Research on Security Control Mechanism of Power Distribution IoT Based on Trusted Computing

Yue Sun¹,a, Qiang Li², Bo Zhou³*, Wei Chen¹, Xiaotian Xu¹ and Gangjun Gong³

¹ State Grid Jibei Electric Power Co. Ltd. Research Institute, North China Electric Power Research Institute Co., Ltd., Beijing 100045, China
² CETC Cyberspace Security Research Institute Co. LTD, Beijing 100020, China
³ Beijing Engineering Research Center of Energy Electric Power Information Security, North China Electric Power University, Changping District, Beijing 102206, China

asun.yue.d@jibei.sgcc.com.cn
*Corresponding author’s e-mail: 13261326733@163.com

Abstract. Performing an in-depth study on the Power Internet of Things (IoT), it is known that the distribution network faces higher security risks due to a large number of terminals, various types of equipment, and the flexible access of each device to the distribution network structure and dynamic boundary. Therefore, it is urgent to make significant research on the security control mechanism for the power distribution Internet of Things, to realize the safe access of IoT devices in the Power IoT. Firstly, this paper analyses the shortage of power system security under the background of the IoT. Secondly, trusted computing technology is represented by the TrustZone and is deeply studied, and the feasibility of its application for the security of power distribution IoT is analyzed. Furthermore, the TrustZone-based security management and control architecture for power distribution novel IoT equipment is proposed, and its integrity measurement and trusted network connection process are analyzed. Finally, the security of this architecture is analyzed briefly.

1. Introduction

The Power Distribution Internet of Things (IoT) is an important support system for the "Three Type, Two Networks" development strategy of the State Grid Corporation of China. The "Active Distribution Network + Internet of Distribution Internet of Things" is also the fundamental foundation for promoting the development of regional energy Internet and integrated energy services[1]. Therefore, the security of the distribution Internet of Things will not only directly affect the safe operation of the distribution automation system and the distribution network, but also affects the overall smart grid and the energy Internet to a certain extent.

Judging from the overall situation of the current power system security protection scheme, the principle of zoning is adopted from the main station to the plant station, and boundary isolation is carried out. Some of these isolation uses forward and reverse physical isolation devices. Some use firewalls, and vertical encryption authentication devices are used in the vertical direction[2]. However, under the background of the construction of the ubiquitous power IoT, the current power system safety protection measures only involve the main station to the plant station, and the comprehensive safety protection measures at the terminal level of the power system IoT are generally weak or even missing.
The most basic and meaningful application of the IoT architecture in the power system is the application in the perception terminal layer of the power system. The power distribution IoT sensing nodes in the power system have the characteristics of a large number, a wide range of types, and a wide range of distribution. Most of the communication between the terminals adopt the power line carrier communication technology, and the communication frequency band is 230MHz[4]. It is precisely because of the characteristics of the same communication frequency band, scattered distribution area, and a large number of IoT terminals that the risk of malicious intrusion of various smart terminals has greatly increased.

2. Theoretical basis

2.1. Feasibility Analysis

Power distribution IoT has the characteristics of extensive interconnection, high intelligence, and open interaction, which makes its network access environment more complex and diverse. The terminal access to various IoT has become the weak point of the network. For this reason, it is particularly critical to analyze the safety protection technology of power distribution IoT, enhance its active defense capabilities, and improve the safety and reliability of various terminals[3].

Trusted computing, as a technology to ensure the predictability of information systems, is used in the research of the secure communication of power distribution IoT terminals, which can not only realize the integrity of the equipment itself but also realize the trusted access between the equipment. Trusted computing can be applied to the IoT in three ways[5]:

- For embedded platforms with weak computing performance, soft TCM design can be adopted, and only basic TCM functions need to be implemented, including integrity measurement and cryptographic calculations;
- For platforms that ARM is equipped with TrustZone and have low TCM performance requirements, TrustZone can be used to build a more complete TCM functional area, and then build the root of trust for the platform;
- Like the host platform, a TCM security chip is built-in/externally to build a complete TCM root of trust function.

Taking into account the characteristics of power distribution IoT equipment: a large number, a wide range of types, complex access methods, and many devices are equipped with ARM processors. Therefore, this article conceives the use of TrustZone trusted design to achieve the security and reliability of the power distribution IoT.

2.2. TrustZone

TrustZone is a hardware architecture designed by ARM for consumer electronic devices. It is used to build a security framework for consumer electronic products to resist various possible attacks. The typical structure of TrustZone is demonstrated in Figure 1.

![Figure 1. The typical structure of TrustZone.](image-url)
TrustZone conceptually divides the feasible execution environment into Secure World and Normal World. All operations that require confidentiality are performed in the secure world (such as password processing, data encryption, and decryption, security authentication), and the remaining operations are performed in Normal World (such as a various application)[6-7]. Secure World and Normal World are converted through Monitor Mode. Secure World and Normal World are equivalent to two different operating systems running on two sub-processors on the ARM processor.

Many high-performance ARM processors in the power distribution network can support the TrustZone architecture, which can be used to improve equipment safety.

3. Distribution IoT security management and control architecture based on trusted computing

The power distribution IoT consists of a main station, sub-stations, and power distribution terminals. To realize the safe and credible information interaction of the power distribution IoT, a power distribution IoT security management and control architecture based on trusted computing is proposed to realize the credible authentication between various layers and the integrity measurement of each device itself[8]. Its specific structure is demonstrated in Figure 2.

![Figure 2. The security architecture of power distribution Internet of Things based on trusted computing](image)

This architecture integrates the power distribution IoT structure and the power system security partition structure. According to the power system organization level, it is mainly divided into the main station layer, the plant station layer, and the Internet of Things terminal layer. At the same time, it also corresponds to the four-layer structure of the "Cloud, Channel, Edge, Terminal" of the power distribution IoT[9].

The plant station layer ("Edge") is composed of substations under the master station, switching station terminal equipment (DTU), feeder terminal equipment (FTU), and transformer terminal equipment (TTU)[10]. In this architecture, the sub-station level equipment is used as an edge computing platform to realize the management and control of the sub-station level equipment to the IoT terminal. For the security management and control of substation equipment, this solution adopts the second and third trusted root TCM construction methods. In this paper, a complete TCM
functional area was constructed by introducing the ARM system-based Trustzone into the sub-station. The integrity measurement of the sub-station and the secure and trusted communication between the master station and sub-stations are realized. The TCM functional area constructed by the TrustZone is located in the secure world, and the data in the secure world cannot be accessed and tampered at will.

The terminal layer ("Terminal") of the Internet of Things is composed of sensing devices (such as smart transformers, fault detectors, etc.) of the Internet of Things, and is responsible for collecting information on the Internet of Things. Due to the low computing power and weak performance of the terminal nodes of the Internet of Things, so in this architecture, the security protection measures for this type of equipment adopt the isolation of the Internet of Things to achieve security management and control.

4. An effective strategy of safety mechanism

The security management and control architecture of power distribution Internet of Things based on trusted computing is proposed above. This section mainly analyzes the trusted management of the main station layer, plant station layer and IoT terminal layer in the architecture, and provides some unique cryptographic service functions that can be verified, including trusted storage, trusted measurement, trusted report, and trusted authentication, which mainly analyzes the integrity measurement of devices in each layer and the trusted network connection between each layer[11].

4.1. TrustZone Integrity measurement

The trusted computing integrity measurement under the TrustZone structure is shown in the figure, the ARM processor is divided into the safe world and the non-safe world, and the TCM functional area is located in the safe world. The integrity measurement process is shown in Figure 3:

![Figure 3. integrity measurement process](image)

When the device starts, power is supplied to the TCM functional area first, and its internal root of trust measurement (RTM) is used as the starting point of integrity measurement. The Boot ROM is measured first, and then the Monitor is measured. Subsequently, the Bootloader, operating system, and software applications in the secure world and the non-secure world are measured respectively, and the trust chain is communicated level by level to realize the trustworthiness of the entire device. The measurement result is recorded by the platform configuration register PCR in the TCM functional area. The device can compare the pre-stored PCR value to determine whether the trusted chain of the device is expanded as expected, thereby achieving the purpose of integrity authentication.
4.2. Trusted network connection

Referring to the architecture of the ternary trusted network connection in Trusted Computing 3.0, the connection hierarchy diagram of the power distribution IoT is shown in Figure 4. The ternary includes plant equipment, master server, and safety management centre.

The plant station equipment is the party that is connected to the master site server, and the master site server is the responder to the access. The function of plant station equipment in the protocol is to issue an access request and complete the two-way user identity authentication with the master station server. The plant station collects the integrity measurement value and sends it to the master station server to complete the two-way trusted platform evaluation with the master station server. Perform access control based on the results generated by the Security Management Centre in the process of user identification and trusted platform evaluation. The Security Management Centre is responsible for formulating trusted platform evaluation strategies and assisting plant equipment and master server to complete two-way user identity authentication. The security management centre verifies the validity of the PIK certificates of both parties, verifies the integrity of the platforms of both parties, and generates identity authentication and trusted platform evaluation results.
The ternary trusted network connection interaction data is shown in Figure 5. The detailed description steps of the trusted network connection are as follows:

**Step 0:** Before establishing a network connection and performing integrity check, both the plant equipment and the master server connected to the trusted network need to initialize the integrity collection module. The integrity measurement mechanism generates its credible report as 4.1 include PCR and SML (Prepare for step 3).

**Step 1:** Establish a communication channel between the plant equipment and the main station server, and guarantee the confidentiality of the communication channel data through the session key. The channel should be in a restricted state and only support the interaction of trusted connection-related information between the two parties. Plant station equipment sends an access request to the master station server $Q1$, the master server responds to the request, and negotiate the communication key.

**Step 2:** After the master server accepts the access request, the master server performs two-way identity authentication with the plant station equipment and the security management center. The security management center is a trusted party. The plant station equipment sends its identity information $V1_{ID}$ and identity key $PIK_{V1}$ to the security management center for comparison. The master server sends its identity information $V2_{ID}$ and identity key $PIK_{V2}$ to the security management center for comparison. The security management center feeds back the identity authentication result according to the comparison result $PIK_{result}$. Both parties control the local port based on the result of user identification.

**Step 3:** After the user's identity authentication and key negotiation are successful, the master station server and plant station equipment respectively send the identity authentication result $PIK_{result}$ to the trusted network connection party and the trusted network responder.

**Step 4:** The trusted network connection party and the trusted network responder receive successful feedback, and the plant equipment sends its integrity report $V1_{PCR}$ and measurement log $SML1$ to the security management center for verification. The main site server sends its identity information $V2_{PCR}$ and measurement log $SML2$ to the security management center for verification. The security management center implements the trusted platform evaluation protocol, performs trusted platform evaluation on trusted network connection parties and trusted network responders, and completes platform identity authentication and platform integrity verification.

**Step 5:** The security management center uses the integrity check module to verify the integrity of the plant equipment and the master server during the trusted platform evaluation process, and finally generates the trusted platform evaluation results of the plant equipment and the master server and send the evaluation results to both parties. The plant station equipment and the master site server determine whether to establish a trusted connection based on the verification result of the security management center. Both the network requester and the access controller will get complete platform identity authentication and integrity verification, so the trustworthy verification work controlled by the administrator can be implemented to prevent the access controller from being destroyed, and it can also prevent collusion attacks on both ends of the connection.

### 5. Summary

This paper proposes a security management and control mechanism for power distribution IoT devices based on trusted computing. In this power distribution IoT architecture, trusted computing based on TrustZone is used to achieve integrity measurement and trusted network connections. The starting point of integrity measurement starts from the root of trust, and the trust chain is passed through the trust measurement mechanism. Whether it is the top-level application or the bottom-level BIOS boot loader, before being executed, it must undergo integrity measurement verification operations, so device integrity is guaranteed. For the ternary trusted network connection, it can be seen from the process of trusted connection that its evaluation results and decision results are controlled by the inspection decision manager. It can also perform comprehensive verification of network requesters and access controllers. Both the access requester and the access controller can execute control
commands according to the situation. This enables the trusted connection to serve a centralized controlled energy network environment meeting a variety of customized security and trusted requirements, and also meet the requirements of the power distribution Internet of Things.

Acknowledgments
We would like to express our sincere gratitude to everyone who helped in this research work. This project is supported by the Science and Technology Project of State Grid Jibei Electric Power Co. Ltd. (52018K190024) and the General Program of Fundamental Research Funds for the Central Universities in 2020 of North China Electric Power University(2020MS084).

References
[1] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, (2019) IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices, IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201.
[2] M. Frustaci, P. Pace, G. Aloisi and G. Fortino. (2017) Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. In: IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495.
[3] Y. Gong, C. Chen, B. Liu, G. Gong, B. Zhou and N. K. Mahato, (2019) Research on the Ubiquitous Electric Power Internet of Things Security Management Based on Edge-Cloud Computing Collaboration Technology. In: 2019 IEEE Sustainable Power and Energy Conference (iSPEC), Beijing, China, pp. 1997-2002.
[4] Z. Georgiopoulou and C. Lambrinoudakis. (2016) Literature Review of Trust Models for Cloud Computing. In:2016 15th International Symposium on Parallel and Distributed Computing (ISPDC), Fuzhou, pp. 208-213
[5] J. Yuan and X. Li, A (2018) Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion. In: IEEE Access, vol. 6, pp. 23626-23638.
[6] H. Sun and H. Lei. (2020) A Design and Verification Methodology for a TrustZone Trusted Execution Environment," In: IEEE Access, vol. 8, pp. 33870-33883.
[7] ZHENYU NING, FEIWEI ZHANG, WEISONG SHI. (2019) A Study of Using TEE on Edge Computing. Journal of Computer Research and Development. 56(07) :1441-1453.
[8] L. Chen, M. Jia, X. Yuan, L. Zhao and Y. He.(2019) A Robust Framework Design of IoT Monitoring Device for Power Distribution Network. In:2019 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Macao, Macao, pp. 1-4.
[9] L. Chen, X. Dong, X. Kuang, B. Chen and D. Hong.(2019) Towards Ubiquitous Power Distribution Communication: Multi-service Access and QoS Guarantees for IoT Applications in Smart Grid. In: 2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia), Chengdu, China. pp. 894-898.
[10] Chen, H., Wang, X., Li, Z. et al. (2019) Distributed sensing and cooperative estimation/detection of ubiquitous power internet of things. Prot Control Mod Power Syst 4, 13.
[11] L. Guan et al. (2019) Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and Physical Space for ARM. In:IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 3, pp. 438-453.