Research on Key Protocol Technology of Safe Access and Imitation Attack for Power Industrial Control Terminal Equipment

Xiaoqiang Wang, Rui, Zhao Xuehai Yu, Jinye Zhang
State Grid Shanxi Province Datong Power Supply Company, Shanxi Datong 037008 China.

Abstract. Industrial control system is widely used in social production activities and its security is directly related to national security and social stability. In this paper, the security threats and protection status of power industry control system are analyzed. A framework of information security evaluation system for power industry control system is proposed, which consists of three parts: experimental verification environment, product detection capability and security service capability, and the construction scheme of the system is discussed. A hardware-in-the-loop simulation and verification platform is constructed to realize the simulation and verification of power industry control system tools. The vulnerability of power industry control protocol can be found in depth. The problem of ambiguous attack mechanism and lack of verification means of power industry control system is discussed, which can provide support for the research of attack and protection of power industry control system.

Keywords: power industry control system, security access, attack simulation, information security.

1. Introduction
In recent years, the ways and methods of network attacks have developed from the early rough and single attack methods to today's complex and comprehensive attack methods. From password cracking, flooding denial of service and Trojan horse to network information detection, network vulnerability detection, network deception attacks, distributed network virus attacks and so on [1]. Our country has begun to consider how to effectively carry out the construction of industrial control safety, through effective integration with existing industrial control safety technology, strengthen the construction investment in power industrial control safety. Some provincial power companies have begun to introduce new methods and ideas to construct industrial control system security system in some production links [2]. For example, in the system boundary, through monitoring and other means combined with data analysis platform, the relevant baseline of industrial control system security detection and evaluation has been formulated, and a set of security early warning mechanism for industrial control system has been formed [3-4]. However, in order to fundamentally solve the problem of network security in power industry control system, it is necessary to model network intrusion and attack behavior, combine with the operation characteristics of power industry control system, and build
a characteristic library of network intrusion behavior with perfect characteristics, so as to better realize the response to attack behavior and prevent it from happening.

2. Detailed Design and Implementation of SSL Security Access Based on VxWorks
The modification of SSL secure access based on VxWorks is mainly based on the open source code of OpenSSL [5]. The system needs certificate management and secure communication and access of SSL by modifying relevant codes and transplanting them to VxWorks embedded real-time operating system.

In order to realize the two-way authentication and encrypted communication between the industrial control terminal equipment and the main station's SSLFVPN gateway, it is necessary to implement the SSL protocol to meet the "Technical Specification of SSLVPN" formulated by the State Cryptographic Administration. Through calling Socket communication module, certificate management module, cryptographic operation module and SSL secure communication and access module, the secure access of SSL is completed. The architecture of SSL secure access involving various modules is illustrated in Figure 1.

Following is a detailed description of the module function description and interface definition of certificate management and SSL secure communication and access implementation based on OpenSSL open source software code base according to Figure 1.

2.1. Certificate Management Module
The module implements certificate management based on SM2 algorithm, including reading device certificates, validating server certificates and so on. The list of functions is shown in Table 1.

| Num | Function class                 | Function description                                                                 |
|-----|--------------------------------|--------------------------------------------------------------------------------------|
| 1   | Certificate Management Class   | Device Import SM2 Certificate and Its Public-Private Key Pairs                       |
| 2   | Device Export SM2 Public Key Certificate |  |
| 3   | Certificate Theme Resolution and Extraction of Certificate Theme Information |  |
| 4   | Certificate Public Key Resolution to Extract Certificate Subject Information |  |
| 5   | Resolution of Certificate Validity Period and Extraction of Certificate Validity Information |  |
| 6   | Validation class               | Verify that the server certificate is legitimate                                    |

Its function use process is as follows:
The process of validating the validity of the device according to business requirements is shown in Figure 2 When the device uses the session, the subject, public key and validity period of the certificate are analyzed, then the validity of the subject format of the certificate, whether the public key is revoked and whether the certificate is valid, and then the connection is established according to the validity [6].
By verifying the validity of the certificate, the legitimacy of the device itself and whether it is in an effective state can be ensured, so that the risk of forgery or failure of the device can be avoided.

3. Design of Information Security Evaluation System for Electric Power Industrial Control System

On the basis of in-depth analysis of the construction requirements of information security evaluation system for power industry control system in China, referring to international and national information security engineering management standards and combining with many years of practical experience of information security protection in power industry, this paper puts forward a framework of information security evaluation system for power industry control system, which consists of three parts: experimental verification environment, product detection capability and security service capability, as shown in Figure 3.

---

**Figure 2.** Process of validation of equipment legitimacy

**Figure 3.** Framework of information security assessment system for electric power industrial control system
The experimental verification environment will be built according to the typical power industry control system architecture and the characteristics of power system in China, including the application system layer, communication protocol layer and terminal equipment layer [7]. The experimental verification environment will be built according to the typical power industry control system architecture and the characteristics of power system in China, including the construction of security experimental verification infrastructure including application system layer, communication protocol layer and terminal equipment layer. Develop information security protection technology and products, verify the existing security protection technology and product protection capabilities, security assessment methods and tools effectiveness and security. Design and develop the evaluation technology and tools for power industrial control system, terminal equipment, power special communication protocol, wireless equipment and so on, test the penetration attack and defense technology for industrial control system. To provide a simulation training environment for security evaluation service, in order to improve the technical ability of information security operation and maintenance personnel.

According to the safety standards and norms of power industrial control system in China, the construction of product testing center of industrial control system will be carried out [8]. The safety service product testing norms and implementation guidelines of industrial control system will be studied and formulated. The product safety testing service will be provided to the suppliers of main station system and terminal equipment, and the system and equipment out-of-factor testing service will be provided to power enterprises.

The construction of security service capability includes two aspects: establishing and improving normalized information security service mechanism, researching and formulating safety evaluation and reinforcement, safety evaluation before going online, grade protection evaluation, implementation guide and operation guidance, and providing normalized information security evaluation service for industrial control system of power enterprise online operation.

The information security evaluation system of power industry control system is an open, dynamic and continuous improvement system. It transforms the information security response of "disorderly, scattered and passive" into the organization of information security activities of "system, coherence and initiative". The construction of information security evaluation system of power industry control system is a systematic project, which needs to draw on the advanced information security technology and management experience of international and foreign countries. Based on the research results of the existing national information security standard system and standard formulation, this paper combines the information security needs and service experience of the design, development, construction, implementation, operation and maintenance, abandonment and other stages of the life cycle of power industry control system. The overall framework of information security evaluation system of electric power control system is put forward to meet the needs of information security service of production control system in important basic industries of the country. The system construction mainly includes three aspects: the construction of experimental verification environment, the construction of product testing capacity and the construction of safety service capacity.

3.1. Construction of Experimental Verification Environment
According to the typical structure of power industrial control system and the characteristics of China's power system, the construction of experimental verification environment of power industrial control system information security will include the main station system layer, communication network layer and terminal equipment layer. Develop and verify the protection capability of safety protection technology, the effectiveness and safety of safety assessment methods and tools, test the penetration attack and defense technology for industrial control system, provide simulation environment for safety assessment, and train the ability of safety service personnel.

3.2. Capacity Building of Product Inspection
According to the safety standards and norms of industrial control system in China, the construction of product testing center of industrial control system will be carried out, and the safety service product
testing norms and implementation guidelines of industrial control system will be studied and formulated, which will provide product development and safety consultation and testing services for industrial control system manufacturers, as well as ex-factory inspection services for power enterprises.

In order to verify the effectiveness of power industrial control system and related equipment security functions, explore and analyze the security vulnerability of power industrial control system and terminal equipment, simulate hackers to implant malicious code or reserve backdoor programs to attack. It is necessary to build a safety test environment for power industrial control system based on the structure of China's power industrial control system, referring to the relevant international standards of power industrial control system and the basic requirements of China's grade protection. In this environment, large-scale simulation and simulation of software running environment are carried out, and its security performance, especially the key equipment in the special architecture, industrial control network protocol and the cryptographic mechanism used, is carried out to excavate vulnerabilities and detect vulnerabilities, so as to verify the conformity of the security and standard requirements of the special equipment of power industrial control system.

At the same time, the safety testing standards and guidelines for power industrial control system products are formulated. The testing standards and specifications should include the testing requirements of typical power plant industrial control system and terminal equipment, such as product architecture, functional requirements, performance requirements, safety requirements, etc., and formulate product testing assurance requirements around industrial control system, such as delivery and operation assurance, guidance documents, testing assurance, vulnerability assurance, risk aversion, etc. The implementation guidelines should include the detection scope, detection process, detection methods, safety management and risk control, management rules of detection tools, detection institutions and personnel management of typical industrial control systems and terminal equipment in power plants.

3.3. Capacity Building of Safety Services
The construction of power industry control system security service capability includes building and perfecting organization structure and personnel team, establishing and perfecting normalized information security service mechanism, researching and formulating work norms and processes of security assessment and reinforcement, pre-online security assessment, etc., in order to provide normalized information security assessment service for power enterprise online operation industry control system.

The construction of security service capability should be based on the security requirements of the whole life cycle of power industry control system, and based on the system information security experimental verification environment and product detection system, to provide normal security assessment service for power enterprise industry control system. From research, design and development, to implementation, operation and maintenance, abandonment and other aspects to provide security advice, advice and information security technology guarantee.

Electric power industrial control system requires high security, reliability and stability of system operation. Therefore, safety evaluation service should be based on ensuring the normal and stable operation of the system and risk control. Evaluators should have the ability and qualification of information security evaluation, reinforcement, design, etc. They should master the background of business knowledge related to power production control. The evaluation tools and methods used can not have any impact on the operation system. In addition to abundant service content, the safety evaluation of power industrial control system needs strict control measures, stable, reliable and controllable technology and management support.

4. Attack simulation and verification of power industrial control system
Attack simulation and verification of power industry control system is to restore the intrusion attack scene from the attacker's point of view, which provides technology and verification means for the analysis of malicious attack mechanism of power industry control system. In this paper, attack
simulation flow construction and attack simulation platform validation of power industrial control system are analyzed to realize attack simulation validation.

4.1. Attack simulation flow of power industrial control system

Combining with the vulnerability analysis of industrial control protocol, the vulnerability information is obtained by identifying the network topology and assets of power industrial control system. The vulnerable key nodes of power industrial control system are found. The feasible attack path is generated based on hierarchical depth-first search. The test sequence is established by using test cases, and the protocol data package is constructed to carry out the attack. The principle of attack simulation is shown in Figure 4.

![Figure 4. Principle of attack simulation](image)

(1). Vulnerability detection

Firstly, according to the vulnerability analysis of the industrial control protocol, the network topology and assets of the power industrial control system are collected to identify its vulnerability, and the collected data are preprocessed to find the vulnerable nodes of the power industrial control system. Network topology information mainly includes all host configuration information (such as firewall rule configuration) and host location in the network, including access rights of hosts in the network, accessibility relations between hosts, etc. Asset information includes vulnerability information such as host, service and port, which can be obtained by vulnerability scanning software.

(2). Feasible Attack Path Generation

After obtaining vulnerable nodes of industrial control system and constructing attack rules among nodes, the threat index of nodes is quantified and key targets are selected. A hierarchical depth-first search method is adopted to establish a feasible attack path from the source node to the destination node.

(3). Designing attack test cases

Extensible attack test cases are designed through formal description and semantic analysis techniques. Attack test cases can be classified from attack purpose, attack mechanism and attack implementation process. The purpose of attack can be divided into denial of service attack, access control rights, code tampering, sensitive information acquisition, etc. The attack mechanism can be divided into memory destruction, input validation, logic error, design error and configuration error. The attack implementation process can be divided into access to primary privilege attack, access to the highest privilege attack, back door attack and so on.

(4). Establishing Attack Test Sequence

An effective attack is a combination of multiple test cases, which collects vulnerability information of the attacking object, designs an attack plan combining with feasible attack path, and establishes an attack test sequence.
4.2. Attack simulation verification of power industrial control system

Based on the hardware-in-the-loop simulation platform, the attack simulation validation of power industrial control system is carried out.

The hardware-in-the-loop simulation platform includes digital simulation environment and real environment. In the digital simulation environment, the software simulation technology is used to simulate the primary system and intelligent control equipment in the electric power field, and the network simulation technology is used to simulate a wide area communication network. The real environment is based on specific basic functional requirements and expanded business needs to build power industry control system, such as intelligent substation system, distribution automation system, dispatching automation system, etc.

Simulated attack environment is built locally, and attack test case set is used to simulate attack. The network protocol package capture tool is used to analyze the full flow packet capture of industrial control protocol. The simulation attack of power industrial control system is validated by simulation environment, and the scenario of intrusion attack is restored. The malicious attack mechanism of power industrial control system is analyzed, which provides basic verification means for the research of attack and protection of power industrial control system.

5. Conclusion

Through the construction of the evaluation system, we can carry out the research and development of evaluation standards and norms, provide product safety testing services for industrial control product manufacturers, and provide normal information security services for power enterprises in the transportation and industrial control system. At present, the security of power industrial control system is facing the problems of lack of security mechanism of industrial control protocol, insufficient depth of product evaluation and vulnerability verification. This paper proposes a dynamic-static vulnerability analysis technology of industrial control protocol, constructs a hardware-in-the-loop simulation and verification platform, and realizes the simulation and verification of power industrial control system tools. It can deeply discover the vulnerability of the power industry control protocol itself, and discuss how to solve the problem of unclear mechanism of malicious attack and lack of verification means in power industry control system, which can provide support for the research of attack and protection of power industry control system.

References

[1] Dragosavac J, Janda Z, Milanovic J V . PLC-Based Model of Reactive Power Flow in Steam Power Plant for Pre-Commissioning Validation Testing of Coordinated Q-V Controller [J]. IEEE Transactions on Power Systems, 2011, 26(4):2256-2263.

[2] Hao S, Yiran Lü, Liu J, et al. Application of classified protection of information security in the information system of air pollution and health impact monitoring[J]. Wei sheng yan jiu = Journal of hygiene research, 2018, 47(1):103-107.

[3] Jasna Dragosavac Z J . PLC Based Model of Reactive Power Flow in Steam Power Plant for Coordinated Q-V Control [J]. IEEE Transactions on Power Systems, 2011, 26 (4): 2256-2263.

[4] Anisimov V G, Zegzhda P D, Anisimov E G, et al. A risk-oriented approach to the control arrangement of security protection subsystems of information systems [J]. Automatic Control and Computer Sciences, 2016, 50(8):717-721.

[5] Zou D, Wang B . Adaptive and robust excitation control with terminal sliding mode for multi-machine power system [J]. Electric Power Automation Equipment, 2010, 30(12):79-82.

[6] Xiaohu Z, Longfu L, Yong L I, et al. Online energy-efficiency monitoring system for large-power industrial rectifier system and its remote calibration algorithm[J]. Electric Power Automation Equipment, 2014, 34(12):123-130.

[7] Menard P, Bott G J, Crossler R E . User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory [J]. Journal of Management Information Systems, 2017, 34(4):1203-1230.
[8] Meso P, Ding Y, Xu S. Applying Protection Motivation Theory to Information Security Training for College Students[J]. Journal of Information Privacy & Security, 2013, 9(1):47-67.

[9] Li H, Ru Y Q, Li Y K, et al. Information Security Protection Design of Electric Vehicles Charging Station[J]. Applied Mechanics and Materials, 2015, 741:681-686.

[10] Mohanty S P. Information Security and IP Protection Are Increasingly Critical in the Current Global Context [Notes from the Editor] [J]. IEEE Consumer Electronics Magazine, 2017, 6(3):3-5.