Security Management for Apps of Intelligent Substation Based on Blockchain Technology

Wang liang¹, Zhang chengwei¹, Chen hanyun¹, Li yangsen², Wang yanguo³, Sun chao³, Ge liqing³, Tian hua*, Teng jingyu³, Wang jianfeng³

¹Economic Technology Research Institute, State Grid Fujian Electric Power Co., Ltd., 350001 Fuzhou, China
²State Grid Fujian Electric Power Co., Ltd., 350001 Fuzhou, China
³NR Electric Co., Ltd, 211102 Nanjing, China
* Corresponding author: tianh@nrec.com

Abstract. There are many kinds of professional apps in station control system of intelligent substation. In this open and shared ecosystem, there are great security risks in app authorized installation, resource control, access control, and border protection. In this paper, a new approach of app security management based on blockchain technology has been proposed. By using the mechanism of tamper free and traceable "ledger" based on cryptography, the objective and traceable supervision of app's life cycle can be implemented through customization of blockchain's ledger. This paper provides a new solution for app security management of station control system in intelligent substation.

1. Introduction
In order to facilitate the flexible expansion of applications and respond to the demand changes of intelligent substation quickly, the station control system adopts the mode of open platform and professional apps. In this mode, the basic platform uses the unified modeling of the whole station information, the unified data collection and management to provide standardized service access interfaces such as resource management, data management, public service and application management. So flexible expansion of various applications can be implemented. Through the construction mode of platform plus app, we can strive to create a co construction, sharing and open ecosystem, which contains many kinds of professional apps. In this open and sharing ecosystem, how to manage apps in this platform of the station control system safely is the top priority.

The key to the security risk of apps in this platform can be divided into the following situations:
• Unauthorized and tampered installation of apps.
• Unauthorized access to IP addresses outside the network address range.
• Excessive consumption of system’s CPU, memory, disk and network resources.
• Unauthorized access to external file directory.
At present, research has been done on blockchain technology for the power industry in many aspects, which mainly focus on the application of public blockchain in power trading and other fields. The station control layer of intelligent substation can access to the public chain through the safety zone III server, which has great potential to improve its automation and intelligent level. First, in the current three-tier two network environment of intelligent substation, the configuration of substation mainly occurs in the network of station control layer, and the total number of nodes is small. Second, blockchain is based on the mechanism of non tampering and traceable "ledger" of cryptography, which is suitable for monitoring the update of configuration objectively. By customizing the content of block ledger, it is easy to locate fault point when problems occur. Third, smart contract provides a mechanism to implement version replacement based on program code automatically, and most of the content for version management can be recorded automatically. Fourth, the consensus mechanism eliminates the unauthorized modification of app's version and data, so that every modification of version and data are involved in the "shared ledger", thus the loopholes that may exist in the process of app's life cycle can be avoided. Fifth, the station network environment is generally an independent network. Blockchain related technologies can provide more security prevention means, which are based on the existing security management and network prevention.

Therefore, in order to improve the efficiency of platform app's security management and ensure the system security in the process of app's life cycle, this paper proposes a complete set of blockchain based security management method for apps of station control system platform. Based on the ledger mechanism of non tampering and full traceable cryptography, the objective supervision of non tampering and traceability of app can be implemented. So the app's security problems such as unauthorized and tampered installation, illegal access to network, excessive occupation of system resources, unauthorized access to app file directory can be solved effectively.

2. Security Management Architecture of APP Based on Blockchain

In accordance with the provisions of power system security protection, a blockchain server is configured in the security zone III of the intelligent substation. And then, a blockchain client is deployed on the blockchain server to access the distributed ledger and provide an access interface to the security zone I. Therefore, the architecture of station control system 's app, which is based on blockchain, is as follows.
Fig. 2. Architecture of station control system.

Fig. 3. App platform architecture of station control system.

Substation operators can generate public key and private key of app management and maintenance through blockchain server. There are also risks in the above technology and management endorsement. Risks include such as the relevant algorithms are broken, key is leakage, etc. Then the relevant algorithms and management measures also need to be updated synchronously. The signature with private key of app manager can be used to submit security registration information, which includes public key of app information maintenance and number of current apps, to generate global configuration of app security management, as follows.

After the testing of an app was completed in station control system, the engineer signed and submitted the hash of app image file and app information with the private key of app information maintenance. Finally, the global configuration of app security management was updated with the private key of the app maintenance, which was implemented in the form of transaction on blockchain.

![Data structure of Global configuration For app security management](image-url)
3. Flow of Application

The flow chart of the application shown in Fig.6.

Step1: When the app manager on the host of station control system receives the installation request of an app (testapp) image, the host reads the latest global configuration of app security management signed by the private key of app management by connecting to the block chain server in security zone III. The app manager calculates the hash of testapp image file which will be installed. The app manager check whether the hash of testapp mage file is consistent with the hash of image file involved in the app information configuration from the global configuration of app security management. If not, the verification fails and the installation exits. When the verification is finished successfully, the app manager continue to execute the image installation of testapp and then starts to run after the installation is completed.

Step2: During the running of testapp, the app manager on the host of station control system connects to the block chain server in security zone III and reads the latest global configuration of app security management, which is signed with the private key of app management. Based on the global configuration, the network access behavior of testapp is monitored in real time. If it is detected that testapp has access to IP and port outside of its corresponding network configuration, app manager will stop the running of testapp.

Step3: During the running of testapp, the app manager on the host of station control system connects to the block chain server in security zone III and reads the latest global configuration of app security management, which is signed with the private key of app management. Based on the global configuration, the resource occupation behavior of testapp is monitored in real time. If it is detected that testapp occupies more CPU, memory, disk and network resources than its corresponding resource allocation limit, then app manager will stop the running of testapp.

Step4: During the running of testapp, the app manager on the host of station control system connects to the block chain server in security zone III and reads the latest global configuration of app security management, which is signed with the private key of app management. Based on the global configuration, the file directory access behavior of testapp is monitored in real time. If it is detected that testapp has access to the file directory behavior other than its corresponding directory configuration, then app manager will stop the running of testapp.
4. Safety Analysis

As an app application environment has been connected to the public chain through security isolation device, the specific security problems faced by this paper mainly include as follows:

1) Risk of blockchain technology

Set DATA as the original data in the process of security management for apps of intelligent substation, then related configuration data and signature of the app received by app manager can be expressed by formula (1) respectively

\[ A = \text{SIG}(\text{HASH}(\text{DATA})) \]  \hspace{1cm} (1)

Among them, A represents signature of configuration. HASH represents hash function. For example, SHA-256 algorithm can be directly used. SIG represents the process function of encryption with private key. There are many options for asymmetric encryption algorithm, such as ECC. After the signature and data have been received, the system verifies the signature, which is used to judge whether formula (2) is true or not.

\[ \text{HASH}(\text{DATA}) = \text{UNSIG}(A) \]  \hspace{1cm} (2)

Among them, UNSIG represents the process function of decryption with public key corresponding to SIG. In the running process of app manager, it is necessary to verify whether the public key has permission for configuration, and then execute the judgment process of formula (2). If the equation is right, the signature is verified successfully. When blocks were generated, a block includes configuration data of multiple app information, which are represented by D1, D2, D3, ..., then the process of generating hash value of this block is shown in formula (3).

\[ \text{hash} = \text{HASH} (\text{Merkle} (\text{HASH}(D1), \text{HASH}(D2), \text{HASH}(D3), ...)) \]  \hspace{1cm} (3)

Among them, hash represents the hash value of the block. Merkle means to generate the root value of Merkel tree according to the hash value of each app’s information data in this block. The above hash function, Merkel tree and asymmetric encryption algorithm are the technical support and guarantee of this scheme. At the same time, private key security, authority management for station control layer host are the management requirements of this scheme. There are also risks in the above technology and management endorsement. Risks include such as the relevant algorithms are broken, leakage of key, etc. Then the relevant algorithms and management measures also need to be updated synchronously.
2) App data tampering and malicious attacks
If you change the app version without permission, you can't do it online successfully. Even if you get this key, the manager will still report the information to the app manager. And the information will finally enter the blockchain after the app configuration is completed, so it can't be hidden.

3) Economic Attacks
Unlike similar systems, security management must also concern itself with attacks on payment mechanisms. We can use the mature technology based on public chain to prevent these attacks in this paper.

4) Sybil Attacks
Malicious actions, performed by pretending to be multiple users, are termed Sybil Attacks, after a patient suffering from multiple personality disorder. We can use the mature technology based on public chain to prevent these attacks in this paper.

5) Eclipse Attacks
In an Eclipse Attack, the attacker's goal is to hide part of a system from itself. The methods employed are generally the network equivalent of privilege escalation attacks: gain control of network positions which have more control of the network, then use that control to acquire more control. We can use the mature technology based on public chain to prevent these attacks in this paper.

6) Man-in-the-Middle Attacks
Actions that can be performed only after inserting oneself between two interacting parties are collectively referred to as man-in-the-middle attacks. Encrypted information may be logged for analysis of metadata (Section 3), while non-encrypted data may additionally be changed to control behavior. If key exchange is not secured, the man-in-the-middle may also trick two parties into wrongly believing the attacker's key is the other party's key. We can use the mature technology based on public chain to prevent these attacks in this paper.

7) Denial of Service Attacks
Attacks centered around taking a specific resource online are termed Denial of Service Attacks (DoS). System behavior during "unexpected" circumstances is often poorly specified and tested. DoS attacks are useful for deanonymizing nodes in P2P networks. We can use the mature technology based on public chain to prevent these attacks in this paper.

8) Hacking
By converting historically trustworthy peers into attack vectors, motivated attackers might directly compromise nodes on the network. When bandwidth is deployed using Chains, iterative hacking may eventually allow an attacker to "backtrace" a connection. Such attacks have important security implications but are out of the scope of the blockchain network. We can use the mature technology based on public chain to prevent these attacks in this paper.

9) Confidentiality
The confidentiality of app data information in intelligent substation is mainly implemented by management means and horizontal isolation and vertical encryption mechanism. The confidentiality of data in the blockchain can also be achieved by adding encryption measures in the compression process.

10) Network traffic
Station control layer is mainly responsible for refreshing, collecting and monitoring the transmission data. Spacer layer is mainly responsible for controlling the transmission of data and relay protection signals. Process layer establishes the connection point between primary equipment and secondary equipment, and intelligent electronic equipment completes real-time electrical quantity inspection and operation equipment state parameters. Detection, operation control, execution and drive work. Among them, the types of messages transmitted by station control layer are the most abundant, and the functions covered by them are the most extensive. In this paper, the blockchain server is deployed in safety III, so it can't be affected by the network traffic of station control layer in safety III.
5. Conclusions

In order to facilitate the flexible expansion of applications and respond to the demand changes of intelligent substations quickly, the station control system adopts the mode of open platform and professional apps. In this mode, the basic platform uses the unified modeling of the whole station information, the unified data collection and management to provide standardized service access interfaces such as resource management, data management, public service and application management. So flexible expansion of various applications can be implemented. Through the construction mode of platform plus app, we can strive to create a co construction, sharing and open ecosystem, which contains many kinds of professional apps. In this open and sharing ecosystem, how to manage apps in this platform of the station control system safely is the top priority.

There are many kinds of professional apps in station control system of intelligent substation. In this open and shared ecosystem, there are great security risks in app authorized installation, resource control, access control, and border protection. In this paper, a new approach of app security management based on blockchain technology has been proposed. By using the mechanism of tamper free and traceable "ledger" based on cryptography, the objective and traceable supervision of app's life cycle can be implemented through customization of blockchain's ledger. This paper provides a new solution for app security management of station control system in intelligent substation.

At present, the blockchain technology has formed some stable technical characteristics, but it is still in rapid development, which requires continuous tracking and flexible selection. In the future research on the safety management of Intelligent substation, special attention should be paid to the progress of the blockchain technology in traceability, immutability, reducing storage capacity and improving operating efficiency.

Acknowledgement

This work is supported by a fund project: State Grid Co., Ltd. Technology R&D Project (Project Name: Research on Secondary System Design Technology of Intelligent Substation Based on Physical Information Fusion, Project No.: 5200-202056139A-0-0-00).

References

[1] LIU Junhong, DENG Zhaoyun, LI Zeke, et al. Automatic information verification technology of Intelligent substation based plug and play[J]. Power System Protection and Control, 2018, 46(2): 137-143.

[2] Satoshi Nakamoto. Bitcoin: a peer-to-peer electronic cash system[Online], available: https://bitcoin.org/bitcoin.pdf, 2009.

[3] Swan M. Blockchain: Blueprint for a New Economy. USA: O'Reilly Media Inc., 2015.

[4] YUAN Yong, WANG Feiyue. Blockchain: The state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[5] YUAN Yong, NI Xiaochun, ZENG Shuai, et al. Blockchain consensus algorithms: The state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2012.

[6] SHAO Qifeng, JIN Cheqing, ZHANG Zhao, et al. Blockchain: Architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[7] CHEN Wei, ZHENG Zibin. Blockchain data analysis: A review of status, trends and challenges[J]. Journal of Computer Research and Development, 2018, 55(9): 1853-1870.

[8] ZHANG Ning, WANG Yi, KANG Chongqing, et al. Blockchain technique in the Energy Internet: Preliminary research framework and typical applications[J]. Proceedings of the CSEE, 2016, 36(15): 4011-4022.