Network Security System and Implementation Scheme of Information Infrastructure in Geological Prospecting Industry

Feihu Huang1,*, Wei Huang2,a
1Information Center. Tibet Autonomous Region Geological and Mineral Exploration and Development Bureau, Lhasa 850000, China
2State Key Laboratory of Mechanical Transmission, Chongqing University, Chongqing 400030, China

*Corresponding author e-mail: 370162517@qq.com, ahuangwei_smile@126.com

Abstract. This paper analyzed the construction requirements of the network security of information infrastructure in the geological prospecting industry, and proposed a network security system of information infrastructure for the geological prospecting industry, including physical security, network communication security, computing environment security, regional border security and security management. With the weak infrastructure of the industry units and the lack of operation management system, the overall solution for the network security construction of information infrastructure for the geological prospecting industry was proposed. Based on the constructed information security system and the overall solution, a typical network security implementation scheme of information infrastructure for the geological prospecting industry units is proposed.

1. Introduction
Since the Eighteenth National Congress of the Communist Party of China, General Secretary Xi Jinping has made a series of important speeches on network security and informatization. He has put forward a series of new ideas and new judgments such as "without network security, there will be no national security, without informatization, there will be no modernization" [1], which points out the direction for the healthy development of China's network and telecommunications undertakings. On the basis of this opportunity, the internal and external environment faced by the geological prospecting industry has undergone tremendous changes. The informatization construction will be an important means and foundation for the future fine-grained management of the geological prospecting industry. At present, the informatization infrastructure of the geological prospecting industry is weak, the shortage of professional and technical personnel, and the level of informatization are still very backward. To cope with the overall development strategy of the geological prospecting industry, and to clarify the development direction, goals and priorities of the future informatization construction, it should be actively and steadily to promote the information construction. With the deepening of the informatization construction of the geological prospecting industry, the network security of information infrastructure is one of the primary problems [2-5]. It is of great practical significance and guiding
significance to study the network security of information infrastructure for the geological prospecting industry.

Domestic and foreign scholars have conducted in-depth research on industry information security issues. Wei et al. [6] proposed an information security risk assessment model for privacy considerations. Singh et al. [7] studied the use of watermarking technology in the health care field to solve health data management problems. Li et al. [8] applied intrusion detection technology to blocks Chain information security model. Takahashi et al. [9] proposed a mechanism for linking, locating and discovering various network security information. Thomas et al. [10] proposed a deep structural framework for information system security. Liu et al. [11] established a factor model for information security evaluation using factor space theory. Ding et al. [12] constructed an energy blockchain security protection system; Yang et al [13] proposed a situation assessment method based on fuzzy dynamic Bayesian networks. At present, industry information security research mainly focuses on the research of specific industry problems, and lacks systematic consideration of information security issues in the geological prospecting industry, and it is difficult to meet the information security needs in the geological prospecting industry. Based on the network security domain division and construction requirements of the geological prospecting industry, this paper constructs a network security system of information infrastructure for the geological prospecting industry. Finally, a typical information security implementation scheme of information infrastructure for the geological prospecting industry is given.

2. Network Security Requirements of Information Infrastructure in Geological Prospecting Industry

2.1. Network Security Domain of Information Infrastructure in Geological Prospecting Industry

The security domain is divided according to the level protection requirements, information nature, usage subject, security objectives and policies, and is a collection of network entities with similar security attribute requirements.

A security domain can be further divided into security subdomains, and the security subdomains can be further refined into secondary security domains, tertiary security domains, and the like. Security requirements between security domains of the same level include two aspects: isolation requirements and connection requirements. The isolation requirement corresponds to the security services such as identity authentication, access control, non-repudiation, and auditing at the network boundary; the connection requirements correspond to security services such as confidentiality, integrity, and availability during the transmission process. The subordinate security domain inherits the isolation and connection requirements of the superior security domain.

Figure 1. shows the network security domain partitioning of information infrastructure in the geological prospecting industry, including the shared platform area, the one-way security switching platform, the unit internal security domain, the branch office security domain, the border security access domain, the core switching domain, the business service domain, the security management domain, and the external network user access domain.

Shared Platform Area includes a database server, a file server, and a business system to implement unified management of data and files.

One-way Security Switching Platform implements the function of one-way isolation and information one-way introduction system (one-way shutter) to ensure data security.
Fig 1. Network security domain division of information infrastructure in geological prospecting industry

Unit Internal and Branch Office Security Domain refers to the security domain defined by the terminal access user and the wireless terminal access user. It is the network security control to realize the data interaction between the internal and branch network equipment and terminals through the firewall and the core exchange domain.

Border Security Access Domain provides the security domains defined by border secure access according to central services, such as routers, next generation firewalls, intrusion protection, etc.

Core Switching Domain provides the network security domain of core switching among other regions. Its core switch bears and aggregates all the traffic of the unit. It has the characteristics of high reliability, high efficiency, high fault tolerance, manageability and low latency, and guarantees the continuity of the whole business system.

Business Service Domain refers to the security domain that provides office business system and production business system.

External Network User Access Domain refers to the security domain defined by the security access of outgoing personnel, personnel outside the unit, etc.

Security Management Domain refers to the security domain defined by the system server providing security management, such as fortress machine, network audit, intrusion detection, IT monitoring, anti-virus and other functions.

Among them, sub-security domains can be divided into finer-grained security domains according to different physical locations, and the same-level security domains adopt the same-level security protection measures.

During the construction of the information infrastructure network security, the phenomenon that multiple security systems require different service systems to share one server should be avoided. Different levels of application systems should be deployed separately to avoid problems and hidden dangers caused by security protection of the corresponding service systems. In this case, in order to protect the service system with high security level protection requirements, stricter security access control measures and other related security policies will be set up, but access to the business system that may cause low security level protection requirements may be affected at this time, such as the related service system ports are restricted. In actual implementation, in order to ensure the normal operation of the service system, security access control measures required for low security level protection must be implemented, which brings great security risks to the system. In practice, according
to different security level protection requirements of each business system, the same level business system is deployed to the same server or an area, and security protection is carried out according to the planned security area to ensure the security of the system and the reliable operation of the business.

2.2. Characteristics of Network Security Requirements for Information Infrastructure in Geological Prospecting Industry

From the division of network security domain of information infrastructure in geological prospecting industry, it can be seen that the network security requirements of information infrastructure in geological prospecting industry have the following characteristics:

2.2.1. Moderate security: No information system can achieve absolute security. In the planning of information security grade protection in geological prospecting industry, it is necessary to balance and compromise security requirements, security risks and security costs. Too many security requirements will lead to the rapid increase of security costs and the complexity of operation.

Moderate security is also the original intention of level protection construction. Therefore, in the process of designing grade protection, on the one hand, we must strictly follow the basic requirements, and strengthen protective measures from the network, host, application, data and other aspects to ensure the confidentiality and integrity of information systems. On the other hand, from the perspective of comprehensive cost, the corresponding protection strength should be proposed for the actual risk of the unit information system, and the design and construction of the security protection system should be carried out according to the protection strength, so as to effectively control the cost.

2.2.2. Key protection: According to the importance degree and service characteristics, the information system with different security protection levels is divided to achieve different levels of security protection, and the centralized resources are prioritized to protect the information system involving core business or key information assets; this program will focus on protection in the design. Geological prospecting industry units involve information systems related to key businesses, and other information systems reduce the level of protection for general design and protection.

2.2.3. Pay equal attention to technology and management: Information security issues have never been a mere technical problem. It is one-sided to understand the prevention of hacking and virus infection as information security issues. It is difficult to completely cover all information security issues in the industry by simply deploying security products. It is necessary to combine technical measures and management measures to more effectively guarantee the overall security of the unit information system of the geological prospecting industry.

2.2.4. Sub-divisional domain construction: An effective method for security protection of information systems is to partition the domain. Since the importance of each information asset in the information system is different and the access characteristics are not the same, it is necessary to gather information assets with similar characteristics for overall protection. Therefore, the effectiveness and consistency of the security policy can be better ensured, for example, the business servers are centralized and isolated separately, and then isolated and accessed according to the access requirements of each business department; and the partition domain also helps the network system. Centralized management, once security incidents occur in some of the security zones, can be spread across the network through strict border security protection.

2.2.5. Standardity: The information security protection system of the geological prospecting industry units should consider the conformity with other standards at the same time. The technical part of the plan will be designed with reference to the IATF security system framework. In terms of management, reference is also made to the 27001-security management guide to make the post-built level protection system. More extensive practicality.
2.2.6. Dynamic Adjustment: The information security problem is not static. It always changes with the organizational policy, organizational structure, information system and operational process related to the geological survey industry unit management. Therefore, it is necessary to track the changes of the information system and adjust the security protection measures.

2.2.7. Scientific nature: The design of the scheme is based on the security assessment of the geological surveying industry units. In terms of threat analysis, vulnerability analysis and risk analysis, it is based on the objective evaluation and the results of the analysis are carried out. Therefore, the measures and strategies of the scheme design can meet the relevant requirements of national level protection on the one hand, and can also solve the security problems existing in the unit’s information network of the geological survey industry on the other hand, and meet the characteristic requirements.

3. Network Security System of Information Infrastructure in Geological Prospecting Industry

In order to implement the security requirements of the secondary system in GB 17859-1999 and meet the security requirements of the five basic attributes of the secondary system in autonomous access control, identity authentication, passenger weight, auditing, and data integrity, Figure 2 shows the framework of the secondary system security protection environment construction of the geological prospecting industry.

3.1. Physical security

3.1.1. Physical location and computer room environment: a) Physical location selection according to the basic requirements of the secondary requirements. b) Renovation of the built machine room site in a building with the ability to prevent earthquakes, wind and rain. The machine room site is not on the second floor of the building or in the basement. c) Waterproof and dustproof paint on the wall and top.

3.1.2. Room management: a) A person or department is responsible for the maintenance of the equipment room facilities. b) Develop computer room maintenance records. c) Complete record content, maintenance date, maintainer, maintenance equipment, cause of failure, maintenance results, etc. d) Special department is responsible for the security management of the machine room. e) Develop job responsibilities document to describe the room security responsibility department and job responsibilities. f) The system has relevant content for managing the confidentiality of the office environment and regulating the behavior of personnel. g) Management content, including staff leaving the post management, visitor management, terminal desktop security management, etc.

3.1.3. Equipment maintenance management: a) Designate special personnel or specialized departments to carry out regular maintenance on various facilities and equipment. b) The responsible department of equipment maintenance management is clearly specified in the department or personnel job responsibilities document. c) Establish equipment security management system. d) The system covers a comprehensive range, including the management regulations for all aspects of equipment selection (selection, procurement, issuance, etc.). e) Recording and approval process for equipment selection, procurement, and distribution. f) Develop an operation manual for devices such as terminal computers, workstations, portable computers, systems, and networks. g) Equipment should be removed from the equipment room. Retain approval record.
3.1.4. Media management: a) The media storage environment is safe and managed by a dedicated person. b) There is a clear definition of media security transmission in the media management system. c) Physical transmission of media selects reliable transmission personnel and selects a secure physical transmission path. d) Registration management records for media use, and the recorded content is complete. e) The archive media is regularly counted. f) Purify the data before destruction. g) Formulating a medium security management system includes a method of strictly managing the use of the storage medium, sending out maintenance, and destroying, and a method of encrypting, monitoring, and managing the storage medium that brings out the working environment. h) Approved by the leader before the destruction of the medium with high confidentiality. i) Recording of repair, take-out or destruction of the storage medium. j) Data and software encryption in important media. k) The importance of the medium is marked in accordance with the regulations.

3.2. Communication network security

3.2.1. Network Architecture: a) The processing capacity of the main network equipment and the bandwidth of each part must meet the peak demand of the service. b) Deploy optimization equipment, reduce network traffic, and better meet redundancy requirements. c) Reasonably planning the route and establishing a secure path between the service terminal and the service server. d) Plan important network segments and configure ACL policies on the routing switch to isolate them. e) The network device plans the bandwidth priority to ensure that important hosts are preferentially protected when the network is congested.

3.2.2. Security audit: Deploy network intrusion detection system, record intrusion behavior and alarm, and reinforce the system through security reinforcement measures according to basic requirements.
3.2.3. **Border protection:** Access and data flows across the boundary are communicated through a controlled interface provided by the border protection device.

3.2.4. **Communication transmission:** Using check code technology to ensure data integrity in communication.

3.3. **Computing environmental security**

3.3.1. **Identity authentication:** a) Application system development application audit function, record the date, time, initiator information, type, description and result of important security events of the system according to the basic requirements, and protect the audit results. b) With the login failure processing function, you should configure and enable the end session, limit the number of illegal logins, and automatically exit when the login connection times out. c) When using VPN technology for remote management, prevent authentication information from being eavesdropped during network transmission.

3.3.2. **Access control (Regional boundary security):** a) Configuration of access control according to basic requirements, including: permission definition, authority management of default account, determination of control granularity, etc. b) Develop strict user rights policies through security hardening measures to ensure that accounts and passwords comply with security policies. c) Develop an ACL policy that meets the basic requirements through the firewall.

3.3.3. **Software fault tolerance:** a) Perform code review and check the input data to ensure compliance with regulations. b) Implement cloud failover using cloud products.

3.3.4. **Security audit (Regional boundary security):** a) Application system development application audit function, record the date, time, initiator information, type, description and result of important security events of the system according to the basic requirements, and protect the audit results. b) Deploy an audit system pair, the record should include the date and time of the event, the user, the type of event, the success of the event, and other audit-related information. c) Protect the audit records and back them up regularly to avoid unexpected deletions, modifications or overwrites.

3.3.5. **Intrusion prevention (Regional boundary security):** a) The principle of minimum installation of the system, only the required components and applications are installed. b) Unneeded system services, default shares, and high-risk ports should be turned off. c) The management terminal managed through the network should be restricted by setting the terminal access mode or network address range. d) It should be able to identify possible vulnerabilities and fix the vulnerabilities in time after thorough testing and evaluation.

3.3.6. **Malicious code prevention:** Deploy terminal anti-malware software, update and update in time; perform vulnerability scanning and timely update system patches.

3.3.7. **Data backup recovery:** Regularly back up important data according to basic requirements; use cloud backup technology to back up important data in different places.

3.3.8. **Resource control:** Limit the maximum usage limit of system resources by a single user or process.

3.3.9. **Data integrity and confidentiality (Regional boundary security):** Check code technology is used to ensure the integrity of important data in the transmission process.
3.4. Security management

3.4.1. Management System: a) Develop a separate overall information security policy document or other relevant management documents covering the overall policy requirements of information security, including the objectives, scope, principles, and framework of information security. b) Formulate and improve the management system, including all aspects of information security management system, management system should include but not limited to physical, network, host, data, application, management and other aspects of management content.

3.4.2. Post setting: a) Establish an information security management function department. b) Establishing positions of responsible persons in all aspects of security management and security management. c) Define the responsibilities of each responsible person. d) Set up system administrators, network administrators, security administrators and other positions. e) Define the responsibilities of each job.

3.4.3. Staffing: a) The number of system administrators, network administrators, and security administrators equipped with the system meets the requirements of business needs and mutual constraints. b) Equipped with a full-time security administrator.

3.4.4. Password management: a) Established a password usage management system. b) The password usage management system covers product or technology selection, procurement, authorized use, daily maintenance, disposal and another lifecycle management. c) The password technology and products have certificates issued by the national password authority.

3.4.5. Network and system security management: a) Designate a person or department responsible for maintaining the network. b) Formulate the responsibility document for the network security management role, including the daily maintenance of the log and network monitoring records and the analysis and processing of the alarm information. c) Established a network security management system. d) The content of the network security management system covers network security configuration, log storage time, security policy, upgrade and patching, password update cycle, etc. e) Keep the current software used as an updated version. f) The working record of the software version upgrade indicates that important content has been backed up before the upgrade. g) Have a network vulnerability scan report, describing the system's vulnerability, severity level, cause analysis and improvement opinions. h) Have a document record that fixes the discovered vulnerability. i) Network equipment inspection is configured according to the minimum service principle. j) The network device does not open the redundant service port in the vulnerability scan test result. k) The configuration file performs remote backup data. l) Regular remote backup configuration work records. m) All external connections have an authorization approval record. n) Regularly check the work records of illegal networking.
4. A Typical Information Security Implementation Scheme of Information Infrastructure in Geological Prospecting Industry

The geological prospecting industry units will plan and construct an information system security assurance system to better support the application and business development in accordance with the requirements of information system level protection. Figure 3 shows a typical information security implementation of information infrastructure in geological prospecting industry. The details are as follows:

(a) Information System Security Status Analysis: According to the established information system protection level, referring to relevant requirements or standards, the system status and security risks are analyzed, and the security construction requirements of hierarchical protection are obtained.

(b) Information System Security Construction Scheme Design: According to the third-party evaluation organization's network security inspection results and rectification suggestions, based on the security requirements analysis results, combined with relevant technical specifications, and the user's real business, prepare a unit information infrastructure network security rectification construction scheme for guidance to network security rectification and construction work.

(c) Network Security Construction of Information Infrastructure: According to the design of security construction scheme of information system for unit users, the security management and security technology are constructed in stages and subsystems, and the security strategy system and system management system are gradually enriched and improved in the process of construction.

Fig 3. A typical information security implementation scheme of information infrastructure for geological prospecting industry
(d) Security self-check or grade compliance assessment: After completing the network security renovation and construction of information infrastructure, internal technical experts can be organized to conduct system self-examination according to relevant regulations; third-party organizations can also be invited to assess the level conformity of system construction and analyze the gap between the actual construction of information system and the level protection requirements; if the gap is within acceptable scope, phase invitation can be formally invited. Official grade assessment is carried out by the evaluation institutions approved by the relevant departments.

(e) Revise the security policy and formulate a security construction rectification scheme: According to the information system security self-check or level conformity assessment results, if there is still a large gap, the security policy needs to be adjusted and revised, a security construction rectification scheme is formulated, and experts are organized. The security construction rectification scheme will be reviewed and demonstrated to guide the rectification and construction work.

5. Conclusion
Due to the weak infrastructure of information system construction and imperfect operation management system, it is urgent to solve the network security problem of information infrastructure in geological prospecting industry. In view of the characteristics of the construction demand for network security of information infrastructure, this paper puts forward a network security system for information infrastructure in geological prospecting industry, and gives the construction framework and solution of secondary system security protection environment. Based on the information security system constructed, a typical implementation scheme of network security of information infrastructure in geological prospecting industry unit is proposed, which guarantees the security of business system and data.

The network security system and specific solutions proposed in this paper for information infrastructure of geological prospecting industry have been successfully applied to the network security construction project of information infrastructure of Tibet Autonomous Region Geological and Mineral Exploration and Development Bureau, effectively solving the information security problems of this unit in the process of information construction, and enabling the unit to meet the Basic Requirements of Information System Security Grade Protection of the Ministry of Public Security and pass grade evaluation once.

Acknowledgments
This work was financially supported by Tibet Geological Prospecting Development Fund.

References
[1] People's Daily Online - People's Daily. Xi Jinping: The overall layout of all parties innovating and developing efforts to build China into a network power. http://cpc.people.com.cn/n/2014/0228/c64094-24488180.html, February 28, 2014.
[2] Solms B V, Solms R V. The 10 deadly sins of information security management [J]. Computers & Security, 2004, 23(5):371-376.
[3] Siponen M, Willison R. Information security management standards: Problems and solutions [J]. Information & Management, 2009, 46(5):267-270.
[4] Karyda M, Kiountouzis E, Kokolakis S. Information systems security policies: a contextual perspective [J]. Computers & Security, 2005, 24(3):246-260.
[5] Yan C P, Liu F, Guo F. Information security system of digital enterprise and its implementation scheme [J]. Chongqing Daxue Xuebao/Journal of Chongqing University, 2010, 33(2):36-41. (In Chinese)
[6] Wei Y C, Wu W C, Lai G H, et al. pISRA: privacy considered information security risk assessment mode [J]. The Journal of Supercomputing, 2018.
[7] Singh A K, Lv Z, Rho S, et al. IEEE Access Special Section Editorial: Information Security Solutions for Telemedicine Applications [J]. IEEE Access, 2018, 6:79005-79009.
[8] Li D, Cai Z, Deng L, et al. Information security model of block chain based on intrusion sensing in the IoT environment [J]. Cluster Computing, 2018(21):1-18.

[9] Takahashi T, Panta B, Kadobayashi Y, et al. Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information [J]. International Journal of Communication Systems, 2017:e3470.

[10] Thomas M, Dhillon G. Interpreting Deep Structures of Information Systems Security [J]. The Computer Journal, 2012, 55(10):1148-1156.

[11] Liu J W, Cao X D, Xu S Y, et al. Research on information security evaluation of oil and gas SCADA system in cloud model [J]. CAAI Transactions on Intelligent Systems, 2018, 13(2). (In Chinese)

[12] Ding W, Wang G C, Xu A D, et al. Research on Key Technologies and Information Security Issues of Energy Blockchain [J]. Proceedings of the CSEE, 2018. (In Chinese)

[13] Yang Y, Huang X F. Network Space Combat Information Security Defense Situation Study Based on Dynamic Bayesian Network [J]. Control Engineering of China, 2017(10):211-217