Research on Security Protection Strategy for Intelligent power terminals

Bin Xu, Feng Zhai and Nan Wang*
China Electric Power Research Institute

*Corresponding author: xubin1@epri.sgcc.com.cn

Abstract. In the context of Smart Grid 2.0, intelligent power terminals are an important part of the smart grid, but their weak security protection can easily become the main target and springboard for criminals to attack the grid. Therefore, ensuring the security of intelligent power terminals is the key to protect the security of smart grids. In this context, this paper through the analysis of intelligent power terminal security threats, proposes a three-layer intelligent power terminal protection framework including "physical layer", "operating system layer" and "communication layer", and thus proposed a security protection strategy for intelligent power terminal devices, which aims to comprehensively improve the security of power system comprehensively.

1. Introduction
Intelligent power terminals play an essential role in the construction of smart grids. They are a communication bridge between the power system and power equipment and a communication medium between the power system and users. Therefore, terminal equipment's safety and reliability are a prerequisite for the power system's stable operation. However, the open environment in which the terminal device is located and its computing and wireless communication functions make it vulnerable to malicious attacks. In recent years, hackers have used the terminal as a springboard to attack the power grid and caused frequent national and enterprise-level power grid security incidents. For example, in the "Stuxnet" incident in 2010, a nuclear power plant was paralyzed due to a virus attack on Siemens' PLC terminal [1]; The large-scale power outage in Ukraine in 2015 was also caused by hackers using terminals to damage the power control system [2]. In this context, this article focuses on the security requirements of intelligent power terminals, firstly introduces the current research status of intelligent power terminals, clarifies the present security risks of intelligent power terminals, and analyzes the main issues involved; on this basis, This paper proposes a security reinforcement framework with intelligent power terminals as the core, and offers a comprehensive intelligent power terminal security reinforcement strategy from the three levels of the physical layer, operating system layer, and communication layer; finally, the security reinforcement of intelligent power terminals Technology summary and outlook.

2. Current Research
Intelligent power terminal devices are typical embedded devices. The literature [3] points out that the attacks against embedded devices are complex and diverse, and embedded system security should comprehensively consider the physical, platform, and application layers. Literature [4] proposes a
security assessment model for intelligent power terminals, dividing the security assessment of intelligent power terminals into hardware security, network security and other five parts, pointing out that many security issues often have a strong integration. The literature [5] points out that the smart grid is a complex system. If there is a security problem with the intelligent power terminal device, it will threaten both the information system and the smart grid's power system. The literature [6] comprehensively analyzes smart meters’ security requirements in terms of confidentiality, availability, integrity, and non-repudiation. It concludes that smart meters’ security, as an intelligent power terminal device, needs to be improved urgently.

From this, we can see that the risks faced by intelligent power terminals are complex and variable, and as an important part of the smart grid, the security of intelligent power terminals is crucial. Therefore, under the severe and complex security situation, the intelligent power terminal needs a complete set of security reinforcement strategies to improve its security.

3. General Protection Framework
Aiming at the security requirements of power smart terminals, this paper proposes a three-layer defense framework of "physical layer," "operating system layer," and "communication layer" of intelligent power terminals, as shown in Figure 1. The physical layer focuses on security reinforcement of the isolation and fault tolerance of terminal equipment. The operating system layer provides security protection for systems and applications from the boot layer, kernel layer, and application layer. The communication layer focuses on protecting network activities—real-time monitoring and ensuring the security of data transmission.

At the physical layer, the isolation of terminal equipment is ensured through shell reinforcement, monitoring and inspection, physical signal processing, and physical access control mechanisms, and the fault tolerance of terminal equipment is improved by building detection systems and formulating emergency plans.

At the operating system layer, the boot layer's role is based on the cryptographic module, which verifies the security of the operating system kernel image and the integrity of the application software through the secure boot module to ensure the safe startup of the system. The kernel and application layers are based on the security storage module and the security audit module, which jointly control the download, installation, deployment, and operation of the software and control the electrical equipment connected to the terminal through port control, access control, and identity authentication mechanisms. On the central side, port control, access control and authentication policies are used to control end devices, and the Secure App Store module implements application security testing and auditing and provides a secure application download interface. Besides, the encryption module ensures the safe transmission of data and the terminal equipment's safe and stable operation through log recording and analysis.

At the communication layer, network activity is monitored in real time by setting up firewalls and building intrusion detection systems, network access is controlled using network isolation and authentication, and secure data transmission is achieved by setting up secure access zones, monitoring and filtering network traffic, encryption modules, and protocol analysis.
Figure 1. Three-layer protection framework for power smart terminals.

4. Security protection strategy

The following is a detailed discussion of the security requirements and corresponding protection strategies of intelligent power terminals from the "physical layer," "operating system layer," and "communication layer."

4.1. Security protection strategy of intelligent power terminal at the physical layer

The focus of physical security is to guard against the adverse impact of external factors on intelligent terminal equipment's power to ensure that the intelligent power terminal will not be damaged or information leakage caused by human-made or natural damage.

According to the characteristics of physical security and security requirements, the following two aspects of isolation and fault tolerance to analyze physical security.

Isolation. Isolation mainly includes two aspects: one is real environment isolation, the other is virtual environment isolation. Physical isolation prevents adverse effects of external factors on equipment, protects terminal equipment from accidental damage such as flood and fire, and prevents damage caused...
by human factors. Virtual signal isolation ensures that the terminal equipment's electrical characteristics, such as execution time, power consumption, electromagnetic radiation, and other physical information, are not exposed to the outside world to avoid bypass attacks.

**Fault tolerance.** Fault tolerance requires that the intelligent power terminal equipment should have an emergency mechanism. When an emergency occurs, it can restore some functions while protecting itself from further damage to minimize the entire power system's loss.

**Strategies on how to enhance isolation.** First of all, the terminal equipment should be ensured to have a relatively independent working environment, such as setting isolation cabinet and other isolation measures. Secondly, there should be protection for the equipment itself. For example, the equipment has a protection mechanism to prevent disassembly; when the equipment is forcibly disassembled by illegal operation, the equipment can timely cut off power and report abnormal conditions. Also, the operating environment of the equipment should be kept pure. For example, it is strictly prohibited to connect personal devices to terminal devices to avoid the external network environment's adverse impact on the equipment. The monitoring of equipment and regular inspection are equally essential.

**Strategies on how to enhance fault tolerance.** To strengthen fault tolerance, electric power enterprises should formulate emergency plans. Add specific protection mechanisms to the scheme. For example, the shell protection mechanism mentioned above, when the first layer of physical protection of the intelligent power terminal is breached, the intelligent power device has the processing capacity to timely report to the monitoring system, cut off the connection with the power system, delete critical data, protect the security of the entire power system, and avoid causing more significant losses. Due to the particularity of the distribution of intelligent power terminal equipment, constructing a complete monitoring system and making comprehensive maintenance plans are also important ways to improve the fault tolerance of the intelligent power terminal.

### 4.2. Security protection strategy of intelligent power terminal at the operating system layer

**Boot layer.** The boot layer of the operating system is based on the secure cryptographic module, enabling the secure boot of the system through a secure boot module. The specific process is shown in Figure 2. Firstly, starting from the boot program, the security verification of the operating system's kernel image is performed. Methods such as hash value-based metrics or key data structure metrics of the kernel are used to determine whether the kernel's integrity is illegally damaged during system operation. Then, verify the application software's integrity using check value comparison and other methods to ensure it has not tampered. At this point, the step-by-step measurement verification of the secure boot layer is completed, and a complete chain of trust will ensure the safety of the system software, and the system can start safely.

![Figure 2. Safety boot module.](image)

**Kernel layer.** The kernel layer is divided into three major parts: control module, application management module, and system management module. In the control module, to achieve resource access control security, the kernel layer unites the application layer and the central side to implement access control, port control, and identity authentication policies. The access control module plays a role in the information interaction between power-using devices and terminals, classifies the access levels of
devices according to their roles, suppliers, and other information, creates a list of trusted devices, establishes device access policies, and sets the permissions of various power-using devices. The port control module continuously monitors the usage activities of all power-using devices. When an unauthorized connection is made, the system alerts and provides a detailed report of the device. The authentication module is aimed at two main types of entities: users and consumer devices. There are three main authentication methods for users: password-based, smart card-based, and biometric-based authentication. For the authentication of electrical equipment, the password-based method is generally used. The application management module is responsible for controlling the application software by the operating system. It has macro control over the download, deployment, installation, and operation of the application software through the software control module. Once the application software is abnormal, the module will receive an alarm from the security audit module located at the application layer, which will promptly trigger the module's internal abnormality processing mechanism to respond to the software abnormality. The process sandbox isolation module achieves application running isolation; application software running will be allocated an independent process space and isolated from other processes; the interaction between different processes need to request system privileges to protect application data from unauthorized access. The system management module is mainly responsible for managing system resources. The security storage module is responsible for storing essential data related to the operating system based on the encryption mechanism and anti-buffer overflow mechanism to realize encrypted data storage and protection. The security audit module is mainly responsible for the analysis of system logs. It contains a detailed system abnormality response mechanism, which can promptly deal with various system abnormalities to ensure the system's safe operation.

**Application layer.** The application layer is mainly divided into three major parts: policy control module, application control module, and security audit module. The policy control module's functions and the kernel layer control module complement each other. The access control security of resources is achieved through three significant policies: access control, port control, and authentication. After the application software is downloaded to the terminal, the application deployment and installation module verify the legality of the source's source and data integrity to ensure that the source of the application software is legitimate and has not been tampered with. In running the application, it is necessary to access the system resources or other application resources through the access control module to prevent the application software from accessing the relevant resources without authorization. The data storage module's function is to encrypt and protect the locally stored business data of the terminal application software to prevent the application software data from being illegally tampered with or leaked. The security audit module uses tools to realize automatic log analysis to monitor the application software running status. Once the software is found to be running abnormally, an alarm will be triggered to ensure the application software's safe operation.

![Application Control Flow](image)

**Figure 3. Application Control Flow.**

**Center side.** The center side mainly includes the end device control module, security application store module, and security audit module. The terminal device control module is similar to the functions of the kernel layer. The access control module aims to assign different permissions to different end-users to achieve safe and correct resources. Currently, there are two central access control policies:
dynamic authorization and denial of implicit access. The port control module on the leading site needs to monitor all connected smart terminals’ usage activities continuously. Whenever an unauthorized end device connection occurs, the system issues an alert and provides a detailed report of the blocked device. The central side determines whether or not to grant certain privileges to the device based on the reports’ analysis and pre-set access policies. The authentication module is mainly responsible for authenticating each terminal device to ensure that each terminal connected to the central side is secure and reliable. When the terminal establishes a connection with the central side, two-way authentication is required for the central side and the access terminal device. When communicating, the central side and the terminal need to periodically refresh the authentication for authentication and real-time monitoring of the online status of the terminal, and timely interrupt the connection with the terminal device when problems are found [7]. To ensure the security of the application software, the secure application store should be the only platform for the terminal to download the application software, which is responsible for testing and reviewing the application software to be uploaded and transmitting data to the application download module on the terminal side. The application has to go through the steps shown in Figure 4 from the developer to the end-user. In the safety audit module, the terminal device regularly reports the operation safety logs. The center side uses the log analysis module to automate log analysis with tools, extract essential information, and monitor the terminal operation status. This module can make corresponding feedback to different levels of logs so that if there is a problem with the terminal, it can find and respond in time to ensure the safe operation of the terminal equipment.

Figure 4. Secure App Store.

4.3. Security protection strategy of intelligent power terminal at the communication layer

Cryptographic Module. The cryptographic module is based on ECC’s SM2 asymmetric key algorithm, which connects the central and terminal sides respectively, while the SM2 algorithm has the advantages of high immunity to interference, low computation volume, and low memory footprint, which is in line with the computing performance and storage space requirements of the power distribution system. Also, the Elliptic Curve Digital Signature Algorithm (ECDSA) can be used to encrypt any control commands
such as remote disconnect/connect and real-time pricing changes. The encryption process is shown in Figure 5.

**Figure 5. Encryption Flowchart.**

**Network access control module.** The network access control module is mainly divided into two parts: network isolation and identity authentication. The network isolation module's function is to isolate the system from harmful network security threats to protect the power data in a safe and reliable network for interaction. Applicable to the power system security isolation technology is mainly universal gateway technology and server-side isolation technology. The function of the authentication module is to authenticate the legality of the terminal device. Each terminal device holds a public-private key pair that can prove its unique identity, signed by SA. The authentication process can be divided into three steps: access authentication, session key establishment, and refresh authentication [8].

**Intrusion detection module.** The intrusion detection module mainly consists of setting up a firewall and establishing an intrusion detection system. The establishment of a firewall can effectively prevent external systems' intrusion, thus ensuring the intelligent power terminal's information security. The traditional firewall technology has packet filtering firewall, transparent firewall, and application gateway firewall, but also some new firewalls with better performance, such as deep detection firewall, which can be directed to the internal traffic after the detection of network information; traffic filtering firewall embedded with proprietary protocols that can filter packets on the application layer, the ability to reorganize data retention, and then the reorganized traffic Embedded firewalls embed firewall software into hardware facilities or gateways, which primarily protects data at the network layer, but not at the application layer [9]. An intrusion detection system's function is to analyse the collected system information using intrusion detection technology to detect whether there are security risks within the system. The implementation of intrusion detection technology can be divided into two stages: prevention of intrusion and unfamiliar network signal access, including intelligent intrusion detection, distributed intrusion detection, database intrusion detection, and wireless network intrusion detection [10].

**Secure access module.** This module realizes the communication between the production control area and the security access area by building horizontal and vertical interconnection schemes to achieve security isolation and identity authentication between the power grid's leading site and the intelligent
power terminal. The forward and reverse isolation device is installed at the two zones' junction to achieve physical isolation. In contrast, the encryption and authentication device is installed between the public network front switch and the public communication network to perform authentication and data encryption and decryption to secure data transmission.

**Monitoring and filtering network traffic module.** The monitoring and filtering network traffic module monitor and filters the traffic in the network to ensure that the traffic entering the network is credible and avoid network traffic attacks, for example, by monitoring periodic attack signatures and accompanying substantial traffic filtering to resist low-rate TCP attacks.

**Protocol analysis module.** The communication carried out by intelligent power terminals must use security protocols, such as IPSec (Internet Protocol Security), SSL (Secure Socket Layer)/TLS (Transport Layer Security) and SSH, encryption, firewalls, user access control mechanisms, etc., to avoid unauthorized tampering or penetration [11]. The protocol analysis process is shown in Figure 6.
5. Conclusion
As an essential component of the smart grid, it is essential to ensure intelligent power terminal devices' security. In this paper, we analyze the security threats faced by intelligent power terminals and propose three-layer security protection based on previous research, namely, "physical layer," "operating system layer," and "communication layer." framework. By analyzing the three levels of intelligent power terminal, a corresponding defense strategy is proposed, hoping that this will comprehensively improve the security and reliability of the existing intelligent power terminal equipment.

The security protection of intelligent power terminal equipment is of paramount importance, and the task of security protection is a long way to go. The protection strategies proposed in this paper provide theoretical guidance and suggestions for the security protection of existing intelligent power terminal devices, hoping further to improve the power system's security protection system and enhance the smart grid's security.

References
[1] Iran's Nuclear Agency Trying to Stop Computer Worm. Tehran: Associated Press. 2010-09-25[2010-09-25].
[2] Information on http://www.tele-graph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-word-first.html.
[3] HU Bo, WANG Xiao-ping. Embedded System Security Analysis and Countermeasure [J]. Computer Knowledge And Technology,2008(29):295-297.
[4] JIANG Zheng-wei, WANG Dong2, WANG Huai-yu, YANG Ze-ming, LIU Bao-xu. Model for power smart terminal security assessmen [J]. Computer Engineering and Design,2014, 35(01):6-10.
[5] Hu Po, Li Lili. A Review of Cyber-Physical Security in Smart Grids[J]. Journal of Information Security Research,2019,5(12):1068-1075.
[6] Xin Wen. Security Requirements of the Smart Meters and Related Strategic Analysis [J]. Process Automation Instruction,2012,33(10):42-45.
[7] Zhao Bao-hua, Wang Zhi-hao, Wang Shui. Research and application of trusted identity authentication technology in power terminals [J]. Cyberspace Security, 2018, 9(07):19-22.
[8] CAO Bing-hua, MENG Fan-tao. Authentication Framework for Network Integration [J]. Information Network Security, 2012(03):49-51.
[9] Li Fei. Research on the application of firewall technology in computer network security [J]. Electronic Test, 2018(4): 67-68.
[10] YU Wei, ZHUANG, Yu-ce, MAO Feng-xiang, ZHOU Shun-Sheng. Research On Intrusion Detection System Based On Role Access Control [J]. Techniques of Automation & Applications, 2019(6):104-108.
[11] Kreutzmann, H., S. Vollmer, N. Tekampe, A. Abromeit," Protection profile for the gateway of a smart metering system. German Federal Office for Information Security," Tech. Rep, 2011.