The Overall Design and Application of Safety Protection for Industrial Control Systems

Peng Wu\(^a\), Maopu Wu\(^b\) and Jun Zhu\(^c\)

CSIC Information Technology Co., Ltd., Lianyungang 222006, China

\(^a\)dubyrd@163.com, \(^b\)wumaopu@126.com, \(^c\)huzi881210@foxmail.com

Abstract. According to the industrial Internet adaptive architecture security system, following the design principles of standardization, overall layout, and top-level planning, it adopts the defense-in-depth concepts of "vertical layering and horizontal partitioning", "boundary control, intra-domain monitoring and auditing, and overall centralized management and control". Aiming at the network security protection of enterprise industrial control systems, it is focused on breakthroughs in technologies of multi-element acquisition and fusion, defense-in-depth security analysis, visual integrated situational awareness. An industrial control network security integrated protection platform has been constructed to realize real-time perception of industrial control security risks and accurate research and judgment of threats. After practical application verification, it is meets and suitable for the safety protection requirements of industrial control enterprises, and provides reference value for the construction of industrial control network security protection in the shipbuilding industry and other industries.

1. Introduction

With the rapid development of big data, the Internet of Things, and cloud computing, the intensified network security has become a new challenge for national security, and national key information infrastructure may be threatened by network security at all times. In recent years, some types of security incidents such as Iranian Seismic Network and Ukrainian Power Grid have shown that the field of industrial control has become a new battlefield for information security and even national security. In May 2017, the "WannaCry" incident that swept through more than 10,000 organizations in more than 150 countries around the world, causing heavy losses in many important industries such as energy, communications, and equipment manufacturing. The "Petrwarp" ransomware virus, which has been severely affected governments, nuclear facilities, banks, power systems, communications systems, enterprises and airports, once again sounded the alarm for the network security of the National Industrial Control System (hereinafter referred to as "ICS"). The grim situation of industrial control network security urgently requires us to have the ability to fight tough battles in the field of industrial control network security.

2. Current status of safety protection technology

In order to deal with the static and unchanged characteristics of the traditional network security defense system, dynamic defense technology is regarded as the most promising research direction by
academia and industry, and domestic and foreign scientific research teams and technical teams have launched relevant technical research and innovative work.

The US federal government-led network security automatic detection project "Einstein" plan, the MTD (Mobile Target Defense System) proposed by the US National Technical Committee, Academician Wu Jiangxing, academician of the Chinese Academy of Engineering, proposed cyberspace mimic defense theory, and researcher of the Beijing Information System Research Institute Yang Lin's proposed dynamic empowerment cyberspace defense system, VEDA intranet protection system and Fil dynamic defense system. Mobile target defense (MTD) is today's most influential security innovation opportunity. In the past few years, international research on mobile target defense has always attached great importance. The US Department of Homeland Security defines MTD technology as a new cybersecurity technology that changes the rules of the game. The US Air Force is preparing to use MTD technology to solve security problems by 2020. International academic discussions on MTD are also in full swing.

The "intelligent dynamic defense" technology independently developed by VEDA combines the tactical essence of Sun Tzu's art of warfare and the advancement of artificial intelligence technology. It is a "killer" technology in the field of network defense and has subversive significance in the industry. At present, VEDA has developed a series of intelligent dynamic defense products and solutions based on this technology, forming a comprehensive dynamic defense system for areas such as border security, intranet security, cloud security, big data security, application security, industrial control security, etc. As of now, the CTF Player Challenge held by VEDA has recruited technical elites worldwide to attack the "illusion-intranet dynamic defense system". However, no one has broken it so far.

3. Security threat analysis of industrial control enterprises

The industrial control system is mainly composed of Siemens, Honeywell, Rockwell, Yokogawa and other SCADA systems [1]. The main industrial control network security threats facing are:

(1) Malicious attacks by hackers and implantation of malicious programs. Some lawbreakers attack by remotely modifying production control strategies and measurement and control parameters; they may also maliciously implant dangerous programs in the SCADA system, causing accidents in process equipment and even loss of production suspension.

(2) General Windows operating system, compilation system, IEC61131 design software and other security vulnerabilities.

(3) Industrial control network WinCC server, TAS server, queuing host, access control host and other industrial hosts, application servers and host computers and other anti-virus and malware management and control vulnerabilities.

(4) Violation of the use of external devices such as U disks and CD-ROMs causes viruses to invade the SCADA system through the network, USB port or service provider's remote operation and maintenance service process.

(5) When the third-party maintenance of the control equipment is carried out, there is a situation of random access to the mobile equipment, or there is no safety protection measures and records when the VPN is accessed by remote operation and maintenance.

(6) At the same time of information construction, the boundary between the production network and other networks is becoming increasingly blurred and the protection is insufficient.

4. Overall design and implementation

4.1. Design Principles

(1) Standardization principle

The security planning, security construction, security rectification and construction of industrial network system security products must comply with information security laws, regulations and relevant industry standards.
(2) Overall layout principle
Adopt the principle of overall optimization, optimize the industrial control network security protection system, rationally arrange security protection capabilities, and reduce waste of enterprise resources.

(3) Top-level planning principle
Adopt top-level planning and design of industrial control network security framework, establish a network security protection system that is compliant, autonomous and controllable, safe and stable, and suitable for industrial control enterprises.

(4) Scalability principle
Custom-developed products must allow users to add new security components and security functions according to actual conditions, and must ensure the ever-increasing needs of industrial network system security.

4.2. Overall design
According to the industrial Internet adaptive architecture security system, following the design principles of standardization, overall layout, and top-level planning, it adopts the defense-in-depth defense concepts of "vertical stratification, horizontal zoning", "boundary control, intra-domain monitoring and auditing, and overall centralized management and control" [2-8]. Aiming at the security protection requirements of different industrial network levels, regions, key equipment, etc., based on fraud prevention, through machine learning, big data analysis and other technologies, an industrial control network security integrated protection platform that runs through different layers, regions, and network boundaries is built. Monitor the security status of industrial control equipment and important business systems in an all-round way, find and report and handle blocking security risks in a timely manner, and ensure the security of mainframes, equipment security, network security and data security of industrial control enterprises. Eventually realize the proactive defense capabilities of industrial control enterprises. As shown in Figure 1.

**Figure 1.** Overall design of industrial control network security comprehensive protection platform.

4.3. System functions
According to the overall design requirements, systematic security function design and guarantee are carried out from the aspects of defense in depth, active defense, situational awareness and linkage
defense. The industrial control network security integrated protection platform function is mainly as follows.

(1) Multi-factor collection and fusion
Real-time collection of fragile data including device and endpoint logs, traffic data, asset data, vulnerabilities and configuration, and multi-source and heterogeneous security element information such as intelligence, identity, business, and various context data, through big data technology carry out fusion, cross-fusion, data governance, dynamic modeling, and monitor the entire process of element information collection, transmission, storage, and utilization.

(2) Deepen safety analysis
Use FLINK's powerful distributed streaming association analysis and iterative calculation capabilities to realize the normalization and componentization of the analysis engine. Based on multiple types of industrial control knowledge bases, correlation analysis of events is carried out, which penetrates into the industry's industrial control network characteristics and generates scene alarms that integrate business characteristics. At the same time, it has general alarms for the entire industry attributes of the industrial network, such as alarms generated for operations such as asset addition, abnormal path, unknown protocol, unauthorized operation, and critical control. Integrate analysis functions such as intelligence analysis, risk analysis, vulnerability analysis, situation analysis, asset analysis, attack chain analysis, and user and entity behavior to form a deepened and three-dimensional analysis network, and comprehensively leverage the advantages of various analysis capabilities.

(3) Scene topology
The network environment and the operating status and security status of each device are displayed through the network topology or intuitive presentation, so as to achieve the purpose of centralized status and performance monitoring of various devices in the industrial control network. At present, the management and presentation of the comprehensive situation of the industrial control network is mainly achieved by customizing the chemical control topology. The industrial control network topology presented on the homepage can be customized according to the actual needs of the industry.

(4) Visual comprehensive situational awareness
Real-time monitoring, warning, reporting and handling of various security events, real-time tracking and research of vulnerabilities, virus events, real-time threat intelligence and risk notification, real-time presentation of industrial control system risks, one-stop security management, automatic security information reporting and other security situation analysis and asset visualization.

4.4. System implementation
According to the system design and function introduction, integrated development of a comprehensive safety protection platform, and use simulation test to ensure the correctness, integrity, safety and quality of system identification software. As shown in table 1.

| Item                                | Demand                                      |
|-------------------------------------|---------------------------------------------|
| Database system                     | Oracle8.1.7                                  |
|                                     | SQL Server2008                              |
|                                     | Windows2000                                 |
| Network operating system            | Linux                                       |
| Development Tools and Environment   | Visual Studio.net                           |
|                                     | SQL Server2008                              |
|                                     | Rose2000                                    |
| System Analysis and Design Tool     | JBuider8.1                                  |
|                                     | Visual Studio.net                           |
| System Development Platform         | OPEN Source Security Information System (OSSIM5.2.0) |
| System Test Tool and Environment    | Spike                                       |
5. Application and effect
In 2019, a ship heavy industry group Co., Ltd. carried out actual offensive and defensive operations on its pipe fittings production workshop. The industrial control network security integrated protection platform for security operations can sense threat attacks in real time, and real-time track and track forensics and effective interception hidden and unknown types of attacks, and effectively blocked the directional attack against the actual production environment of the industrial control system, and achieved the purpose of intelligent and safe operation.

(1) Visual comprehensive situation
The visualization module includes visual attack chain status display, risk dashboard display, alarm event type distribution display, asset risk distribution display, latest security event list, etc. It supports a series of security situation awareness functions such as large security screen, security blocking statistical analysis, abnormal traffic perception, intrusion perception, virus perception, Internet behavior perception, public sentiment awareness, hacker portrait, attack interest point analysis, and attack traceability. Based on various security event logs, collect, store, and summarize comprehensive analysis of abnormal traffic monitoring function module logs such as DoS attacks, scanning intrusions, and DNS queries.

Figure 2. Visualize comprehensive situation diagram.

(2) Asset topology
View related information such as topology, type, and location distribution of surviving assets on the network.

Figure 3. Scene topology diagram.
In the process of safety protection construction of the pipe processing and production workshop, a set of the industrial control network security integrated protection platform for safe operation was established, and key technologies such as edge computing, AI big data security analysis, and multi-source heterogeneous aggregation were innovatively used to achieve Real-time perception and accurate research and judgment of threats of industrial control security risks.

6. Conclusion
The industrial control network security comprehensive protection platform designed for industrial control enterprises has been verified by practical application. The platform has good suitability, compliance and compliance for industrial control enterprise security protection, provide reference value for the construction of industrial control network security protection in the shipbuilding industry and other industries. It has important economic and social benefits.

Acknowledgments

References
[1] Majed Al-Asiri and El-Sayed M and El-Alfy, On Using Physical Based Intrusion Detection in SCADA Systems (Procedia Computer Science, Amsterdam, 2020), pp. 34-42.
[2] Tschroub Abdelghani, Implementation of Defense in Depth Strategy to Secure Industrial Control System in Critical Infrastructures (American Journal of Artificial Intelligence, UNITED STATES, 2020), Volume 3, Issue 2.
[3] Jiang Ning and Lin Hu and Yin Zhenyu and Huang Yan, Research on Information Security and Defense-in-depth Architecture of Industrial Control Network (Journal of Chinese Computer Systems, Shenyang, 2017), pp. 830-833.
[4] Rahman M. Tanjidur and Rahman M. Sazadur and Wang Huanyu and Tajik Shahin and Khalil Waleed and Farahmandi Farimah and Forte Domenic and Asadizanjani Navid and Tehranipoor Mark, Defense-in-depth: A recipe for logic locking to prevail (Integration, AMSTERDAM, 2020), pp. 39-57.
[5] Wei He, Tobacco industry industrial control security solution based on defense in depth (Application of Electronic Technique, Beijing, 2019), pp. 88-91.
[6] XianRong Gan, Design of Information Security of Industrial Control System Based on Defense in Depth (Industrial Control Computer, Nanjing, 2018), pp. 38-39.
[7] Peng Wu and Jun Zhu and YongLei Han, Research on Application of Industrial Control Network Security Technology in Discrete Manufacturing Enterprises (Information Technology and Network Security, Beijing, 2019), pp. 42-45.
[8] Hui Li, The significance of online safety monitoring and defense-in-depth system to the safety protection of industrial control (Scientific and Technological Innovation, Harbin, 2018), pp. 20-21.