Trusted Security Immune Model of Power Monitoring System

Wenwei Tao¹, Jinyu Wu¹,*, Zhihong Liang² and Zeming Jiang¹

¹China Southern Power Grid Company Limited, Guangzhou 510000, China
²Digital Grid Research Institute Cyber Security Branch, CSG. Guangzhou 510000, China

*Corresponding author e-mail: wujinyu@csg.cn

Abstract. Power monitoring system is an important national infrastructure; its security has a vital position. In recent years, malicious attacks against power information systems emerge in an endless stream, which makes power systems worldwide suffer a major blow. Aiming at the hierarchical structure of the power monitoring system and the security threats it faces, this paper proposes a security immune model based on trusted computing technology. The security analysis shows that the model can guarantee the credibility of the power monitoring system.

Keywords: Power Monitoring System, Trusted Computing, Security, Immune

1. Introduction

While information technology and network technology bring impetus to the development of industrial control systems, they also bring safety issues. The use of standardized application components has revolutionized information, communications and applications that have broken the security barriers established by new proprietary solutions. The trend of complex information systems and networks and distributed computing has brought severe challenges to information security protection.

In recent years, organized and purposeful security attacks against industrial control systems, represented by Stuxnet and Flame viruses, have occurred from time to time, and the security threats to industrial control systems have become increasingly serious [1]. Due to the professionalism of industrial control systems and the requirements for high reliability of system operation, the network security protection of industrial control systems is unique. Although various industries have begun to pay attention to the security protection of industrial control system networks in recent years, due to the lack of systematic theoretical support, most of the current security protection measures are directly applied to existing information security technologies and specifications. However, traditional technical means and methods based on public information network security protection such as firewalls and intrusion detection systems have not achieved satisfactory results. The main reason is that traditional information security theories are based on the security threats and security protection foundations of public information networks. The industrial control system network is very different from the public information network, mainly in three aspects:

The architecture is different. The public information network adopts an architecture whose main goal is openness and interconnection. The core is simple and the edges are complex: while the
industrial control system network is relatively closed. The main consideration is stability and performance when constructing, with clear boundaries and complex core functions.

The goal of security protection is different. The main goal of public information network security protection is to ensure the security of information, while the main goal of industrial control system security protection is to ensure the reliability, stability and real-time nature of business systems.

The security threats to prevent are different. The public information network mainly prevents external attacks including theft of sensitive information and infiltration attacks, while the industrial control system network mainly prevents internal attacks that mainly tamper with operating instructions and business logic.

The power system is an important national infrastructure and a typical industrial control system. The monitoring system that controls the operation of the power grid is a key attack target in a national-level network confrontation. China’s electric power system has established a network security in-depth protection system based on network isolation and border protection. However, in recent years, advanced attack methods have emerged one after another, with malicious codes such as "Stuxnet" [2], "Flame" [3] and "Black Energy" as the main technical means. Advanced persistent threats (advanced persistent threat, APT) [4] have caused great harm to industrial control systems such as energy. The process of spreading and destruction is much concealed, and it can break through the existing security protection measures based on "isolation, detection, and killing". Give the system a fatal blow.

Trusted computing [5] technology takes cryptographic hardware as the core, adopts a variety of security mechanisms and measures from the bottom up, and achieves full active blocking of attack methods from the entire mechanism of concealed spread of attacks, spy infection, execution of damage, and destruction after destruction, ensuring the computing environment and the network environment are safe and reliable, and have the ability to be immune to new unknown malicious attacks to achieve active defense. Based on trusted computing technology, this paper studies the trusted security immune model of the power monitoring system to protect the power monitoring system.

2. Related Work
In response to the security threats of the power control system, many scholars have carried out a series of research work.

Traditional security solutions for power monitoring systems are based on authentication, intrusion detection and other methods. For SCADA smart grid, Mahmood et al. [6] proposed the corresponding authentication scheme to ensure the security of basic communication between the substation and its control centre. Some scholars [7] combine the current popular blockchain technology and combine this technology with the smart grid to achieve end-user authentication and behaviour monitoring. The intrusion detection system is the most commonly used technology for power monitoring system security. With the development of artificial intelligence technology, intrusion detection systems for power monitoring systems are also combined with it, Such as deep learning-based IDS [8], Decision tree-based IDS [9], and Bloom filters-based IDS [10]. However, these methods are not enough to deal with the increasingly harsh network environment. In particular, the intrusion detection method is based on existing malware, malicious code, etc. for intrusion detection, which is difficult to prevent unknown network attacks.

Research on the application of trusted computing technology to power monitoring systems is still very small, and there are very few people who apply trusted computing technology to power terminal protection, but they have not risen to the entire power monitoring network.

3. The Security Risk of the Power Industry Control System
The power monitoring system needs to deal with different security risks from different levels, which can be discussed from the following four aspects.

3.1 Power Terminal Risk
Compared with the traditional information control system, the safety protection of the power industry control system is mainly concentrated on the terminal production equipment and its operation process. Terminal production equipment (such as PLC, operator workstation, engineer operating station, etc.) as the final control unit of the power system, directly controls the production operation and monitors the operating data information of the system. The security of the terminal server is the security of the computer equipment at the operating system and database system level.

3.2 Cyber Risk
Establishing a secure network environment is an important part of ensuring system information security, so a comprehensive and in-depth risk analysis of industrial control networks must be carried out. The security and stability of the information network can ensure the safe operation of industrial control equipment, provide reliable and effective network services for enterprises, and ensure the security, integrity and availability of data transmission. For the network infrastructure environment in the power industry control system, business and operational requirements are often changed, and the security impact that potential environmental changes may cause is usually rarely considered. As time goes by, security vulnerabilities may have penetrated into part of the foundation Facilities, some loopholes may be connected to the industrial control system through the back door, which seriously threatens the stable operation of the industrial control system.

3.3 Application Risk
The application layer runs various applications of the industrial control system, including network applications and specific business applications, such as e-commerce and e-government. Analyzing the application risk is to protect the system's various business applications to run safely. Many power industrial control equipment do not have an identity verification mechanism. Even if they do, most of them are the default user names and passwords of the equipment manufacturers, which are easy to guess or crack. Passwords are usually not changed regularly, which is extremely risky. At the same time, it is necessary to prevent the risk of unauthorized use of application system resources (such as files, database tables, etc.). The lack of redundant configuration of key components leads to insufficient detection, processing, and recovery capabilities of the application program, lack of verification of the program interface input format and verification of injection attacks, such as SQL injection attacks, and the system faces the risk of exposing the database.

3.4 Data Security Risks
Although the internal and external networks of the power system have been physically separated, a large amount of sensitive power data has been accumulated in the management information area, such as the marketing data of the power market, residential power consumption data, power company financial statements, human resources data, etc., internal personnel, Operation and maintenance personnel or program developers visit the electric power database too much, which can easily cause the leakage or tampering of these sensitive data. The current database not only contains electricity consumption data, but also stores personal information of residents. The personal and property risks of residents are increasing. Data such as power grid resources, dispatching, operation and maintenance, and maintenance are easily queried in batches, and then sensitive information is derived. The lack of filtering of sensitive characters will bring great risks. These power data often lack regular backups. If the data is mistakenly operated or deleted or changed, or the database itself fails, goes down, or the server hardware fails, the data is easy to lose.

4. Safety Immune Model of Power Monitoring System
In order to deal with the security risks faced by the power monitoring system, this paper is based on trusted computing technology, combined with the current hierarchical structure of the power monitoring system, to study its security immunity model. This chapter will introduce the security
model proposed in this article from three aspects: the basic principles of trusted computing, the hierarchical structure of the power monitoring system, and the security immune model.

4.1 Trusted Computing

Trusted computing technology starts from the computer architecture and hardware security, establishes a trust chain transmission system to ensure the trust of the terminal, and solves the trust problems between people and program codes, people and machines, and people to people from the source. Trusted computing group (TCG) defines "trustworthiness" by the expectation of entity behavior: if an entity's behavior meets the expected goal in the expected way, the entity is trusted. Academician Shen Changxiang, a well-known information security expert in China, believes that "credibility" must ensure that an entity's behavior is always consistent with the expected result when achieving a given goal, emphasizing the predictability and controllability of behavioral results. And under the leadership of Academician Shen Changxiang, feasible computing technology has developed into "Trusted Computing 3.0".

The basic idea of trusted computing is to establish a root of trust in a computer system. The credibility of the root of trust is ensured by physical security, technical security and management security. Then establish a trust chain from the root of trust to the hardware platform, to the operating system, and then to the application, one level of measurement, one level of trust, one level of trust, to extend this trust to the entire computer system to ensure that the entire computer system is trustworthy. As shown in Fig.1.

![Figure 1](image-url)

**Figure 1. Principle of Trusted Computing**

4.2 Power Monitoring System Structure

As shown in Fig. 2, in this paper, we only consider the field control layer and process monitoring layer in the power monitoring system, but the higher level including the enterprise management layer is not considered in this paper. The process monitoring layer supervises and controls the relevant systems of power generation, transmission and other processes, including engineer station, operator station, OPC server, etc. The field control layer forms a control loop with the field device layer through the field bus or real-time network. It operates the data collected by the sensors of the field device layer, executes the relevant control algorithm, and outputs it to the relevant equipment of the field device layer for execution. This layer of equipment includes PLC, data acquisition and monitoring system (SCADA), distributed control system (DCS), etc. The real-time nature of the power grid control business is very strong, and the control command delay is required to be controlled at the second or even millisecond level. At the same time, the business continuity requirements are high, and the business system has been running for many years without interruption.
4.3 Safety Immune Model of Power Monitoring System

According to the above-mentioned typical three-tier structure of power control system, this paper researches and designs a security immune model for power monitoring system based on trusted computing technology. The overall structure of the model is shown in the Fig. 3, and it mainly includes four parts: Trusted Computing Environment, Trusted communication network, trusted area boundary, and trusted management center.

Trusted Computing Environment: The trusted computing environment is composed of trusted computing nodes, enabling the application system to operate safely under the support of trusted computing resources, ensuring the safety and credibility of on-site control, production monitoring and scheduling. The trusted computing environment consists of a trusted system master station in the process monitoring layer and trusted on-site measurement and control equipments in the field control layer.

Trusted system master station: The trusted system master station mainly includes the core key servers used in high-security production control systems and information management systems, such as power dispatch control systems, important business systems, important management information systems, etc., which are used in power dispatch control systems The SCADA, front-end and workstation equipment at the core nodes are used in key business systems such as e-commerce platforms, power transactions and other core servers, and in important management information systems, they are used in core servers such as marketing and finance.

The construction of a trusted system master station can be carried out according to the following ideas: build an independent security entity with active defense in the server, realize the measurement and control of the computing environment, and construct a dual-system computing architecture with trusted defense and computing; Processors and motherboards with trusted computing functions to realize the hardware guarantee of the dual-system structure trust chain establishment and transfer technology; form a trusted operating system and trusted supporting software compatible with the dual-system server platform, and ultimately realize the credible behavior of business applications.
Figure 3. Hierarchical structure of power monitoring system

Trusted on-site measurement and control equipment: With the continuous development of information technology, the computing capabilities of smart terminal devices continue to improve, and different types of core chips, operating systems, and business applications have emerged, forming a fragmented software and hardware platform environment. Its fragmented characteristics will bring greater difficulty to the realization of the trusted security defense of its computing environment. In view of the above situation, the standardization of the intelligent unit software and hardware platform should be realized, and a unified standard and technical framework should be established to achieve effective and unified management. The most important thing is that while the intelligent unit software and hardware platform is standardized, a trusted intelligent unit software and hardware platform with unified standards, such as trusted chips, trusted operating systems, and trusted application management technologies, is applied to form a platform with autonomous defense Functional intelligent terminal equipment.

Existing terminal equipment adopts three binding measures of certificate, terminal, and SIM card for encryption. After the system is started up, the SIM card is forced to scan through software, and the terminal system is not controlled. Therefore, a trusted chip can be introduced into the embedded terminal, the existing terminal prototype startup code and part of the OS kernel code can be measured, and the application trusted integrity measurement mechanism can be added at the system kernel layer. Through the application trusted integrity measurement, ensure the reliability and uniqueness of the source of the terminal loading program, prevent malicious attacks from tampering, and realize the active immunity of the terminal to unknown malicious programs through mandatory control based on the whitelist mechanism.

Embedded trusted smart terminals mainly include trusted mobile (handheld) terminals, trusted power distribution terminals, trusted concentrators, etc. Among them, trusted mobile (handheld) terminals can be used for mobile inspections of smart substations and standardized mobile power supply bureaus. For operations management, mobile office, interactive business halls, etc., trusted power distribution terminals are mainly used in power distribution automation and other services, and trusted concentrators are mainly used in power consumption information collection systems and intelligent road network lighting control systems.
Trusted communication network: The boundary of the trusted area is the boundary of the system's trusted computing environment, as well as related components that connect the trusted computing environment and the trusted communication network and implement security policies. The trusted boundary part itself should also be securely constructed through a trusted architecture, which is the same as a trusted node. The trusted zone boundary implements security functions such as access control, packet filtering, security auditing, and boundary integrity protection.

Trusted area boundary: The boundary of the trusted area is the boundary of the system's trusted computing environment, as well as related components that connect the trusted computing environment and the trusted communication network and implement security policies. The trusted boundary part itself should also be securely constructed through a trusted architecture, which is the same as a trusted node. The trusted zone boundary implements security functions such as access control, packet filtering, security auditing, and boundary integrity protection.

Trusted management center: The Trusted Policy Management Center is a unified management platform responsible for the formulation, distribution, maintenance and storage of trusted software-based trusted policies. Its main functions include system management, policy management and audit management. System administrators, security administrators, and audit administrators are identified in the Trusted Policy Management Center. The system administrator is responsible for node management and policy management, the security administrator is responsible for defining the security level and authorization, and the audit administrator is responsible for policy audit operations through specific commands or operating interfaces.

5. Safety Analysis
The safety of the above safety immune model for the power control system can be analyzed from the safety risk corresponding to its hierarchical structure.

For the system master station layer, the trusted system master station can dynamically monitor malicious attacks on the master station through trust measurement technology, kill the attack in the cradle, and ensure the safety and feasibility of the system master station.

For on-site measurement and control terminals, the static measurement in trusted computing technology ensures the trusted startup of the equipment, the authentication function ensures the authority of the operator, and the dynamic measurement technology ensures the legitimacy of the operation process and the safety of the terminal equipment.

From the perspective of the communication network layer, the trusted communication network guarantees the trusted access of devices and the safe and reliable transmission of data, and the border of the trusted area ensures reasonable access to data through technologies such as access control.

6. Conclusion
Aiming at the hierarchical structure of power monitoring system and its corresponding security risks, this paper proposes a security immune model of power monitoring system based on trusted computing technology to deal with the increasingly complex network environment and various security threats faced by the power monitoring system. Through security analysis, it can be known that the security immunity model can realize security protection and automatic immunity from all levels of the power monitoring system.

References
[1] Sanjab, W. Saad, I. Guvenc, A. Sarwat and S. Biswas, "Smart Grid Security: Threats, Challenges, and Solutions", 2016.
[2] Nourian, S. E. Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet", IEEE Transactions on Dependable & Secure Computing, vol. PP, no. 99, pp. 2-13, 2018.
[3] L. Yao, C. T. Tank, "Based on the Analysis of Flame Virus Attack on China Information Security Considerations", Information Security & Technology, 2014.
[4] Dorothee, Frank, "Advanced Persistent Threats", Europaeische Sicherheit & Technik, 2016.
[5] H. Zhang, J. Luo, G. Jin, Z. Zhu and F. Yan, "Development of Trusted Computing Research", Wuhan University Journal of Natural Sciences, vol. 11, no. 06, pp. 1407-1413, 2006.
[6] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication", Future Generation Computer Systems, vol. 81, no. APR., pp. 557-565, 2017.
[7] J. Wang, L. Wu, K. R. Choo and D. He, "Blockchain-Based Anonymous Authentication With Key Management for Smart Grid Edge Computing Infrastructure", IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1984-1992, 2020.
[8] H. Yang, L. Cheng and M. C. Chuah, "Deep-Learning-Based Network Intrusion Detection for SCADA Systems", in Proc.2019.
A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour and H. Janicke, "A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models", in Proc.2019.
[9] A. Khan, D. Pi, Z. U. Khan, Y. Hussain and A. Nawaz, "HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems", IEEE Access, vol. 7, no. 4, pp. 89507-89521, 2019.
[10] S. A. Rotondo, "Trusted Computing Group", https://www.trustedcomputinggroup.org/home, pp. 1331, 2011.