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

Jindong He¹, Dan Wu², Zhichao Zhao³ and Qian Guo⁴,*
¹,²,³ State Grid Fujian Electric Power Research Institute, Fuzhou, China
⁴ Global Energy Interconnection Research Institute co. Ltd. State Grid Key Laboratory of Information & Network Security, Nanjing, China

*Corresponding author email: marsmana@hotmail.com

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

1. Introduction
Network security is the foundation of power grid security and plays an important role in its stable operation. In recent years, a number of blackouts caused by cyber attacks have occurred at home and abroad, indicating that the existing level of cyber security in the power grid is still seriously inadequate. Cyber 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]. There is an urgent need to analyze grid network security risks from a global network perspective.
In recent years, full life cycle management (WLCM) has been widely used in various information systems. Scholars from various countries have conducted in-depth research 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 cyber security level [4-5]. It has been applied in Windows Server. This technology effectively reduces the occurrence of vulnerability.
In order to improve the security protection level of the power information system and enhance the security management and control capabilities [6], this paper builds a PGIS based on WLCM based on previous research. 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. This method improves the security of power grid information system and enhances the cyber security level of power grid.

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 [9]. Different from traditional asset management, WLCM focuses on the entire management process and the overall situation, and focuses on improving the efficiency of asset management in power companies [10]. It has increasingly become the core theory of lean management in power companies.

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 [11]. 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 cyber 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. This technical support system supports the safety management of the entire life cycle. It is mainly composed of platform layer, tool layer and system layer. It promotes the effective implementation of various security activities through certain guarantee mechanisms, such as technical supervision and personnel assessment.

Figure 1. Cyber security Architecture Based on WLCM
4. PGIS Management Process Based on WLCM

The PGIS management 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 entire life cycle management of the power information system, it greatly improves the network security protection level of the power grid information system and plays an important role in ensuring the stability of the power grid operation. As shown in Figure 2.

**Figure 2. Needs Analysis of PGIS**

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

Requirement analysis: Complete a comprehensive network security risk analysis of business processes, important assets, network architecture, business systems, and data streams. Security requirement analysis is completed and documented. The project safety requirement document is passed.

4.1. Planning and Design of PGIS

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

Security coding: The code must be written according to the enterprise's unified security programming specifications and compiled through a unified development platform. Avoid using third-party software and plug-ins that have not been verified. If you need to introduce open source software, you must pass a third-party security test.

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.
4.5. 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.

4.6. 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.

4.7. Offline Management of PGIS
Remaining information clearance: To ensure the safety of data transmission, clearing and management. Perform cleanup of system memory buffers, disk space, other recording media, and registers.
Software and hardware processing: Timely clean up useless software and hardware 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.

The platform layer is composed of a unified development platform, test platform and monitoring platform. The unified development platform mainly provides safe and reliable coding templates, interfaces and security functions. 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 aims to further promote the effective implementation of various security activities through technical supervision, personnel evaluation and other measures. As shown in Figure 4.

![Figure 4. Mechanism guarantee system](image)

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] D.Wang, C.P.Chen, J.Yan, et al. “Pondering a New-generation Security Architecture Model for Power Information Network” Automation of Electric Power Systems, vol.40, pp.6-11, 2016.

[2] Z.W.Li, W.M.Tong, X.J.Jin. “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”, Automation of Electric Power Systems, vol.40, pp.147-151,2016.

[3] Y.Peng, C.Q.Jiang, F.Xie, et al. “Industrial control system cybersecurity research”, Journal of Tsinghua University(Science and Technology), vol.52, pp.1396-1408, 2012.

[4] B.Feng. “Software Security Development Key Technology Research and Implementation”. 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] W.Yao. “Whole Life Cycle Management of Power Enterprises Cyber security”, Electric power ICT, vol.13, pp.94-99, 2015.

[7] X.Liang, K.L.Gao, Z.B.Xu, et al. “A Survey on Cybersecurity of U.S.Electric Power Industry”. Power System Technology, vol.35, pp. 221-228, 2015.

[8] Y.H.Chen, Y.C.Jiang. “Build an Integrated Management System of Information Operation and Maintenance with Power Grid Chara”, Electric Power Information and Communication Technology, vol.9, pp.165-169, 2011.

[9] J.B.LIU. “Life cycle management of power enterprise assets”, Technology and Market, vol.19, pp.101-102, 2012.

[10] J.X.Zhao, C.Zhou, Y.X.Cai, et al. “Application of equipment lifecycle management in power information system” China Electric Power Education, vol.9, pp.213-214, 2014.

[11] W.M.Lin. “The reliability research of electricity terminal equipment based on life cycle”, Shanghai Jiao Tong University, 2013.