An information security model of industrial control network in the coal industry

Xu Jian Guo, and Tian Chuan*

Shandong University of Science and Technology Department of Computer Science and Engineering,
Qingdao, Shandong 266590, China

Abstract. The coal mining industry is taking the development path of information industrialization and promoting the “deep integration of the two technologies”, which involves the construction and citation of many new technologies and new business models. With the introduction of cloud computing and big data technologies, data sharing is becoming more and more important. The industrial control system becomes more and more open, and the safety protection measures for the industrial control system are seriously lagging behind, leading to the extremely prominent information security problems of the industrial control system of the coal industry. This paper analyzes the industrial control system of the coal mine industry, researches the specificity of the coal mine industry and its applicable protection technology, and combines IEC62443, GB/T30976 and other industrial control system safety general technical standards, and proposes a coal mine industry industrial control network information security model.

1 Introduction

With the acceleration of industrial control system (Industrial Control System, ICS) and information technology (Information Technology, IT), the originally closed and independent industrial control system began to use cloud computing, big data and other technologies for data storage and analysis [1]. In this process, the industrial control system is faced with multiple threats from external networks. In traditional industrial control systems, data is transmitted in clear text. If the plain text data is directly sent and stored to the cloud platform, it may cause data Threats such as leakage and tampering have caused irreparable losses to the safe operation of industrial control systems. In recent years, countries around the world have put forward some very useful indicators and guidelines for safety practices. China has also promulgated the “ Cyber security Law of the People's Republic of China ”, proposing to strengthen the security protection of key information infrastructure and maintain national cyber security. [2].

---

*Corresponding author: Email: io1996.chuan@gmail.com

2 Industrial control network security status

Network security management lags behind

At present, many domestic coal mining companies have relatively vague concepts of network security, and their security awareness is not strong. In particular, old managers of some enterprises randomly request DCS (Distributed Control System, distributed control system) manufacturers to add network interfaces, change the network topology, and mess up management of important places such as computer rooms, dispatch rooms, and information centers, and use them in the DCS system at will. U disk copy data, etc., bring a great hidden danger to the entire industrial control network information security [3].

Industry-specific security risks

(1) Disorganized non-standard communication protocol

In addition to the international and national standard communication protocols, the industrial control system of the coal industry also has many industry standard protocols and private protocols, such as: MT1116 data exchange protocol based on industrial database, private protocol based on RS232 bus, Modbus serial communication protocol, etc. , The protocol is messy and mostly plain text transmission protocol. At the beginning of design, most industrial control protocols only consider the efficiency, function and reliability of the protocol, and do not consider the security of the protocol. Even within the dedicated network of the control system, it is easy to Implement monitoring and tampering data on the nodes to launch attacks. Traditional industrial communication protocols have been difficult to meet the security requirements of modern information systems [4].

(2) Special policy requirements

The state and industry have formulated a series of regulations to regulate the production and operation of the coal industry, and the National Coal Mine Safety Supervision Bureau has networking requirements for real-time data on coal mine safety monitoring and monitoring, and safety protection must comply with relevant policy requirements.

(3) Special network topology

Mine ring industrial Ethernet is a flat network topology, all devices on the ring network are interconnected, and virus worms can quickly spread in the industrial ring network [5].

In general, coal mine enterprises still do not have enough knowledge about the safety of industrial control systems, generally lacking due information security protection measures and due protection responsibilities. In the path of new-type industrialization development, insufficient supporting safety measures, industrial control system information of the coal industry The security situation is very grim [6-7].

Information security model of industrial control system in coal industry

According to the current status of coal mine production network security, combined with the management requirements in the “Industrial Control System Information Security Protection Guide ” issued by the Ministry of Industry and Information Technology, an industrial control system information security model is proposed, as shown in Figure 1, to ensure that

- (1) Only trusted devices can access the industrial control network.
- (2) All data is encrypted and transmitted on the industrial control network.

- (3) All operation requests are recorded.
- The main changes between this model and the traditional industrial control network model include two-way authentication technology, data encryption module, internal access control plug-in, border access control hardware and security audit module. Their functions are:
- (1) Two-way authentication technology: prevent ARP spoofing attacks and illegal device access.
  - (2) Data encryption module: The encryption implemented by the SSL proxy provides backward compatible data encryption.
  - (3) Internal access control plug-in: implemented by a lightweight plug-in to block various areas of the internal network and prevent the internal spread of viruses.
  - (4) Boundary access control hardware: A firewall device built with reliable hardware and software is used to isolate the internal and external networks of the industrial control network.
  - (5) Security audit module: The main function is to record security logs and provide security audit reports for security administrators.

Fig. 1. Industrial Control Network Information Security Model

3 The key protection technology for the applicability of industrial control systems in the coal industry

There are many devices and nodes in the communication network of the industrial control system that can become the entrance of malicious network attacks. The vandals can easily access, steal and tamper with the plain text data uploaded by the industrial control commands or data collection equipment.

Traditional industrial communication protocols (such as Modbus protocol) have been widely used for many years, and it is unlikely to change in a short period of time. At the same time, a large number of mature and stable host computers and industrial control equipment use traditional industrial communication protocols, so data encryption must ensure compatibility with traditional Industrial communication protocol.

As a security protocol based on the transport layer, SSL provides encryption and data integrity for network calls [4]. Install an SSL proxy client on the industrial communication gateway to accept the data request of the original data collection device or host, establish an encrypted transmission channel, convert the original data into SSL protocol encrypted data, and send it to the DCS equipped with SSL proxy server In the center or private cloud storage, the SSL proxy service decrypts the encrypted data into plain text data. The plain text communication protocol originally supported by the device receives the plain text data and executes the original business logic.

Fig. 2 SSL proxy traditional industrial communication network

The main function of two-way authentication is to ensure the legitimacy of the client (device and its users) and the server (cloud) [1]. Before using the device or host, employees insert the U shield into the USB interface. The U shield has built-in encryption algorithms and Client_seq, which identifies the employee's identity, is stored in the U-Shield with the serial number and keyword KEY of the unified constraints of the client and server. External programs need to use the agreed interface to read the data and calculation results in the U-Shield.

- (1) Two-way authentication can ensure that the device or host is connected to the correct server, which can effectively prevent ARP spoofing attacks.
- (2) Two-way authentication can ensure that the device is not illegally used by non-employees.

Taking the AES algorithm as an example, the flow of two-way authentication is shown in the figure:

The server generates a random number `Server_rand`, and transfers the random number to the server's encryption lock, and calls the encryption method in the encryption lock. The encryption method reads the server serial number `Server_seq` and key `KEY` in the encryption lock, and combines it with the random number `Server_rand` to encrypt the incoming value, and then calls the AES encryption algorithm provided by the encryption lock to output the ciphertext. Finally, it is transmitted to the client through SSL communication.

The client passes the received ciphertext, `Server_rand`, and `Server_seq` to the encryption key of the client together. The encryption key calls the verification algorithm, reads the key `KEY` in the encryption key, and combines with the random numbers `Server_rand`, `Server_seq` to form an encrypted incoming value Then call the AES encryption algorithm provided by the dongle to output the ciphertext. Finally, the ciphertext is matched with the ciphertext transmitted from the server, and the matching result is returned. At this point, the server verification is over.

If the server authentication is successful. Client verification will be performed, the process is the same as above.

Fig. 3. Two-way authentication process

Access control

The main function of access control is to filter resource access requests issued to any node in the industrial control network.

- (1) On the boundary between the industrial control network and the private cloud, access to firewall-based hardware protection equipment is the first line of defense to protect the internal network, isolate the interior of the industrial control network, and generally choose reliable and mature firewall products.
- (2) On the data collection equipment or industrial protocol gateway within the industrial control network, complete the two-way authentication and establish the connection based on the whitelist and identity-based access control strategy. Due to the large number of nodes, it is not appropriate to use expensive firewall equipment, generally using plug-ins Implementation, as shown in Figure 4. The whitelist-based access control strategy is more cautious than the blacklisted access control strategy. Only people in the terminal's whitelist

can use the device, and the access control of any resources they access can effectively prevent employees or malicious personnel from The unauthorized use of equipment records the use of equipment through security audits.

Fig. 4. The access control process used inside the network

Security audit

Enable user-level security audits for the entire industrial control network, mainly including login status, login identification number, date and time of attempt to log in, date and time of log out, equipment used, content running after login, network requests attempted after login , Files and resources accessed by users.

The log file can choose to record part or all of the event content according to the security intensity requirements. Usually for a single event, the log should include the time of occurrence, the user who caused the event, and the event results.

Since the audit system is the direct evidence for tracking and recovery, it is of great significance for accountability after the fact. Therefore, the storage and review of audit reports and log files must have strict security requirements. The storage system should prevent unauthorized modification, deletion and access.

Fig. 5 Security audit module

Intrusion detection

Intrusion Detection System (IDS) is an automated software and hardware combination system that performs intrusion detection monitoring and analysis. It monitors data traffic behind the firewall in real time and is the second line of defense behind the firewall [8]. IDS monitors and analyzes the activities of users and systems, identifies abnormal behavior patterns, finds behaviors that meet the characteristics of attacks or signs of being attacked in industrial control networks, and sends alarm logs to security administrators to enable them to intervene as quickly as possible to deal with intrusions , The damage is controlled to a minimum, the attacked logs can also be played back as judicial evidence.

Fig. 6. Intrusion detection module

4 Conclusion

The coal industry control network information security model proposed in this paper solves the following problems by standardizing the network structure:

Data encryption prevents information from being illegally stolen or altered. Two-way authentication solves the problems of identity authentication, unauthorized access and unauthorized device access. Two-layer access control isolates different areas of internal and external networks and internal networks, making it difficult for virus worms to spread. Intrusion detection and security audit provide technical support for security accident investigation and evidence collection.

In general, the model proposed in this paper can better solve the problems existing in the traditional coal mine industrial control communication network.

References

1. T. Yuanfei, S. Qingjian, Y. Geng, *Journal of Electronics and Information Technology*, **42:2** (2020)
2. L. Trautman, et al., *University of Miami Law Review*, (2017)
3. Y. Weiqiang, Ch. Ke, Zh.Chunshan, et al., *Instrumentation Users*, **26:06**, 38 (2019)
4. G. Ruiqiang, Zh. Hong, J. Lidong, et al., *Chemical Engineering Design Communication*, **45:01**, 129-131 (2019)
5. W. Yantao, D. Ping, X. Fanxue, *Member Congress of Shandong Coal Society and Coal Mine Geothermal Prevention Academic Forum*
6. Zh. Xiaohu, Zh. Kai, Zh. Zhikai, et al., *Industrial and Mine Automation*, **044:004**, 1-7 (2018)
7. Ch. Zhigang, *Electronic Technology and Software Engineering*, **000:009**, 187-187 (2017)
8. Y. An, S. Limin, W. Xiaoshan, Sh. Zhiqiang, *Computer Science - Research and Development*, **9**, 2039