Industrial Control Trusted Computing Platform for Power Monitoring System

Jinyu Wu\(^1\), Wenwei Tao\(^1\), Yuyang Lai\(^2\) and Zuming Qin\(^1\)

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

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

Abstract. The traditional network security protection methods are not enough to cope with the increasingly harsh network environment. It is of great significance to construct the active defense system of power monitoring network through trusted computing technology. Based on trusted computing technology, this paper studies the trusted computing platform for power monitoring system, mainly studies the trusted computing platform of master station and the trusted enhancement of field measurement and control equipment. Trusted platform of master station and trusted enhancement of field measurement and control.

Keywords: Power Monitoring System, Trusted Computing, Trusted Computing Control Platform, Master Station, Field Measurement and Control Equipment

1. Introduction

With the rapid development of Internet technology and Internet of Things technology and the advent of the industrial 4.0 revolution, the demand for industrial control systems (ICS) to connect to the information network is increasing, and the resulting information security problems of industrial control systems have become increasingly prominent. The early island-style industrial control system has hidden security risks in the aspects of communication protocol, operating system, security management strategy and management process, application software, etc., making the industrial control system information security vulnerabilities full. Marked by the outbreak of the Stuxnet [1, 2] virus in Iran, it has aroused widespread concern about the information security of industrial control systems in various countries. The information security issues of industrial control systems are related to industrial production operations, national economy, national defense security, and people’s lives and properties. The security situation of industrial control systems is severe and is attracting more and more serious attention.

The information security threats of the core devices of industrial control systems mainly include external network security threats and internal terminal security threats. External network security threats are mainly reflected in the attackers illegally entering the control network to access system resources without the authorization of the system. The prominent manifestations are tampering with...
control instructions, spreading viruses, forging status information, and interfering with the normal communication of the control channel at critical moments to cause the system Paralysis, etc.; internal terminal security threats are mainly reflected in malicious programs that can be easily implanted into software systems with open platform architecture. Traditional malicious code detection techniques can only detect abnormal conditions during software execution, and cannot be effective for the security of the software itself. Verification, once the malicious code hidden in the system firmware program is remotely activated by an attacker, it may lead to serious consequences such as the theft, deletion of system confidential information, and even the destruction of the system.

Traditional IT information system defense methods are generally a combination of isolation firewall, intrusion detection, and virus defense, which have limited application effects for industrial control systems. Aiming at new types of viruses or attacks that bypass security software, this kind of prevention technology implemented by pure software can only be implemented by means of patching and patching the loopholes afterwards. This is undoubtedly fatal to high-availability industrial control systems. Moreover, the update of the virus database will continue to increase the virus database, and the intrusion detection process will become more complicated, which not only increases the complexity of the security software, but also increases the burden on the system and errors in intrusion detection. The investment cost of reporting rate and safety precautions.

With the in-depth integration of informatization and power industry [3], the originally relatively independent smart grid system is increasingly interconnected with the enterprise management network, and the network information security problem of the power system has become increasingly prominent.

As a typical industrial control system, the power monitoring system is facing increasingly severe security threats. [4] The existing security solutions for industrial control systems are not enough to deal with the dilemma it faces.

Severe security threats, the existing security solutions for industrial control systems are not enough to deal with the dilemma they face.

Trusted computing [5] is a new technology for information system security, including trusted hardware, trusted software, trusted network, and trusted application software. Trusted computing realizes the information system level protection and protection system, which changes the traditional "Blocking, checking and killing" and other "passive response" protection modes. Its core idea is to carry out security protection while calculating, so that the calculation result is always the same as expected, and the whole calculation process is measurable and controllable without being disturbed. It is a new calculation mode in which calculation and protection coexist and active immunity. Research on the industrial control trusted computing platform for power monitoring system is very important to solve the safety problem of power monitoring system.

The rest of this article is organized as follows. Section 2 briefly introduces the safety-related work of industrial control systems. Section 3 introduces the knowledge of power monitoring system. Section 4 specifically describes our industrial trusted computing platform for power monitoring systems. Finally, section 5 summarizes this paper.

2. Related Work

Most of the existing ICSs network attack detection technologies are based on traditional intrusion detection systems [6, 7], which are mainly used for IT security analysis [8]. Intrusion detection systems are mainly divided into signature-based and machine learning-based. Learning-based methods improve the efficiency of managing accidental intrusions by identifying process trends or behaviors [9-11], while signature-based methods use databases and fixed signatures to detect known attacks, but they are not efficient in addressing unknown and new attacks [12].

No matter what kind of method it is based on, the intrusion detection system has a certain lag in unknown attacks and new attacks, which are a fatal flaw for industrial control systems, especially power monitoring systems. Research on active defense systems based on trusted computing is crucial. Among them, the research of trusted computing platform occupies an important position.
3. Power Monitoring System
The power industry control system is mainly composed of data acquisition and monitoring system (Supervisory Control and Data Acquisition, SCADA), distributed control system (Distributed Control System, DCS) and other control systems configured on key infrastructure such as programmable logic controllers (Programmable Logic Controller, PLC) and other components, with real-time, reliability, distributed, systematic and other characteristics.

The main function of the SCADA system is to collect communication and telemetry data, and issue remote control and dispatch commands, which are mostly used for power transmission dispatching, substation and power plant monitoring, power market operation, power consumption information collection, and distribution automation systems.

The power, information and business involved in the power industry control system are highly unified. The power transmission process includes: power plant generation, line transmission, transformer substation, user power distribution and power consumption. The power communication network has covered all aspects of the power control system. In principle, the control principle adopts “safe partition, network dedicated, physical isolation, vertical authentication” method, and has the following characteristics:

Fast system response: Compared with the traditional industrial system, the power industry control system does not allow excessive delay and system shock, and the response must be punctual and reliable to cope with different industrial control situations on site.

More system threat sources: Such as terrorist organizations, industrial espionage, malicious intruders, etc., attackers destroy and invade the industrial control system network through various forms of network attacks, including backdoor attacks, IP fragment attacks, malformed packet attacks, DoS attacks, brute force cracking, and communication capture Package etc. Once the security line of defense of the industrial control system is breached, it will cause serious damage to the industrial communication network and infrastructure.

Large amount of system data: The power industry control system involves the collection, transmission and information sharing of a large amount of power data, including the power transmission and transformation parameters of the system, and the power consumption of the power consumption terminal. This real-time information is required to ensure the accuracy and speed of power dispatch.

4. Industrial Control Trusted Computing Platform for Power Control System
Generally, the security problems of computer terminals are mainly solved based on software models, such as host anti-virus, human intrusion detection, and encryption authentication software. Obviously, software-based security solutions have great flaws, because any security software itself may be attacked and cause modification. Based on the computer terminal protected by the security software, its security function may become fake. Trusted computing considers security issues from the architecture, comprehensively considers the chip, motherboard operating system, application programs and other aspects and creates security architecture to ensure higher security of computer terminals. The security of the trusted computing platform is rooted in secure hardware with certain security protection capabilities. It is based on secure hardware to implement services such as isolated computing, computing environment integrity assurance, and remote security property certification to ensure the credibility of the behavior of computing entities on the platform Sex. Trusted computing starts from the computer architecture, and proposes a brand-new architecture-level system security scheme for the security requirements of information systems and various attack methods.

From the perspective of the industrial control system, the power monitoring system can divide the equipment in the power monitoring system into master station control equipment and field measurement and control equipment. In this paper, the research on the trusted computing platform for power monitoring systems will also start from two aspects: the trusted computing platform of the master station and the trusted computing platform for on-site measurement and control.
4.1 Master Station Trusted Computing Platform

In the power monitoring system, the process monitoring layer monitors the related systems of the power generation and transmission processes, including the engineer station, the operator station, and the OPC server. Deploy the trusted computing platform of the master station on the master stations of these systems to provide trusted services for the process monitoring layer. As shown in the Fig.1, the trusted computing platform of the master station includes a trusted hardware part and a trusted software part.

Trusted hardware: The most important thing in trusted hardware is the root of trust for system hardware. In this paper, the trusted platform control module is selected as the root of trust for hardware. For the power monitoring system, the main problem faced by this solution is: the need to modify or discard the existing server motherboard to integrate the crypto chip, and it does not have the conditions for large-scale applications. This article considers dealing with different scenarios, adopting PCI-E to implement the trusted platform control module in the motherboard modification or plug-in method for the existing equipment, and for the new equipment, it can be realized by the CPU built-in TPCM developed in China.

![Figure 1. Schematic diagram of trusted platform of master station](image)

Trusted software: The most important thing in trusted software is the trusted software base. TSB is embedded in the host's basic software, and under the support of trusted hardware and firmware such as TPCM, runs in parallel with the host's basic software to realize their respective functions and jointly form dual-system architecture. Dual architecture refers to the host software system and the trusted software base (TSB). The host software system is the part of the trusted computing platform that realizes normal system functions. The trusted software base is the entirety of trusted software components that implement trusted functions in the trusted computing platform. It is not an independent system, but is composed of multiple trusted software components within the host system that are logically interconnected and integrated.

4.2 Functions Implemented

Platform authentication: Based on the password support provided by TPCM to realize the identity authentication of users logging in to the platform.

Trust chain establishment: The theoretical chain of trust establishment process takes the trusted chip as the root of trust, starting from the root of trust, to the hardware platform, to the operating system, and then to the application, the first level of measurement and certification, the first level of trust, and the extension of this trust. To the entire computer system. This paper adopts TPCM as the...
root of trust. The establishment of the trust chain starts from the system boot program, and the measurement code is embedded in the operating system boot device to form the boot measurement device to realize the measurement of the operating system boot device code itself and ensure the initial state of the boot environment. Then the boot loader measures the operating system, and the operating system measures the application program. The specific process is as follows: load the operating system booter, start the measurer, call the cryptographic module through the trusted cryptographic module CPU real-mode drive, and perform integrity measurement on the memory initialization code and the bootloader code program of the operating system system booter to build trust. The starting point of the chain; the boot program measures and loads the integrity of the operating system kernel module and the trusted software base module. The measurement operation needs to call the cryptographic module through the trusted cryptographic module CPU real-mode driver; the trusted software base of the operating system kernel layer. The measurement is completed during the installation and startup phase of the application program to ensure the initial state safety of the application program; the real-time security of the power monitoring program is realized by dynamic measurement during the software operation.

Access control: In power control system applications, security labels are assigned to each subject and object according to the attributes of files and other resources and the permissions of the process for access control of the application process. At the same time, at the kernel layer of the operating system, another kernel layer access control strategy based on ports and services is maintained and executed by the trusted software base. The two together form a dual mandatory access control mechanism at the application layer and the kernel layer.

Enforcement control: Classify the processes on the server and classify the basic platform processes as public domains. Each advanced application process is defined as an independent private domain. Only private domains are allowed to call public domain processes, and public domains are prohibited from calling private domain processes. Calls between private domain processes.

Trusted network connection: Realize trusted authentication and secure communication between network communication nodes.

4.3 On-site Measurement and Control Trusted Computing Platform

The programmable embedded equipment represented by PLC is the core of industrial control system, and it has almost no safety protection ability. Through the application of trusted computing technology to PLC, it is in the dynamic security protection, so as to realize the active security protection of the core equipment of industrial control system and build a high security, high trust industrial control network overall operating environment. Trusted PLC is realized by adding or modifying some functions on the basis of traditional PLC software and hardware, and the built-in trusted chip realizes the trusted startup function. In this paper, trusted PLC is taken as the research object to study the trusted computing platform of field measurement and control.

PLC embedded real-time control system is composed of operating system core layer and application support layer. The core layer of operating system mainly includes board level kernel and driver package of embedded operating system and application support layer includes real-time control operation system for processing configuration logic and operation instructions. TPCM provides reliable support through board level expansion.

PLC real-time control operation system (RCRS) includes main task module, communication module, loading and running module, IO management module, auxiliary function module, etc. The main task system realizes the functions of transaction processing, state switching, fault diagnosis, system configuration and initialization.

Show as Fig.2, enhance the credibility of field measurement and control equipment through four sides:

Active measurement of PLC: To realize the reliable start of PLC, to ensure its initial credibility, to dynamically measure its running process, and to realize the credibility of its software and operation process.
Trusted software

Application support layer

Processing configuration logic

communication module(authentication)

Load running module(Signature verification)

RCRS(Trust enhancement)

Operating system core layer

Hardware support

Trusted hardware

Motherboard Extended Hardware Trusted Root

Figure 2. Schematic diagram of credible platform for field measurement and control

Trusted transformation of communication module: It supports the trusted authentication of the upper computer and encrypts the operation instructions. Only when the authentication is passed can the communication be run.

Trusted enhancement of loading and running module: Before loading and running the configuration project file, the signature verification is carried out first. Only the configuration project that passes the verification is allowed to run.

Add user identity rights management: Through authentication to determine whether the user has access and use rights to resources, so that the access policy of the system can be implemented reliably and effectively, prevent attackers from impersonating legitimate users to gain access to resources, and ensure the security of the system and data.

5. Conclusion
Aiming at the traditional network security technology that cannot meet the security problems faced by current power monitoring systems, this paper studies an industrial control trusted computing platform for power monitoring systems based on trusted computing technology. The research includes the trusted computing platform of the master station for the host computer in the power monitoring system and the trusted computing platform for the on-site measurement and control equipment. The trusted computing platform in this paper can provide effective and trusted functions for the power industrial control system to ensure the safety of the power monitoring system.

References
[1] J. P. F. R. Rohozinski, "Stuxnet and the Future of Cyber War", Survival, 2011.
[2] T. Alladi, V. Chamola and S. Zeadally, "Industrial Control Systems: Cyberattack trends and countermeasures", Comput. Commun., vol. 155, pp. 1-8, 2020.
[3] J. Wang, K. Meng, J. Cao, Z. Chen, L. Gao and C. Lin, "Summary of research on information technology of energy internet", Computer Research and Development, no. 05, pp. 1109-1126, 2015.
[4] M. Z. Gunduz, R. Das, "Cyber-security on smart grid: Threats and potential solutions", Comput. Networks, vol. 169, pp. 107094, 2020.
[5] C. Shen, H. Zhang, H. Wang, J. Wang, B. Zhao, F. Yan, F. Yu, L. Zhang and M. Xu, "Research on trusted computing and its development", Sci. China Inf. Sci., vol. 53, no. 3, pp. 405-433, 2010.
[6] S. Pan, T. Morris and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems", IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 3104-3113, 2015.

[7] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni and H. V. Poor, "Machine Learning Methods for Attack Detection in the Smart Grid", IEEE Transactions on Neural Networks & Learning Systems, vol. 27, no. 8, pp. 1773-1786, 2017.

[8] F. Zhang, H. A. D. E. Kodituwakku, W. Hines and J. B. Coble, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data", IEEE Transactions on Industrial Informatics, pp. 1, 2019.

[9] A. N. J. A, S. H. A, A. D. B, K. K. R. C. C, H. K. D. E. N. E and R. M. P. F, "An improved two-hidden-layer extreme learning machine for malware hunting", Computers & Security, vol. 89, 2020.

[10] S. D. D. Anton, S. Sinha and H. D. Schotten, "Anomaly-based Intrusion Detection in Industrial Data with SVM and Random Forests", 2019.

[11] M. Kravchik, A. Shabtai, "Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks", 2018.

[12] A. R. Revathi, D. Kumar, "An efficient system for anomaly detection using deep learning classifier", Signal Image and Video Processing, vol. 11, no. 2, pp. 1-9, 2016.