Design of Power Grid Information Security Framework Based on Whole Life Cycle Management

Li Qiang, Liu Bo, Guo Qian, Shi Congcong and Fei Jiaxuan

December 6, 2018

Design of Power Grid Information Security Framework Based on Whole Life Cycle Management

Li Qiang[1], Liu Bo[1], Shi Congcong[2], Fei Jiaxuan[2], and Guo Qian[2]
1 State Grid Henan electric power company, Zhengzhou Henan 450018, China,
2 Global Energy Interconnection Research Institute co. Ltd. State Grid Key Laboratory of Information & Network Security, Nanjing 210003, Jiangsu Province, China.
marsmana@aliyun.com

Abstract

The whole process security of power information system is the key to ensure the safe and stable operation of the power grid. Firstly, the concept and characteristics of whole life cycle management (WLCM) are summarized by this paper systematically. Secondly, the information security architecture of power grid based on life cycle management is constructed, which is designed to protect the information security of power grid from three aspects: control flow, technical support system and mechanism guarantee system. Thirdly, the management and control flow of power grid information security, the technical support system of power grid information security (PGIS) and the mechanism guarantee system based on life cycle management are proposed. And the control flow, technical support and guarantee mechanism were designed in detail. Finally, the application of the method proposed in this paper is carried out in a provincial power company. The results show that the proposed method can effectively reduce the risk of power grid information security and improve the level of power grid information security, which is of great significance to the safe and stable operation of power grid and has strong engineering application value.

1 Introduction

Information security is the basis of ensuring the safe and stable operation of power grid, and plays an important role in the safe and stable operation of power grid. In recent years, a number of blackouts caused by cyber attacks have occurred at home and abroad, indicating that the existing level of information security in the power grid is still seriously inadequate. Information security risks exist in all phases of power cyber information system, such as inadequate pre-demand analysis, unreasonable security design and insufficient testing, which will lead to the level of cyber security protection of power information system [1-3]. It is urgent to conduct a comprehensive analysis of power grid information security from a global perspective.

In recent years, whole life cycle management (WLCM) has been widely used in various systems, and scholars at home and abroad have done a lot of research work in this field. For example, Microsoft launched the Security Development Life cycle SDL in 2004 in order to strengthen the software source code security and improve the software information security level [4-5]. It has been applied in Windows Server 2003 and Windows XP SP2. The technology effectively reduces the probability of vulnerability.

In order to improve the security and protection level of power grid information and strengthen the management and control ability of power grid information system security [6], based on previous studies, this paper constructs a PGIS architecture based on WLCM. According to the characteristics of power grid information system [7-8], a process management and control method of power grid information system based on the WLCM is proposed. Requirement analysis, planning and design, system development, security testing, system deployment, on-line operation, off-line management and other stages were designed in detail. The technology support system of PGIS based on the WLCM is constructed, and a series of technical systems are designed from the platform layer, the tool layer and the system layer. The security mechanism of PGIS based on the WLCM is constructed. The security mechanism of PGIS is guaranteed from the aspects of technical supervision, personnel training, evaluation and assessment. The method proposed in this paper improves the security of power grid information system and reduces the risk of high informatization. This method improves the information security level of power grid greatly, and has great engineering application value.

2 Overview of WLCM

2.1 Concept of WLCM

WLCM is a kind of management idea and method which considers the whole process of planning, designing, manufacturing, purchasing, installing, debugging, running, maintaining, renovating and discarding the equipment or project from the long-term economic benefit of the equipment or project, and minimizes the life cycle cost under the premise of satisfying the reliability method [1]. WLCM is a fundamental change in the traditional asset management. From the whole management process and the overall situation, it plays an irreplaceable role in improving the efficiency of asset management in power enterprises, and has increasingly become the central theory of lean management in power enterprises.

2.2 Characteristics of WLCM

The characteristics of WLCM can be summed up as "three systems" - the whole system, the whole cost and the whole process. System-wide: WLCM runs through the entire process of the enterprise, from the initial planning and design to the final failure, from one end. It takes the overall situation of the enterprise as the object of consideration to achieve the overall benefits as the starting point, after comprehensive analysis and selection of various schemes to choose its optimal scheme implementation. Total cost: the ultimate goal of every enterprise is to get the maximum return from the smallest capital investment. WLCM is to integrate all aspects of the cost of the enterprise into the game and balance between the minimum cost and the maximum benefit, seeking the lowest cost. Whole process: WLCM once determined to implement, the entire process must be strictly in accordance with the prior design, planning for operation, can not be temporary, arbitrary change, from the design to maintain its accuracy and stability, from the system to ensure its normal operation.

3 PGIS Framework Based on WLCM

The PGIS framework based on WLCM includes three parts: the whole life cycle management and control process, the technical support system and the mechanism guarantee system. As shown in Figure 1.

The WLCM and control process is the core of the information security system. By optimizing and adjusting the development process, the security activities of all links of the information system can be standardized fully. The framework mainly includes requirements analysis, planning and design, system development, security testing, system deployment, on-line operation, off-line management. The technical support system mainly supports the whole life cycle safety management and control work, mainly consists of platform layer, tool layer and system layer. Safeguard mechanism is mainly to promote the effective implementation of various safety activities, mainly including technical supervision, personnel training and assessment.

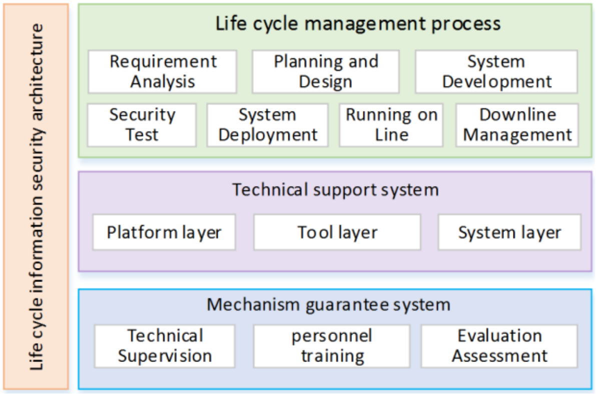
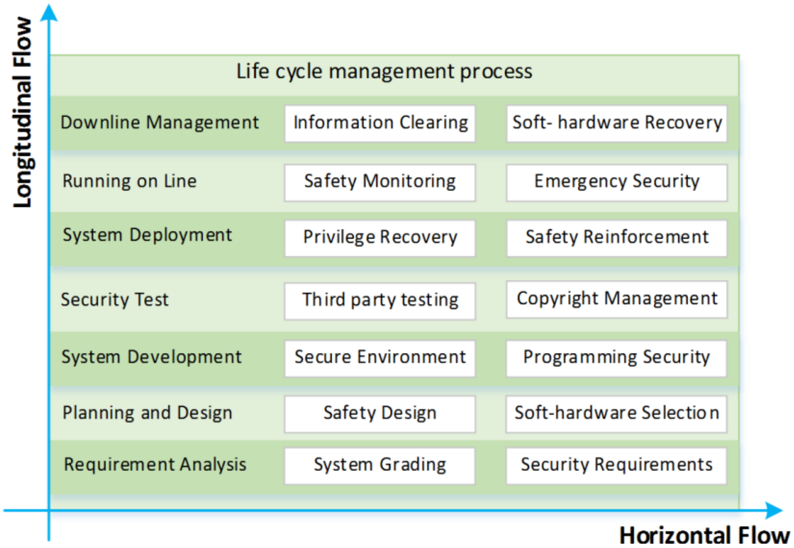


Figure1: Information Security Architecture Based on WLCM

4 PGIS Management and Control Process Based on WLCM

The PGIS management and control process based on WLCM mainly includes requirements analysis, planning and design, system development, security testing, system deployment, on-line operation, off-line management and other processes. Through the design of the whole life cycle management and control of the power information system, the information security level of the power grid is greatly improved, and it is of great significance to ensure the safe and stable operation of the power grid. As shown in Figure 2.



Downline Management	Information Clearing	Soft- hardware Recovery
Running on Line	Safety Monitoring	Emergency Security
System Deployment	Privilege Recovery	Safety Reinforcement
Security Test	Third party testing	Copyright Management
System Development	Secure Environment	Programming Security
Planning and Design	Safety Design	Soft-hardware Selection
Requirement Analysis	System Grading	Security Requirements

Figure2: Needs Analysis of PGIS

System Grading: In this stage, according to the principle of system grading, the information security level is divided, the importance of system business and the impact of attacks.

Requirement analysis: Comprehensive system security risk analysis is carried out by considering business process, important assets, deployment of Intranet and intranet, business interface and data security protection, and security requirement analysis is completed and documented. The project safety requirement document is passed.

4.1 Planning and Design of PGIS

Security design: System security design, including security function design, data security design, interface security design. Safety design plan can only be developed through accreditation.

Selection of software and hardware: Selection of key software and hardware products used in the process of system development or implementation. It is necessary for design and development units to organize safety testing in the design phase to ensure that the safety requirements are met.

4.2 System Development of PGIS

Environmental safety: The development environment and test environment should be isolated from the actual operating environment and office environment, and the test environment prohibits the use of production data. In the core R & D environment, the computer USB port should be sealed in principle.

Security coding: code is compiled according to enterprise unified safety programming specification and unified development platform. Avoid using third-party software and plug-ins without security. It is really necessary to introduce open source software and pass third-party security testing.

4.3 Security Test of PGIS

Security testing: Before the system goes on line, it should organize the third-party security evaluation, including security function testing, code security testing and so on, to find and repair deep-level code security vulnerabilities, preset security backdoors and other risks.

Copyright Management: Before the system goes online, the software copyright data should be handed over in time, and the authenticity, integrity and usability of the submitted data should be ensured, so as to ensure that the submitted code and the security test pass the code version.

4.4 System Deployment of PGIS

Privilege Recycling: Before the system goes online, the temporary accounts and privileges, such as privileged users, test accounts and so on, are reclaimed. During the period of transportation, the system should periodically (half a year) review and clean up the user rights of the information system, delete old and useless accounts, and timely adjust the authority allocation data that may lead to security problems.

Safety reinforcement: Before the system put on line, safety reinforcement should be organized, and risk assessment and safety reinforcement should be carried out in coordination with the operation environment.

4.5 On Line Operation of PGIS

Safety monitoring: Strengthen the real-time monitoring of system operation and safety status, timely discovery and feedback of abnormal events.

Emergency support: formulate contingency plans and conduct emergency drills regularly.

4.6 Offline Management of PGIS

Remaining information clearance: when offline, do a good job of data security transfer, data security destruction and data security management, the system memory buffer, disk space, process space, other recording media, registers and external equipment to clear the remaining information.

Software and hardware processing: timely disposal of the waste software and hardware involved in the system.

5 Technology Support System of PGIS Based on WLCM

The Technology Support System of PGIS Based on WLCM consists of three layers, namely the platform layer, the tool layer and the system layer, as shown in Figure 3.

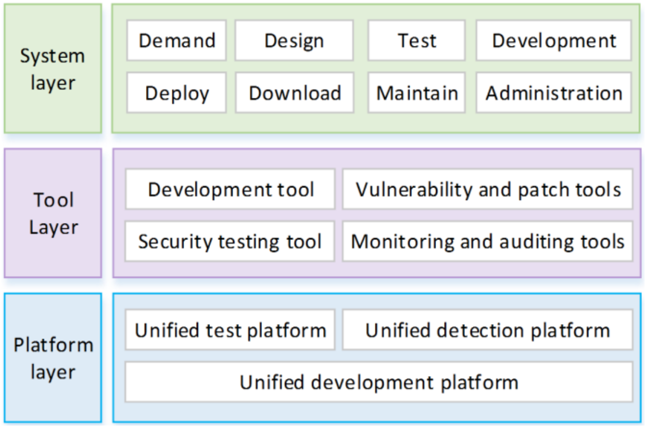


Figure3: Technical support system

The platform layer is made up of unified development platform, unified test platform and unified monitoring platform. The unified development platform mainly provides a unified, secure and reliable encoding template, interface, and general security function mechanism. The test platform has a series of test tools, standards, specifications and methods, which can be used to test the system in all directions. The unified monitoring platform mainly monitors all kinds of network, boundary, Internet outlet, host computer, server, system software and information system running state on-line, which can effectively improve the level of cyber security monitoring.

Tool support layer mainly provides supporting tools for the system, such as security development toolkit, security testing toolkit, vulnerability patch toolkit and monitoring audit toolkit.

The system support layer is a life cycle process management system, mainly including requirements, design, development, testing, deployment, download, maintenance and management.

6 Safeguard System of PGIS Mechanism Based on WLCM

The safeguard mechanism intends to further promote the effective implementation of various safety activities by means of technical supervision, personnel training, evaluation and assessment. As shown in Figure 4.

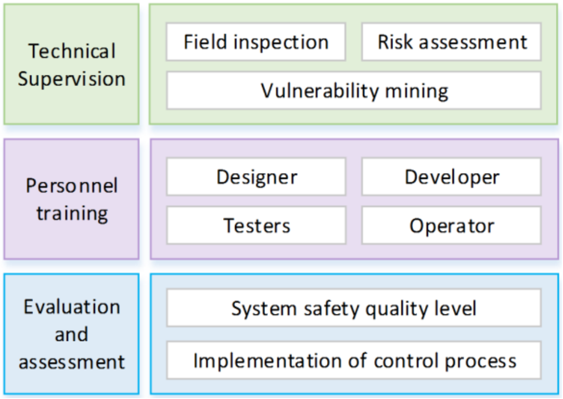


Figure4: Mechanism guarantee system

Technical inspections mainly include regular on-site inspections of R&D environment, regular vulnerability mining and risk assessment of on-line systems. Improve the level of cyber security protection from the technical level.

Personnel training for information system designers, developers, testers, operators to carry out regular cyber security training, strengthen cyber security knowledge, laws and regulations, to identify the trainees, strengthen the construction of cyber security personnel, support cyber security protection work.

Evaluation and assessment mainly assess and assess the implementation of the system safety and quality level as well as the implementation of the control process. Through the establishment of information system life cycle safety assessment system, through the use of qualitative and quantitative assessment of the system safety and quality level and the implementation of the management and control process assessment and evaluation.

7 Conclusion

Aiming at the shortcomings of the current security protection of power grid information system, this paper proposes a set of information system life cycle security management and control system and method suitable for large enterprises. The architecture of PGIS based on WLCM is constructed, and the security protection of PGIS is realized by the control flow, technical support and mechanism guarantee. It improves the security of power grid information system and reduces the risks brought by the highly informationalized power grid business. Through the comprehensive application and popularization of information system life cycle security management and control system, the security and reliability of power grid information system has been greatly improved.

References

[1] 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(02):6-11.

[2] 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(08): 147-151.

[3] PENG Yong, JIANG Changqin, XIE Feng, et al. Industrial control system cybersecurity research[J]. Journal of Tsinghua University(Science and Technology), 2012，52(10): 1396-1408.

[4] FENG Bo. Software Security Development Key Technology Research and Implementation [D]. Beijing University of Posts and Telecommunications, 2010.

[5] MSDN: Security development lifecycle phases[R] ， http//msdn2.microsoft.com/en-us/library/ms995349. Aspx，2005.

[6] YAO Wei. Whole Life Cycle Management of Power Enterprises Information Security [J]. Electric power ICT, 2015, 13(08): 94-99.

[7] LIANG Xiao, GAO Kunlun, XU Zhibo, et al. A Survey on Cybersecurity of U.S.Electric Power Industry[J]. Power System Technology, 2011，35(12): 221-228.

[8] CHEN Yuhui, JIANG Yuanchen. Build an Integrated Management System of Information Operation and Maintenance with Power Grid Chara[J], Electric Power Information and Communication Technology, 2011，9(02):165-169.

[9] LIU Junbao. Life cycle management of power enterprise assets[J]. Technology and Market，2012，19(02): 101-102.

[10] ZHAO Junxiang, ZHOU Cheng, CAI Yuxiang, et al. Application of equipment lifecycle management in power information system[J]. China Electric Power Education, 2014(09): 213-214.

[11] LIN Weili. The reliability research of electricity terminal equipment based on life cycle [D]. Shanghai Jiao Tong University, 2013.