Information Security of Power Corporations and its Reinforcement Measures

Xiang Yuan 1 You Wang 2 Yang Zhou 3 Zhenxing Qian 4
(1.Zhejiang TaiZhou electric power bureau 2.Zhejiang WenZhou electric power bureau 3.Zhejiang QuZhou electric power bureau 4.Zhejiang HuZhou electric power bureau)
(1.yuanxiang.yx@163.com 2.wang_you@zj.sgcc.com.cn 3.383506383@qq.com 4.qzx111@21cn.com)

***Abstract*—Information system security of power corporations is mainly exposed to physics security risk, network security risk, application security risk and management security risk. The success of information security normally relies on 30% technology support but 70% management investment. Therefore, rigid management plays a crucial role in threat prevention. After a critical summery of the current research on power information system security technology and security management home and abroad, the paper points out a necessary emphasis on information security of production control system and Internet power information system and security management in the future, based on the features and requirements of power information system. First of all, the paper reviews information security and its classification. Then it puts forwards corresponding strategies based on the analysis of various risks, such as network equipment security reinforcement, service security reinforcement, and application security reinforcement. Meanwhile, it gives an introduction of physics security, data security prevention and management regulations.**

***Keywords*—Power corporation; Information security; Network security; Mainframe security, Application security; Data security; Information security management.**

PREFACE

Electric power enterprises is beneficial to the people's livelihood support important industry, but also the earlier realization of production and management of enterprise information. In recent years, with the power of the rapid development of information technology, computer network has been widely used in electric power enterprises in all aspects and achieved good effect, in safe production, energy saving, reduce cost, shorten the construction period, improve labor productivity and achieved obvious economic benefits and social benefits. Can say, the production and operation of power enterprises information network dependence is stronger and stronger, while the enterprise information system security the importance also increasingly protruding comes out now. Electric power information security for power system security, stability, and high quality operation of electric power enterprises, to guarantee the normal production and operation order, ensure the reliable power supply of the society has very important significance. Therefore, how to combine the characteristics of electric power industry and doing well the information security work, should become the current of electric power enterprise is an important content of the work.

CONNOTATION AND RESEARCH DIRECTION OF INFORMATION SECURITY OF ELECTRIC POWER

According to the United States Department of defense [1,2]on information security definition, as well as domestic definition of [3,4,5], electric power information security is to power the main business system and enterprise information security, security from unauthorized access, use and modification, as a legitimate user to provide safe, reliable information service, ensure the confidentiality of information and information systems, integrity, availability, authenticity and non-repudiation.

Power enterprise information security for [6]: the main business system and data security, including financial management system, office automation system, power marketing management system, production management systems, human resources management system, material management system, project management system, foreign website, internal website management information system and business data; network area boundary safety, including the management information area and production control region boundary, management information area and integrated data network (WAN) boundary, access management information region boundary, and Internet access management information region security region boundary security; security infrastructure. Network and infrastructure includes the integrated data network (WAN), management information area network (LAN), room or data center computer room. Specific research directions are as follows:

(1).the production control system, should first study the computational entity security. Production control system using a large number of programmable controller (PLC) mode of operation is the cyclic scanning, and having a large number of input and output interface. In addition, production control system in order to improve the calculation efficiency, the use of digital signal processor

(DSP) and CPU synergistically complete computing tasks. And ordinary PC and server different architecture, makes the control system calculates the entity faces threat to information security and defense in different ways. Secondly, to study the production control system in network security. Production control system using a communication protocol is different from civil network, should be a detailed study of the IEC 60870standard definitions of telecontrol communication protocols used in EMS, DMS and other systems may be encountered in the types of attacks, security protocol security.

(2).interconnected electric power information system, first of all should focus on the different electric information systems between gateway device, including physical isolator, routers and other security, study these gateway equipment penetration test method. The second study in different interest subject, electric power information security infrastructure construction PKI, focuses on the certification body (CA) cross certification. Finally, our country is carrying on the smart grid construction, in order to adapt to the network of flexible structure, realization of reconfigurable information flow, power information system contains information system will be more, coupling also will be more and more closely, must advance research for smart grid strong, flexible, resistant to attack and defense of information interaction platform in the [7].

(3).safety management, first of all should speed up the different types of power information system of interrelated information security standards set construction. Secondly we should study for early warning, protection, decision, response and recovery (wPDRR) process management mechanism, enhance the power information system active defense ability. Finally, to further strengthen the information security risk assessment research, focuses on the assessment of what, how to measure and how to value the problems and risk calculation model of electric power information security, the specific technical layout reasonable and effective.

ELECTRIC POWER INFORMATION SECURITY PROBLEMS

a).Information security awareness of weak [7] .Information security due to the inability to quantify, without the occurrence of major accidents, often overlooked, many units of the network and systems in open state; in addition, the power enterprises IT users because do not know the security threat to the grim situation and the current security situation, in the use of personal computers, networks, application systems only concern is easy to use, ignored safety.

b).information security work not normalized. Information security work to check, such as the SERC, the superior company safety inspection, information safety leading group, the working group only in information security events play a role, did not form a normal working mechanism.

c).information security operation mechanism is not perfect. Is mainly reflected in the business continuity plan is not complete, business development is part of the lack of safety testing and delivery of the test data management, information and document management not standard.

d).short board phenomenon is obvious. Electric power enterprise office geographically dispersed (such as power supply, business hall), different area of IT operation and maintenance (hereinafter referred to as safe operation), the lack of standardized management, information construction in backward areas, as a result of the economic, technical level and other factors, often in the presence of information security short board.

e).system security design defects. Service system construction at the lack of safety design, resulting in System SQL injection, cross accounted for scripting, no detailed audit log, identity authentication information strength is insufficient, the problem such as difference of software fault tolerance.

POWER ENTERPRISE INFORMATION SECURITY RISK ANALYSIS

Power enterprise information security refers to the electric power enterprise information network hardware, software and system data to be protected, not because of accidental or malicious reasons and destroy, change, disclosure, the system for normal operation and reliable, information service interruption. Electric power enterprises with network coverage of the big, big data processing, high security requirements, its safety is a systematic project, must fully consider various safety factors, a comprehensive analysis of the security risk, and then take appropriate safety measures. Therefore, the correct safety risk analysis is a very important link. Current, electric power enterprise information system facing the main risks exist in the following aspects.

(a). physical security risk

Physical security refers to the various servers, routers, switches, workstations and other hardware equipment and communication link security. Sources of risk earthquake, lightning, floods and fires and other irresistible natural events, man-made destruction or incorrect operation, configuration, design, electromagnetic interference, equipment inherent weaknesses or defects. Physical security threats can be a direct result of entire firm system and network paralysis, loss or corruption of data, the loss may be very massive, irreparable.

(b). the network security risk

Enterprise network Unicom for the transfer of information to provide a convenient way. The enterprise

has many applications such as office automation system, power marketing system, distance education and training system, through a wide area network data transmission. At the same time, the electric power enterprises and the government, research institutes and companies have a lot of work, many daily information, data are needed to transmit by internet. Open network vulnerable to various attacks and threats from the outside, may cause network failures, the system of denial of service, information theft, tampering with.

(c). application security risk

Application security refers to the host system software application level security. Most of the application system software without security design of application system software is introduced, which brings convenience to the user at the same time, also gave the network the new threat. The network has become the main means of transmission of the virus, every point of information may be imported without safety factors, such as virus and hacker program, if there is a problem, the consequences will be unbearable to contemplate.

(d). the safety risk management

Electric power information safety biggest hidden danger lies in the management of. Information security management system is not perfect, duty authority differentiates unidentified and lack of maneuverability, can result in safety risk management.

ELECTRIC POWER INFORMATION SECURITY SYSTEM CONSTRUCTION

Information security policy

Information security policy of security decision-making layer shall formulate and conduct propaganda, can be obtained from the provincial power grid dimensions developed company security strategy, the power supply bureau responsible for implementing. Electric power information security strategy should be combined with the national information security grading protection policy, to promote enterprise whole anti-virus, tamper resistant, anti attack, leakage prevention, prevention of paralysis ability as the foundation, combine oneself informatization construction level.

Information security management

Comparison of information security framework, in the electric power enterprise information security management is strengthened urgently, embodied in the following aspects: although established information security management organization, but there is no effective operation; company employees still think that information security is a IT department, including information technology department of the interior part of managers, not establish full awareness of information security; security responsibilities are not clear or fails to perform his duties, the safety management systems ignore; lack of effective safety reporting evaluation mechanism; not to establish risk management control system; information security management system has not formed a plan, implementation, examination, treatment (plan, do, check, action, PDCA) closed loop.

(1).information security organization, should establish security decision mechanism, management mechanism, executing mechanism and supervision mechanism. Safety decision-making body shall provincial Power Grid Corp was established, and at least annually held meeting of job of information security of electric power information security, communications status and Safety Planning Inspector mechanism; enterprise interior each unit can transfer information security business the backbone of the composition, of at least a month to information safety condition for the prosecution and reporting; clear and various information security responsibilities, make safety management organization real work.

(2).the security risk management is to the enterprise residual risk management control, prevention of risk. The implementation of information security risk management process optimization, control changes brought about by the risk, ensure that the risk control, the implementation of annual risk management audit mechanism, the safety inspector institutions risk audit.

(3).the power of information security should be introduced into the PDCA closed-loop management thought, establishing safety supervision and evaluation mechanism and information security evaluation criteria, the information security policies, standards, rules and regulations, the implementation of the measures to check and using information technology means to the analysis of information security situation, constantly optimize the security management process.

Information system maintenance department to system safety risk most clearly, but the operator usually are afraid of responsibility, blame, increased workload, involved in the risk investigation enthusiasm is not high, therefore should mobilize first-line maintenance personnel investigation risk actively, in the information system management and maintenance department to establish the risk mechanism of internal investigation, every month investigation, submit monthly report; safety management and information system management and maintenance departments jointly organized special subject investigation; safety supervising institutions every year compulsory sampling inspection, Department of active investigation, expert of safe prosecution for added safety supervision mechanism.

Safety assessment should be combined with the safety supervision, at least1 times a year, by the unit or organization according to the self-examination self

assessment, followed by the safety supervising institutions according to the assessment results, some departments in the implementation of mandatory sampling inspection, in order to protect the security of the objectivity of evaluation. In addition, according to the safety assessment results briefing and reward.

(4).IT emergency response mechanism is the common problem of no business sector into emergency system, when the information safety accident occurs, will directly affect the production, marketing, office automation, the core business of the normal operation of the system, the system once the paralysis, service sector can only wait for the accident treatment completion. Should establish information with business departments joint emergency response system, enhance the overall enterprise dealing with security incident handling capacity.

(5).the information security management system need to be improved, we should consult international best practice, the establishment of a complete set of system, formed province, ground level two security management system. Power Grid Corp developed information security management level one or two documents, development of information security management requirements and general technical specification; Municipal Power Supply Bureau developed grade three or four files, involving business system operating instructions, operating procedures, information security management rules, clear company safety requirements specific to the implementation.

(6).personnel security information security management process is the most complicated part. First of all, the information construction of electric power enterprise operation relates to internal staff, HS units, developers and other units of staff, often appear overly dependent on external cooperation unit, external assist personnel access control is insufficient, the developers admission deployment, test part of the lack of control a problem. Secondly, personnel safety consciousness is weak, the surface of information security seriously, it is a safe T formality. Moreover, part of the unit staff technology level is insufficient. Therefore, in the personnel security, should develop external assist units, developers management approach, emphasizing external personnel access, operation authority approval, recycling; carry out warning education, establish the full participation of information security environment, especially to improve the leadership in the face of information security awareness; each unit to conduct regular technical training, and in pre - technology assessment, execute technical personnel to hold card mount guard.

Information security operation

Information security of electric power operation is established through the operation technical specification, operation and maintenance instructions, operation and maintenance process, operation and inspection standards or mechanism, ensure that on the basis of environment, software and hardware platform, the main business system, safe operation and maintenance terminal.

(1).infrastructure includes computer room, office environment, IT equipment, should establish the infrastructure or equipment operation and maintenance process of technical specifications, work instructions, process. Contents include: clear computer room equipment and supporting the regular inspection, safety inspection, access control, access control security, operating norms; designated infrastructure or equipment management responsibility and the maintenance repair, normative foundation facilities or equipment access permissions, application and approval, to recover the process and procedures.

(2).hardware platform, should establish a daily operation examination, configuration management, change management, performance management specification; specific hardware platform, running state of health examination, log inspection T; various hardware devices (such as a server, network equipment configuration specification), including configuration, port access control, network connection maintenance records, ensure the completeness and correctness of the establishment of various types of hardware equipment; the user management, including user registration, account, operation, and security audit.

(3).software platform should be established, operating system, database, middleware platform such as El often maintenance check, configuration management, change management, specification, detailed database backup and recovery plan, regular recovery drill; clearly defined software platform running state health examination, log check T as operating system, developed to include; database, middleware, application and domain management, anti-virus system system configuration specification, account management, log management standard specification for.

(4).normative business system operation process, including the system change, maintenance, testing and management process, improve the application service of the correctness and reliability of system operation; to establish business management requirements, specific application system maintenance duties and working content, including El regular maintenance, adaptability and corrective maintenance, maintenance; building clear business system change process, including the change of business functions, business data to update records, change data, realize the maintenance work of traceability.

(5).terminal includes a personal computer and office should establish self-service terminal, terminal desktop security configuration standard, build unified domain

management, developed terminal equipment operation, improve the terminal operation safety.

Information security technology measures

Identity authentication and access control through the public key infrastructure (public key infrastructure, PKI) technology for unified management, establishment of province level authentication center, providing directory services, identity management, certificate management, access management function. The realization of the host system, network equipment, security equipment, application system of unified identity authentication management.

On the marketing, finance and other systems in the confidential data, should be used for encryption and decryption, digital signature, message authentication code and other means of protection, improving the system service and data access non-repudiation. At present, most of the communication process of electric power enterprise system did not take security measures such as encryption, digital signature, and the enterprise network did not implement effective access control, the electric power information security cause huge risk, must as soon as possible through various information confidential attribute, overall planning, on the application of the system upgrade, and implementation of intranet access mechanism.

Power management information network should be set up within virus prevention, detection, isolation and removal mechanism, prevention of unknown viruses, rapid isolation of infected hosts, identify and remove network known virus.

Reinforcement refers to information system security field protected object for their own safety reinforcement protection, mainly including the network equipment security, server security, application security reinforcement reinforcement.

Network equipment security reinforcement

1.isolation: intranet network prohibited the use of the following radio equipment: wireless router, wireless AP; should develop information intranet network terminal access management rules, should have access to perform internal terminal application and approval procedures; supreme network records, external terminal supreme network record; substation, the business should not present a terminal communication link together situation; room should not exist for the communication link using a dialing device.

2.structural safety : should keep in line with the latest operation network topology map; important network link and network equipment should achieve redundancy; should be a separate build server and desktop terminal domain domain.

3.Access Control: reasonable configure firewall access control policy, there is no useless, repeat, ineffective strategies, it is strictly forbidden to all ports of the network equipment or open; should enable routing ACL control strategy.

4.security audit : the network management system should be able to record the running state of the equipment, network traffic, user behavior and other important events; the important network and security devices such as firewall, audit records, IDS, core, server access, should be dedicated log server unified audit, important log should be maintained for more than 6 months.

5.invasion guard: in the network boundary should deploy IDS or IPS anti-intrusion device; intrusion device coping two tier server domain and desktop systems domain monitoring; rational allocation of IDS or IPS strategy.

6.The network equipment protection: check whether the user name password authentication; whether the configuration of AAA certification; should configure device only allows network administrators login; network equipment remote login should be used when the SSH security communication link; close the network equipment source routing protocol, CDP service, keeplive service, BOOTP service; check device configuration file password whether the encrypted password, equipment application seals a person responsible for the preservation of equipment has a corresponding; password complexity, figures and letters of more than 8; the SNMP should not use Public, Private default field.

Host security reinforcement

1.equipment has a corresponding authentication password complexity, figures and letters of more than 8, from the same user name and password, password application equipment seal has special responsibility for preservation; should open screen saver password protection function; SSL shall be used for remote management of encrypted; should set a password complexity requirements, set strategy system user minimum password length is 8, check the password must meet complexity requirements, set a password is used for a period of 60days should be the allocation of account five failed login lock, lock 30 minutes each time.

2.access control : no default sharing (IPC$, C$, D$...); shut down unnecessary default account, the system default account to rename, disable the GUEST account, should not exist useless account.

3.security audit: audit policy change, in response to event log, system events, account login events, account management and project; in the event viewer to access to the related events of the time, the main object identity and event results and other information.

4.intrusion prevention: should stop unnecessary services such as Alerter, Clipbook, Computer (Browser, Fax Service, Internet Connection Sharing, IndexingService, Messenger, NetMeeting Remote Desktop Sharing, Network DDE, Network DDE DSDM, Remote Access Connection Manager, Routing and Remote Access, Simple Mail Transport Protocol (SMTP), Task Scheduler, Telnet etc); in the network security device (a firewall or network equipment such as 1391413445) in limiting virus vulnerable port.

5.prevention of malicious code inside, outside the host should install anti-virus software.

6.resource control system to respond to the management of the IP address and access restrictions; the remaining disk space should be greater than 30%.

Application safety reinforcement

1.application of identity authentication system provides the user login module, requires the user to input a username and password for authentication, public information release system, the backstage management function to provide login module; system in tried many times (5) after a failed login, should end the session or lock account, not allowed to log in for at least 10 minutes, system for login failed times and login failure time configuration; system should not allow duplicate identification, such as multiple users using the same username; forced the user first logs on to the system to modify the distribution of initial password, the system should provide the password complexity check function.

2.application of access control system provides authority management module, authority management to set user, user groups, such as the main role of the Tim censored search changed data access; access control scope shall cover all users, will not allow the existence of authority control is absent, access control should be refined to Tim censored search to a variety of operations; the system should not present a temporary or test account, create new accounts, accounts for a low initial access permissions; system should at least set system administrator, general business users and Security Auditor three roles, the system administrator, general business users and Security Auditor three role should be separate, exclusive and minimization.

3.security audit system to provide secure audit, audit information should be covered on each user's operation; audit information should be only Security Auditor role can access, should cover the user management, authorization management, safety parameter modification, audit log, login logout business operations; audit content includes at least: event time, user ID or username user operating a client, IP, a content of the event (the user operation content) and outcome (success or failure).

4.The communication secrecy : the application of system in the process of communication for the sensitive field (such as the password field) should take the encryption transmission.

5.application of software fault tolerance and intrusion prevention system should not exist, cross-site vulnerability, upload script injection vulnerability.

6.resource control application system should have the login timeout exit function; the same user cannot repeat login.

Monitoring and auditing can improve the security of information, improve the problem occurs when the reaction speed, effectively prevent safety problems occur. Should undertake unity planning, the establishment of IT monitoring platform. The Guangdong power grid and provincial Power Grid Corp have begun implementation of monitoring platform construction.

Backup and recovery technology mainly includes the backup, redundancy, fault-tolerant and uninterruptible power supply protection4 aspects. Backup recovery and disaster recovery center is related, establish a disaster recovery center unit should be at least once a year of disaster backup and recovery training, no disaster recovery center unit should be marketing, production, finance and other core data regular off-site backup, and regular backup and recovery training, improve their ability to deal with natural disasters.

THE END

Information security of electric power production and business management are closely related, but because the information security can not be quantified, a lot of information security work flow easily at the form or busy. Information security work mostly without normalization, systematization. The power enterprises should be fully aware of the serious situation of information security, to develop enterprise information security policy, unified planning security system. This paper analyzes the common power enterprise information security risk, expounds the power information security system framework and key points in construction, the electric power enterprises in the planning and construction of security system, we must analyze the enterprise informatization construction stage, combined with their own situation, step-by-step implementation, to ensure electric power information system security, reliable, stable, and efficient operation.

REFERENCE

[1] Luo Jianjun bank IT security architecture [J] Journal of Wuhan University of Science and Engineering,2008,21(12) :37- 40.LUO Jian-jun. Study on the Architecture of Banking IT Safeguarding[J] Journal of Wuhan University of Science and Engineering (18,20,21(12) : 37-40.

[2] Binxing safeguard national cyberspace security [J] information and communication security .2001(6) :9- 12.FANG Bin Xing Ensuring the Security of National Cyberspace[J].China Information

Security,2001(6) :9-12.
[3] Zhao Ling, Liu Jianhua telecommunications network information security model based on [J] two University of Posts and telecommunications,2009,14(3) :11,14.ZHAO Ling, LIU Jian-hua Research on Inform ation Security Assurance Model in Telecommunication Network[J].Journal of Xi ' an University of Post and Telecom,2009.14(3) ::11 - 14
[4] Wang Na, Katahama Oki, Luo Jianzhong, and other"5432 strategies": towards the national information assurance framework [J] Journal on communications,2004,25(7) :1,9.WANG Na, FANG Bin Xing, LUO Jian Zhong, et a1."5432 Strategies" towards the National Information Assurance: Framework[J] Journal of China Institute of Communications,2004. 25(7) :1-9.
[5] Shen Changxiang on strengthening information security assurance system [M] Wuhan: Hubei science and Technology Press,2002.SHEN Chang-xiang Thoughts on Strengthening Information Security Assurance System [M] Wuhan:Hubei ScientificTechnical Press,2002
[6] just Jun, Zhang Xuesong, Guo Zhizhong of electric power information security monitoring and analysis [J] power system technology,2004.5(9),5053.GANG Jun.ZHAN G Xue-song, GUo Zhi-zhong.Monitoring and Analysis of Electric Power Information Security[J]Power System Technology,2004,5(9) :50-53.
[7] Zhang Xiaofei, Jane Zhu. Discussion on information security of electric power [J] computer security,2009(4) :89,93.ZHANG Xiao-fei, ZHU Jie Discussion of Security of Electric Information[J] Computer Security,2009(4) ::89 - 93
[8] Hu Yan, Dong ming-chui, Han Yingduo. Power industry information security [J]. automation of electric power systems,2002,26(7) :1-4,12.HU Yan, DONG Ming-chu, HAN Ying-duo.Consideration of information security for electric powerindustry[J].Automation of Electric Power Systems,2002,26(7) : 1-4,12.
[9] Li Wenwu, Wang Xianpei, Meng Bo, et al. The power industry information security on the system structure of [J]. China electric power,2002,35(5) :76-79.LI Wen-WU, W ANG Xian-pei, MENG Bo, et a1.Theearly study of information security architecture of electric power industry[J] .Electric Power,2002,35(5) ::76 - 79
[10] Jia Jing, Chen Yuan, Wang Lina. The security and confidentiality of information systems [M]. Beijing: Tsinghua University press,1999.JIA Jing, CHEN Yuan, W ANG Li.na.Security and secrecy for information system[M].Beijing.Tsinghua
University Press,1999
[11] Duan Bin, Liu Nian, Wang Jian, et al. Based on PKI / PMI substation automation system access security management [J]. automation of electric power systems,2005,29(23) :58-63.DUAN Bin, LIU Nian, ANG Jian, etⅥ, a1.Access security management of substation automation systems based on PKI / PMI[J].Automation of Electric Power Systems,2005,29(23) :58 63
[12] Duan Bin, Wang Jian. Substation automation information exchange security certification system [J]. automation of electric power systems,2005,29(9) :55-59.DUAN Bin, WANG Jian.A security authentication system of substation automation information exchange[J].Automation ofElectric Power Systems,2005,29(9) :55-59.
[13] Liao Jianrong, Duan Bin, Tan Buxue, etc. Based on password authentication data and communication security of substation [J]. automation of electric power systems,2007,31(10) :1-5.LIAO Jian-rong, DUAN Bin, TAN Bu-xue, et a1.Authentication of substation automation data and communication security based on password[J].Automation ofElectric Power Systems,2007,31(10) :1-5.
[14] Liu Nian, Zhang Jianhua, Duan Bin, et al. Substation automation communication system under the environment of network vulnerability assessment [J]. automation of electric power systems,2008,32(8) :28-33.LIU Nian, ZHANG Jian-hua, DUAN Bin, et al.Vulnerability assessment for communication system of network-based substation automation system[J].Automation ofElectric Power Systems,2008,32(8) :28-33.
[15]Taylor C, Krings A, Alves - Foss J.Risk analysis and probabilistic survivability assessment (RAPSA) :an assessment approach for power substation hardening[C].//ACM Workshop on Scientific Aspects of Cyber Terrorism,2002:1-9.
[16]Oman P, Schweitzer E, Frincke D.Concerns about intrusions into remotely accessible substation controllers and SCADA systems[C].//27th Annual Westem Protective Relay Conference,2000(4) :73-96.
[17]Oman P, Schweitzer E, Roberts J.Safeguarding IEDs, substations, and SCADA systems against electronic intrusions[C].//Proceedings of the 2001Western Power Delivery Automation Conference,2001(1) :86-96.
[18] Wu Guowei digital substation information processing and network security analysis [J]. relay,2007,35(12) :18-22.WU Guo.wei.Information disposal and netw ork securityanalysis in digital substation[J].Relay,2007,35(12) :18-22.
[19]IEEE PSRC CI Working Group.Cyber security issues for protective relays[C].//IEEE PES General Meeting,2007:1-8.
[20]Allen Risley, Jeff Roberts, Peter Ladow.Electronic, security of real-time protection an d SCADAcommunications[C].//5th Annual Western Power Delivery Automation Conference,2003:12 - 37

Xiang Yuan(1982.10-), male, engineer, master of science, information system construction and operation in Zhejiang Province, Taizhou city Linhai Lucheng Road No. 278,317000,13676658261, Email:yuanxiang.yx@163.com.

You Wang(1985.12-), male, assistant engineer, Bachelor of engineering, information system construction and maintenance, Wenzhou city Lucheng District Fairview road Electric Power Mansion,325000,15888743377, Email:wang_you@zj.sgcc.com.cn.

Yang Zhou(1986.10-), male, assistant engineer, Bachelor of engineering, information system construction and maintenance in Quzhou City, Zhejiang province New River along the No. 6,324000,13957039312,Email:383506383@qq.com.

Zhenxing Qian (1981.04 -), male, engineer, Bachelor of engineering, information system construction and operation, the Zhejiang province Huzhou city of Phoenix Road No.777,313000,13511220899, Email:qzx111@21cn.com.