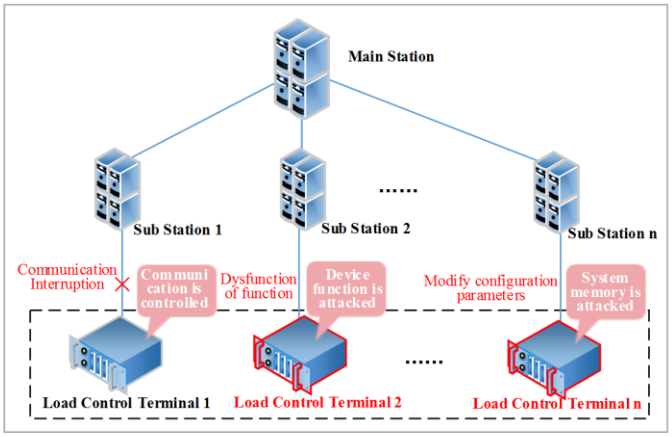


Figure 3: Attack scenario of terminal side

5 Cyber Attack Verification

5.1 Cyber Attack Verification Environment Construction

In order to improve the power grid's ability to deal with cyber attacks and excavate more potential vulnerabilities, based on the above risk analysis results and the attack process constructed, the attack experimental environment shown in Figure 4 is built to verify the terminal's key equipment.

Attack experiment verification environment is mainly composed of RTDS power grid simulation system, load simulation equipment, stability control system and cyber attacks host. The RTDS power grid simulation system is mainly responsible for simulating the real operation state of the power grid and providing the real operation environment for the experiment. The load simulator is mainly responsible for simulating the real grid load. The stability control system consists of two parts, namely the main-station / sub-station control system and the load control terminal. The stability control system is responsible for analyzing the collected voltage, current, flow and other information and issuing instructions to the load simulation equipment. Cyber attack hosts are mainly responsible for launching attacks on distributed load control terminal.

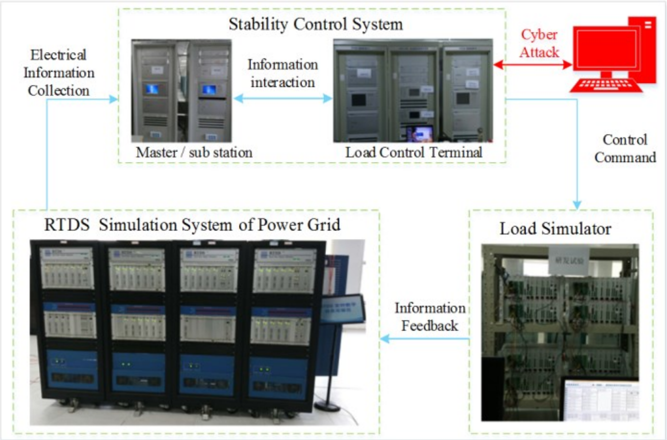
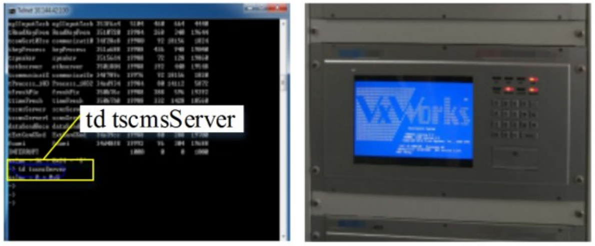


Figure 4: Attack experiment environment for terminal side key equipment

5.2 Attack penetration test

1) Conventional function attack

After invading the stabilization equipment, VMware Workstation is used to launch the equipment restart attack. The attack steps are divided into two steps mainly: the first step is to type the TSCMS server command in the programming interface; the second step is to type the TD TSCMS server command in the programming interface. The attack site and attack effect are shown in Figure 5.

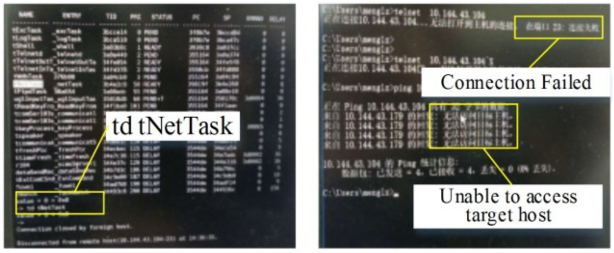


a) Attack scene b) Restart interface

Figure 5: Conventional function attack of stability control equipment

2) Information channel attack

After invading the stabilization equipment, typing the command td tNetTask in the main operation interface can attack the communication port of the stabilization equipment, as shown in Figure 6 a). After successful attack, all communication ports of the stability control equipment can be turned off, as shown in Figure 6 b).



a) Attack code

b) Attack effect

Figure 6: Information channel turn off attack

3) Memory system attack

Connect the stability control equipment, first invade the Telnet remote login port. Then use the Root password to invade the memory system of the control equipment. After successfully invading the memory system, the data of the memory system is changed, and the specific changes of the memory data are shown in Figure 7.

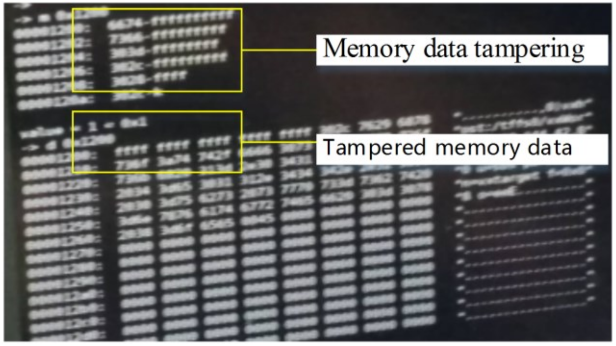


Figure 7: Tamper with stored data attacks

5.3 Attack result analysis

1）Conventional function attack

When an attack is made on the function module of the load control terminal, its function will be seriously affected, and the system will be restarted frequently. Which verifies that the load control terminal has functional protection vulnerabilities, as shown in Figure 5. When the equipment restart attack is carried out, the stable control equipment can't collect the grid operation data, and can't accept and execute the commands sent by the superior dispatching system. During the period of failure and emergency control, the scope of accident impact will be expanded, resulting in significant national economic losses.

2）Information channel attack

After attacking the information channel of the stabilization equipment, the equipment appears the message of "port connection failure" and "unable to access the target host", which verifies the existence of information channel protection vulnerabilities in load control terminal, as shown in

Figure 6. Once the attacker turns off all the communication ports of the stabilization and control equipment, the data collected by the terminal will not be uploaded to the main station, and the main station will not be able to sense the operation status of the power grid in time. The control instruction of the main station can't be sent to the terminal in time, and the terminal can't respond to the main station instruction. Then the grid operation is abnormal, and the power grid is safe and stable.

3）Memory system attack

Once an attacker attacks the equipment's memory, he can modify its memory data arbitrarily, which verifies the terminal stability equipment's network memory protection vulnerability, as shown in Figure 7. In the actual operation of the power grid, attackers can download the system FTP file by using FTP weak password vulnerability. Modify it, such as modifying the main-station / sub-station setting. Or directly forge voltage, current and other data, destroy the normal operation of the stability control equipment, serious cases will lead to blackouts.

6 Conclusion

KEPG plays an important role in the safe and stable operation of power grid, and it is of great significance to improve the cyber security protection capability of KEPG.

After analyzing the network risk of KEPG, it is found that there are loopholes in the operating system and database of the main-station / sub-station, and there are risks of being injected into Trojan horse programs and malware. Information channels run the risk of packets being illegally listened for parsing and being attacked by DDos. Load control terminal functionality, communications, and memory are at risk of attacked.

Based on cyber risk and attack scenario, a series of attack tests were carried out on terminal key equipment. The attack results show that there are certain vulnerabilities in the routine function, communication channel and system memory of the terminal key equipment, which verifies the correctness of the risk analysis. The cyber risk and attack scenarios analyzed in this paper can be used for reference in cyber risk analysis, attack test and vulnerability mining of other KEPGs in the future.

References

[1] TANG Yi, WANG Qi, NI Ming, et al. Review on the Hybrid Simulation Methods for Power and Communication System [J]. Automation of Electric Power Systems, 2015, 39(23):33−42.

[2] DENG Honggui, LUO An, LIU Yanqun, et al. Research On remote Monitoring and Fault diagnosis system for key equipments in power system [J]. Power System Technology, 2003(05):51-54.

[3] LI Zhongwei, TONG Weiming, JIN Xianji. Construction of Cyber Security Defense Hierarchy and Cyber Security Testing System of Smart Grid: Thinking and Enlightenment for Network Attack Events to National Power Grid of Ukraine and Israel [J]. Automation of Electric Power Systems, 2016, 40(8):147−151.

[4] WANG Dong, CHEN Chuanpeng, YAN Jia, et al. Pondering a New-generation Security Architecture Model for Power Information Network[J]. Automation of Electric Power Systems, 2016, 40(2):6-11.

[5] Yamaguchi Y, Ogawa A, Takeda A, et al. Cyber Security Analysis of Power Networks by Hypergraph Cut Algorithms[J]. IEEE Transactions on Smart Grid, 2015, 6(5):2189-2199.

[6] Hu Q, Fooladivanda D, Chang Y H, et al. Secure State Estimation and Control for Cyber Security of the Nonlinear Power Systems [J]. IEEE Transactions on Control of Network Systems, 2017,

(99):1-1.

[7] LIU Daowei, ZHANG Dongxia, SUN Huadong, et al. Construction of stability situation quantitative assessment and adaptive control system for large-scale power grid in the spatiotemporal big data environment [J]. Proceedings of the CSEE, 2015, 35(2): 268-276.

[8] Titcombj. Ukrainian blackout blamed on cyber-attack[EB/OL].(2016-01-05)[2016-05-29].https://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html

[9] Zhang Y, Wang L, Sun W, et al. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids [J]. IEEE Transactions on Smart Grid, 2011, 2(4):796-808.

[10] ZHU Lianggen, ZHANG Yuqing LEI Zhen Jia. Research on DoS Attack and Preventions [J]. Computer application research, 2004(07): 82-84+95.

[11] Zhang X, Yang X, Lin J, et al. On false data injection attacks against the dynamic microgrid partition in the smart grid[C]// IEEE International Conference on Communications. IEEE, 2015:7222-7227.