Construction of Safety Protection System for Power Industrial Control System and Enhancement Design of Communication Protocol

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

Abstract. The safe and stable operation of the power system has always been a common problem related to social stability and economic development in the world. To adapt to the development of "Internet +" and energy Internet, to ensure the information security of the power industrial control side, the power industrial control system Information security raises higher requirements. First, the ICS communication model is abstracted, the security risks and threats faced by ICS are sorted out, the most urgent and critical security requirements are clarified, and then a communication enhancement scheme is designed without affecting functions, efficiency, and rapid deployment. This includes one-way authentication and integrity checking of critical communication messages, combined with a timestamp mechanism and registration mechanism. Finally, through the security analysis of the enhanced scheme, it proves that it can resist common attacks such as camouflage, tampering and replay.

Keywords: industrial control system ICS, communication protocol, safety protection.

1. Introduction
The power system is mainly composed of power generation, transmission, substation, power distribution, power consumption and dispatching. Among them, the power generation enterprise is one of the most important parts of the entire power system [1]. With the advent of "Internet +", the deep integration of the Industrial Control System (ICS) and "Internet +" is the future development trend. Advanced information technologies such as mobile Internet, cloud computing, big data, and Internet of Things are applied to the safe production of power plants to promote power plants to intelligence. Development, digitization and other directions. At the same time, with the rapid development of power automation production technology, industrial control system products are increasingly using common protocols, general hardware and software, network equipment, the closure of the industrial control system in the physical environment and the specificity of hardware and software are gradually being broken. Therefore, the intelligence of the industrial control system improves production efficiency and management efficiency, and also creates opportunities for malicious attackers [2]. Domestic scholars have just started research on the safety of power industrial control systems, and most of the research is to apply public information network security theory and security technology directly to the security protection of power industry control systems [3-4]. Security technology is not enough to cope with the ever-changing attacks.
In 2015, the National Energy Administration organized a special supervision work on the safety protection of power industrial control systems nationwide, focusing on the network safety management of power industrial control systems in the power industry, the implementation of management regulations, the implementation of overall technical protection strategies, the investigation of hidden dangers of PLC equipment and the rectification of loopholes. Supervision and inspection of the work of publicity, education, training [5].

2. Typical ICS system
ICS systems are widely used in power systems, water and electricity, petrochemicals, transportation and many other industries. For example, in the tap water data collection and monitoring system, the water temperature, conductance, pH value and other data collected by the pipe network pressure measuring terminal and the water source water quality monitoring terminal deployed in each pipe network and water source include the dedicated line channel, the wide area network channel and the GPRS. A variety of channels, such as a wireless transmission channel, are reported to the primary station system, and the primary station system analyzes and processes the data for scheduling, pipe network water quality monitoring, and water source water quality warning [6]. The ICS system communication model consists of the main station system, communication channel and terminal. The basic working principle is that the terminal collects the industrial process measurement data and sends the data to the main station through the channel. After the primary station analyzes, commands such as control or parameter settings are sent to the terminal through the channel. The terminal then acts on the industrial process and returns the execution results and/or status to the primary station.

3. Safety Characteristics and Risk Analysis of Power Industry Control System

3.1. Safety Characteristics of ICS
The ICS includes the following features: First, the primary station system communicates with multiple terminal systems simultaneously through different types of channels, and the computing resources are relatively rich. The second is that the communication channel is diversified and unsafe. The third feature is that the number of terminals is large and deployed in a wide range of environments with complex environments according to system requirements. The computing power of the terminal is much lower than that of the primary station side, and there is no reliable source of time, and it is necessary to obtain the timing from the primary station by communication. Then is the degree of safety hazard. Traditional information system attacks mainly affect virtual assets, while attacks against power industrial control systems may directly damage physical devices [7].

3.2. Risk Analysis of ICS
Analysis of the above security risks from the threat angle can reveal that the software and hardware vulnerabilities, virus Trojans and other communication risks are huge, and require long-term investment and gradual solution. Because this paper hopes to solve urgent and critical problems quickly, we will not consider this part of the threat, but focus on communication security threats, including camouflage, tampering and replay attacks on critical control communications [8-9]. Control messages often result in changes in the state of critical equipment such as switches or valves. Another aspect is the threat of information theft. It is a threat when you get important information by listening to the stolen information. The important information can be the communication content itself, or it can be derived from the information obtained through communication with other channels.

4. Safety Protection System of ICS
On the basis of in-depth analysis of typical industrial safety incidents and investigation of relevant safety technologies of power industrial control systems, this paper summarizes a set of safety protection systems for power industry control systems from the aspects of safety detection, safety monitoring and safety protection.
4.1. Safety Detection

Security detection establishes security detection capabilities from vulnerability detection, malicious code detection, malicious behavior detection, etc., and timely discovers abnormal conditions of the power industrial control system. First of all, vulnerability testing is aimed at on-site measurement and control equipment, network equipment, computer equipment, security equipment, industrial control communication protocols in smart grid industrial control systems, combined with techniques such as stain propagation analysis, symbolic execution, dynamic binary analysis, software reverse engineering, and penetration testing. Means to implement vulnerability detection and mining. Second, malicious code is one of the main threats to power industrial control systems. Therefore, a malicious code detection and protection system is deployed in the main station end of the production control area, the important plant station end, and the enterprise management information area, and the key industrial control equipment, the underlying components, the temporary access equipment, and the remote control protocol. Such as the implementation of multi-level malicious code scanning detection, timely update the malicious code signature, view the killing record, take measures to prevent malicious code. Then there is malicious behavior detection, which collects the malicious database of intelligent security system to form a business security threat sample database and extract relevant features.

4.2. Safety Monitoring

Safety monitoring is to establish a comprehensive monitoring of the operation status of the power industrial control system, network traffic, communication protocols, external interactions, etc., to achieve a comprehensive grasp of the security status of the smart grid industrial control system. The first is the operation status monitoring to realize the group management of assets, and monitor the key control equipment of the power industrial control system and the occupancy of equipment resources. Then you need to monitor network traffic [10]. Through acquisition, identification, storage and diagnosis, it is possible to identify illegal outreach, abnormal network applications and communication behaviors through abnormal network traffic identification, and to alarm real-time abnormal network traffic. Then an important point is the monitoring of industrial communication protocols. Monitoring the communication process and status of commonly used power industrial control communication protocols.

4.3. Safety Protection

Improve the security protection capability of power industrial control systems from terminals, networks, data, applications, etc., and improve the ability to detect and defend various types of threats. When formulating industrial firewall rules, only the special industrial control protocol is allowed to pass, and illegal access from the operation station is intercepted. The industrial control private network Intrusion Detection Systems (IDS) system is uniformly deployed in the production control area. The data security in the power industrial control system mainly includes the security of the data itself and the security of the data protection. Data security protection is implemented from the aspects of encryption algorithm and backup recovery respectively.

5. security protection design of ICS

Vulnerabilities in the live environment can be exploited by attackers and subject to different types of attacks. Major security vulnerabilities were discovered through risk analysis of power plants. Before designing the protection plan, combined with the risk analysis results, calculate the risk value caused by the exploitation of each vulnerability, and judge the severity of the damage to the power industrial control system. The calculation formula is:

\[ R = P \times F \times S \]  

Where risk value is R, probability index (P) is the probability of attacks and it ranges from 0 to 10. Fluency index (F) refers to the frequency at which the attack is exploited ranging from 0 to 10. And the severity (S) if the serious results which also ranges from 0 to 10.
In this paper, the value of vulnerability risk and the grade of risk in ISC are followed by Table 1 and Table 2.

**Table 1. Translation performance**

| Security vulnerability probability          | P | F | S | R |
|--------------------------------------------|---|---|---|---|
| Weak network border protection measures    | 7 | 7 | 8 | 498 |
| Weak host application protection           | 7 | 8 | 7 | 418 |
| Lack of WEB application protection         | 8 | 8 | 8 | 512 |
| Lack of APT attack warning                 | 7 | 8 | 7 | 387 |

**Table 1. Grade of risks in ISC security**

| Risk value | Risk level | Risk index |
|------------|------------|------------|
| 700~900    | High       | Level 3    |
| 500~700    | Medium     | Level 2    |
| 300~500    | General    | Level 1    |
| <300       | Low        | Level 0    |

5.1. Safety Protection Design

The security protection design of ISC in this paper is based on the security module of mandatory access control idea. It needs to intercept and arbitrate at a certain key point of the access control process before the access is about to reach the visited resource. The security module is in the system call at the key point of the kernel implementation, is responsible for collecting the behavior information of the current access, querying the security policy center, and returning the arbitration result. The security module includes a configuration file sub-module, a parsing sub-module, and an access control sub-module. They work directly with each other to achieve secure control of resource access. The scheme is shown in figure 1.

5.2. Security Enhancement Scheme

This paper proposes a security enhancement scheme for the ICS system communication model, which features elliptic curve public key algorithm for identity authentication and integrity protection. In addition, the suffix design is used to ensure compatibility with the original message. The second is to use a key control communication registration mechanism to combine time stamp checking mechanisms to prevent replay attacks. The idea of the security enhancement scheme is: No change is made to the packets other than the control packet. The reply message of the terminal does not change, and the reply to the primary station side is still in the original clear text. The core processing flow is shown in Figure 2. This section will enhance the security of the solution from several aspects of the attack perspective. Camouflage and tampering attacks. When an attacker pretends to be a master station to issue a command to the terminal, or tamper with the command issued by the master station, both types of attack behavior will be avoided by the verification signature algorithm. That is, it is considered that a camouflage and tampering attack has been encountered, so the message is discarded. For a simple replay control message attack, the attacker captures the control message and then finds the appropriate time to replay the text at
a reasonable time to try to make the terminal generate the wrong action. The main station side of this security enhancement program is basically a denial of service attack vulnerability due to the active party in communication, and the terminal side has weak computing power.

![Diagram of security enhancing scheme](image)

**Figure 2.** Main procedure of security enhancing scheme

Based on the above analysis, it can be seen that this security enhancement scheme can defend against the usual attack behavior and meet the required security requirements. Its security functions are shown in Table 3.

| Safety solution          | Before applying | After applied |
|--------------------------|-----------------|---------------|
| ID verify                | None            | One way       |
| Privacy                  | None            | None          |
| Integrity protection     | None            | One way       |
| Non-repudiation          | None            | One way       |
| Anti-denial service      | None            | One way       |

### 6. Conclusion

In this paper, the protocol enhancement scheme for the typical ICS communication model design is positioned to quickly improve the security of the most critical control communication without affecting the original functions and efficiency of the industrial system. It can be seen that the communication model, security requirements and protocol enhancement schemes identified in this paper have certain universal applicability. The follow-up will continue to focus on and study the security situation of ICS, improve the security enhancement scheme of this article, and research and apply lightweight cryptography.

### References

[1] Wang J Y, Sun L M, Ye L I, et al. Research on Critical Technologies of Attack Simulation and Verification Towards Electric Power Industrial Control System[J]. Electric Power Information & Communication Technology, 2017.

[2] Mohammed S. Advanced Sensor Technology and Applications in Industrial Control System[J]. International Journal of Distributed Sensor Networks, 2013, 2013(3):1-2.

[3] Kim S, Shin D H, Woo S, et al. Identification of IT application areas and potential solutions for perception enhancement to improve construction safety[J]. Ksce Journal of Civil Engineering, 2014, 18(2):365-379.

[4] Srinivas M, Hussain I, Singh B. Combined LMS–LMF-Based Control Algorithm of DSTATCOM
for Power Quality Enhancement in Distribution System[J]. IEEE Transactions on Industrial Electronics, 2016, 63(7):4160-4168.

[5] Mudd D B. A virtual hydroelectric power system for distributable industrial control system security research [J]. Dissertations & Theses - Gradworks, 2014.

[6] Oruganti V S R V, Bubshait A S, Simões M G. Real-time control of hybrid active power filter using conservative power theory in industrial power system [J]. Iet Power Electronics, 2017, 10(2):196-207.

[7] Zhong Z C. Security Monitoring Technology of Power Grid Industrial Control System Based on Network Traffic Anomaly Detection[J]. Electric Power Information & Communication Technology, 2017.

[8] Li X, Ran H, Jing L, et al. System Construction of Protection Solutions of Secondary Power System in Power Plant Based on Information Security [C]/ Asia-pacific Power & Energy Engineering Conference. 2009.

[9] Huang X F, Zhou C J, Qing Y Q, et al. Applying System Theory to Transient Fault Tolerance and Safety Enhancement of Tunnel Construction Wireless Monitoring and Control System[J]. Advanced Materials Research, 2011, 204-210:1370-1377.

[10] Lemaire L, Vossaert J, Jansen J, et al. A logic-based framework for the security analysis of Industrial Control Systems [J]. Automatic Control & Computer Sciences, 2017, 51(2):114-123.