DOI: 10.53469/jtpes.2023.03(04).02

Industrial Internet Situation Awareness System and Application

Xuejie Yan

Caofeidian College of Technology, Tangshan, Hebei, China

Abstract: ***With the development of technology and economy in the current society, industrial enterprises are experiencing the transformation of "informatization", "digitalization" and "intellectualization". The network of industrial enterprises is no longer a closed network, but more of a large and interconnected network. Only in this way can the regulation effect of industrial Internet industry be brought into play. While the management and production mode are changing, new network security threats are also introduced. Through the terminal, network, application and other different levels of the industrial control network device network probe, data collection and summary to fully perceive the security of the network. The situation awareness system of industrial Internet is composed of four modules: data acquisition, data storage, data analysis and data presentation. Data acquisition is the basic part of the system, which provides data sources for data analysis and data presentation. In this paper, according to the requirements of Industrial Internet Security Framework, combined with the current industrial technology, the security perception system is designed.***

Keywords: Industrial Internet; Situational awareness; Data acquisition; Data storage; Data analysis; Data presentation.

1. INTRODUCTION

1.1 Background

Electric power, energy, chemical industry, transportation, water conservancy, metallurgy, aviation and other industries are the lifeline industries of the state-owned economy. The industrial control system in these industries is to guarantee the normal operation of the industry, and is an important part of the industrial Internet. All kinds of control equipment and systems in the industry are gradually connected from the enterprise Intranet to the Internet. Network security attacks also gradually threaten the equipment in the industrial interconnection. Illegal attackers and hackers at home and abroad scan the system and application software vulnerabilities through various tools, and implant offensive tools such as viruses and trojans on important industrial equipment and systems. To threaten to attack important industrial equipment. Once such equipment is attacked, it will cause major accidents, have a serious impact on social order, endanger people's lives and safety, and even cause serious harm to national interests.

1.2 Policy

In November 2016, the Network Security Law was released, which for the first time mentioned network security to the national legal level, so that the network security incidents can be followed by laws. Issued by the State Administration for Market Regulation in May 2019. The Network Security Level Protection 2.0 standard system has been released, which for the first time includes cloud computing security, mobile Internet security, Internet of Things security, industrial control system security and other requirements under standard jurisdiction. In January 2020, the "Cryptographic Law" has been officially implemented, mainly affecting the application of business secrets (electronic signature, etc.) and improving the penetration rate of cryptographic mechanism in network security. In November 2017, The State Council issued the Guiding Opinions on Deepening the "Internet + Advanced Manufacturing Industry" to develop the Industrial Internet. In the guiding opinions, China's Internet security is planned from the top level and corresponding regulations are introduced, which fully demonstrates the importance the country attaches to Internet security. Industrial Internet security is the premise and guarantee of normal industrial production, through the construction of a complete industrial network security situation awareness technology system and service system, to meet the requirements of industrial safety and safety management emergency mechanism, so as to resist the risk of external attack and eliminate internal security risks, so as to ensure the healthy and orderly development of industrial Internet.

2. SYSTEM INTRODUCTION

2.1 System composition

Industrial control network security situation awareness can comprehensively monitor the physical, transmission and application levels of the industrial Internet, timely discover network attacks, system/software vulnerabilities, Trojan horses and malicious code attacks, defend against external attacks, reinforce internal hidden dangers, and conduct early warning aircraft for future security situations through existing security events. Effectively help security personnel control security risks, improve the overall level of industrial Internet security protection. The system mainly collects security day events, alarms and logs in the industrial Internet through the installation of network probes, gathers relevant data into the sensing platform, conducts business modeling on the data according to the business model used by users, discovers network anomalies and threat events in time, and presents the converged threats and anomalies to security maintenance personnel through the visualization platform. The

closed-loop management of security risks can be realized through alarm and event response detection, recording and tracking, disposal and management.

2.2 Module Introduction

2.2.1 Data Collection

For the industrial Internet, security information is collected from five aspects: equipment, network, control, application, and data security. Security information includes alarm notification, security events, and system logs. The sensing platform receives system logs from heterogeneous systems, processes them in a unified planning, and then stores and analyzes them.

2.2.2 Data Store

Alarm notifications and security events uploaded by the front-end probe are stored in a structured manner in a unified format. A large number of network audit data streams in network security are stored in half structure. For the original file system involving data security, the distributed file storage system is used.

2.2.3 Data Analysis

By classifying and collecting massive alarm and event data, the system performs real-time statistical calculation based on the streaming data, calculates the features of security hazards based on the correlation between alarms and events, and predicts security events based on historical data.

2.2.4 Application Rendering

Application presentation provides a visual interface, provides data presentation of different dimensions of network security alarms and events, and can form various reports according to user requirements. And handle major alarms through the work order process.

3. SYSTEM DESIGN

3.1 Data Collection

3.1.1 Device Security

Device security includes the physical security and system security of device endpoints. For devices connected to the industrial Internet, security vulnerability scanning and hardening must be performed, and corresponding security logs must be formed. At the same time, the system upgrade of device endpoints should be carried out in time according to the patches provided by device hardware manufacturers, so as to ensure that devices are protected from security attacks due to vulnerabilities.

3.1.2 Control Security

Control security can be divided into three aspects: control protocol security, control software security and control service security. Through the interface of the control software, the system logs of the control software can be obtained, the vulnerabilities can be scanned, and the security vulnerability alarms can be generated, and the sensing platform provides corresponding security hardening software packages.

3.1.3 Network Security

Industrial Internet is to realize the interconnection of each endpoint of industrial control equipment, the expansion of the network scope, the expansion of the scope of security, security audit of the network process and network equipment security monitoring, the formation of security alarms, events, logs and other information, for the perception platform to provide the basis for security display.

3.1.4 Application Security

Industrial Internet application security should also be protected from two aspects: industrial Internet platform security and industrial application security. For platform security, security protection should be carried out from vulnerability scanning, security isolation, attack defense, security audit and other aspects to form security alarms, events, and logs. For application security, it is necessary to conduct security monitoring from the aspects of application development, testing, deployment, operation and maintenance.

3.1.5 Data Security

For data security, including data collection, transmission, storage and processing, data security protection should be carried out in these links, and encryption technology can be used in these links to protect data. During storage and use, data leakage, damage, and loss are prevented. Logs or alarms are generated for these events and displayed on the situational awareness platform in a unified manner.

3.2 Data Storage

For the data collected by the system acquisition layer, there are mainly structured data (Production, alarm, event), semi-structured data (all kinds of streaming security logs, network security audit messages), unstructured data (network protocol transmission file system), the perception system respectively unified data cleaning, data modeling, data storage of three types of data. And the data storage for security backup management, to prevent attacks and tampering.

3.3 Data Analysis

The data analysis platform utilizes big data technology to carry out classified statistics and modeling calculation for massive alarms, and can adopt distributed computing method to horizontally expand the analysis and calculation capacity. The data modeling model is used for flow analysis and processing of massive probe logs, and the association model is used to associate alarms and normalize massive alarms, realizing the alarm merging function and reducing the workload of manual alarm troubleshooting. In addition, the alarm statistics and features are collected in real time, which provides the basis for the upper-layer to quickly display and analyze services.

3.4 Data Presentation

Upper-layer service applications provide application interfaces to display asset, alarm, and event data based on different dimensions (business, region, and responsible person/unit). Based on massive data, users can implement second-level responses to keyword queries. Users can customize service processing processes. According to the severity of the alarm, different order sending processes are triggered for the alarm to quickly operate and maintain security faults. In addition, you can customize various service reports based on customers' daily usage to reduce the workload of security maintenance personnel.

4. SCENARIO APPLICATION

This system is mainly in the field of industrial Internet, the industrial control network security of the vast number of industrial enterprises has monitoring, early warning function, the use of flat security monitoring ability, effectively strengthen the modern management level of enterprises. Electric power is an important foundation industry in our country, which concerns the people's livelihood. In recent years, the national grid develops rapidly in the direction of informatization, digitization and intelligentization. To ensure that the power supply device and the power supply system are local
The safe operation of the SCADA system can prevent major network security accidents from occurring in the system. When network security accidents occur, the SCada system can quickly locate the cause of accidents, quickly isolate faults and resume production. It can predict security accidents according to a large number of security event characteristics, report early warning signals, and change from passive network security protection to active perception defense stage, greatly improving the level of enterprise management.

5. CONCLUSION

By collecting data from five aspects including equipment, control, network, application and data, and realizing the lossless storage of highly concurrent data based on big data storage technology, the data is distributed and analyzed by a large number of business models to meet the requirements of multiple upper-layer application data display and business disposal, and the network security situation is perceived from the macro level. So that the security situation is "visible, manageable, controllable, and preventable", effectively meet the regulatory needs of government security departments and industry management departments, greatly improve the level of enterprise security management, at the same time, a large number of network security data collection, for the future industrial Internet security big data application, artificial intelligence technology (AI) intelligent prediction to lay the foundation, Thus, it lays a good data foundation for network security management unmanned duty.

REFERENCES

[1] XIA Bing. Network Security Law and Network Equal Protection [M]. Beijing: Publishing House of Electronics Industry, 2017.
[2] LU Genghong, FENG Dongqin. Industrial Control Network Security Situation Awareness Based on Improved C-SVC [J]. Control and Decision, 2017(7).
[3] Du Jiawei et al. Network Security Situation awareness: Extraction, Understanding and Prediction [M]. Beijing: China Machine Press, 2018.

[4] YAO Yu et al. Industrial Control Network Security Technology and Practice [M]. Beijing: China Machine Press, 2017.