Research on Information Security for the Solution for Controller of Coordinate Measuring Machine(CMM)

Yong Zhu[1,a], Ruwei Cui[1,b], Yingang Yang[2,c]

[1]Aviation Key Laboratory of Science and Technology on Precision Manufacturing, Beijing Precision Engineering Institute for Aircraft Industry, NanYuan East Road NO.5,FengTai District, BeiJing, China

[2]Beijing Institute of Information High Technology, Qinghe Xiaoying Road No.32 Haidian District, BeiJing, China

[a] email: rogerustb@163.com, [b] email: cuiruwei@126.com,[c] email: yangyingang@sina.com

Keywords: CMM; ICS Security; Information Security; Information Audit

Abstract. By means of analyzing the Controller of CMM and its information model in the net, this article obtains the flimsiness and requirement to defend attack of the system. This article researches the interface of communication and communication protocols in the application layer of the main Controller of CMM. Based on the research, the article gives the design of information security protection of the Controller of CMM, including the hardware and software program of the information security protection module. The design is based on the communication content to audit and warn, this can improve the information protection level of the Controller of CMM, and guarantee the safety of the information of the Controller of CMM.

Introduction

"Stuxnet" virus make the world realize that, with the development of industrialization and information technology, there are serious information security risks in industrial control system network. In the process of deep integration of industrialization and information technology, equipment interconnection is an inevitable trend. However, frequent information security incidents lead to the existence of industrial control information security concerns, when companies consider the formation of the network. There has been contradiction between the convenience of the Internet and information security.

Industrial control system can be divided into monitoring and data acquisition systems, distributed control systems, discrete manufacturing industrial control systems. Discrete manufacturing is the process of performing a series of steps on a single piece of equipment to create the final product by assembly. Discrete manufacturing industrial control system includes processing, testing and testing of three categories; the measurement system is a typical representative of the industrial control system is the most information security vulnerabilities in the industrial control system. Most of the coordinate measuring system is in the streaking state, almost no information security measures. The measurement data related to military research and production capacity information, information security requirements have led to digital design, manufacture, testing of closed-loop information system fault status, has seriously hampered the further development of military manufacturing capacity [1][2][3].

The following section includes four parts: Part 1 introduces the basic structure of CMM and information flow model, and analyzes the vulnerability of the system; Part 2 describes the existing industrial information security protection technology, and analysis of its applicability; Part 3 analyzes the communication interface form and the application layer communication protocol of a mainstream CMM numerical control system, and forms the demand analysis. On this basis, the design scheme of the information security protection module of the CMM numerical control system is given; Part 4 draws the conclusion.

Vulnerability Analysis of CMM

Measurement system configuration

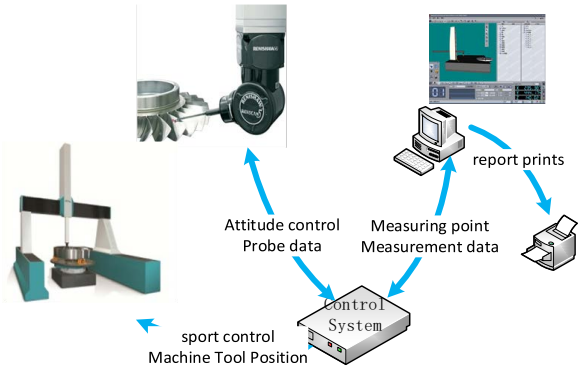

Fig.1 Typical measurement system structure

Fig.1 is a typical structure of the geometric measurement system, including mechanical body, control system, probe, a pre-installed Windows system used to run the measurement software computer, a printer used to print measurement reports. A typical measurement process is as follows: First, the operator uses measurement software to open the number of parts of the mold, to complete the man-machine interaction coordinate system establishment in 3D view, measurement path planning, interference checking, motion simulation ,the generation of measurement points issued To the control system; Next, according to the measurement point ,the control system complete the corresponding taking point movement process, receive the probe data, and send control system data to the measurement software; Finally, the operator uses measurement software to analyze the measurement data and give the measurement results. At the same time, the measurement process, the measurement software and the control system will produce their own log files which record some status information, communication information and measurement tasks.

Network Information Flow Model

Information flow model describes the flow of information from the OA network to the industrial control network, industrial control network in all aspects of circulation, the final flow back to the OA network process, as shown in Fig.2. According to the research situation, the information flow model of coordinate measuring system is drawn. Import and export of the information includes the production process cards, three-dimensional digital model, quality documents and numerical control procedures and other production operations documents, part definitions and design data, CAD drawing files, engineering analysis and validation data, manufacturing plans and specifications, NC programming Inspection and measurement information (gage number), test results information, quality reports, machine status and so on.

The information transmitted between the OA network and the CMM CNC system includes measurement codes, measurement data and measurement solutions. They are stored in * .dmi, * .xlsx, *. Sln formats, as shown in Fig.3.

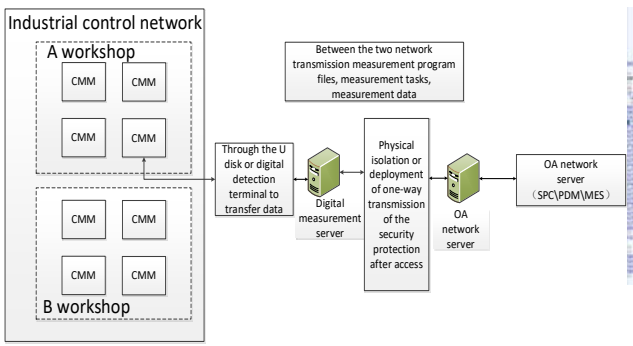

Fig.2 CMM numerical control system and its network information flow model

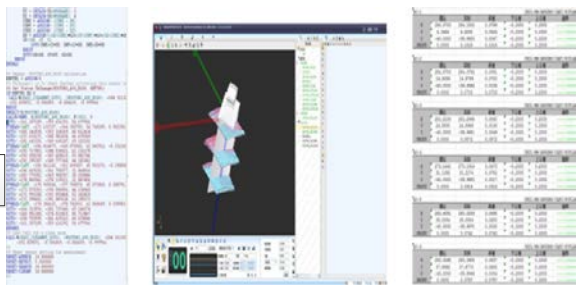

Fig.3 measurement data format

Vulnerability Analysis [4] [5]

Risks from the OA network

Industrial control network and OA network interconnection is the future trend. In the OA network to the industrial network to transfer measurement procedures and other information in the process, will use some of the standard communication protocol transmission, the attacker may be in the process of stealing and modifying files.

The information of the OA network can be indirectly flowed to the measuring machine through the digital detection server, which can steal the information of the OA network through the measurement system. Similarly, the virus in the OA network may spread to the measurement system and affect the safety of the measurement network.

Risks from industrial network

As the traditional information security products can not be compatible with the measuring machine CNC system, measuring machine CNC system can not patch, install antivirus software and other information security products. In addition, the NC system operating system and vendor software patch can not be updated and installed. In addition, there are threats in the measurement system that attackers can exploit printer vulnerabilities to attack measurement systems. Because there is a lack of proper password policy for the CNC system, the unauthorized access to the CNC system may result in unsafe and unnecessary open ports, which leads to the failure of the NC system.

The computer of the measuring machine system stores files such as digital model, measurement program, measurement result, and its CNC system and digital detection server need to be interconnected. The vulnerability of measurement system leads to these files being easily tampered or stolen. The general situation, industrial control systems and industrial equipment integration, installation, maintenance and so on are completed by professional firms. Foreign personnel can obtain program data, production logs, measurement results, etc., or attack measurement systems through USB disks, notebook computers, etc., and can also use the vulnerability of measurement systems to steal information in the OA network.

As the industrial control network is connected with the OA network, for some industrial network platform software, the attacker may use buffer overflow, DOS attacks to achieve a variety of attacks, to get some important information from the OA network. In the same way, the vulnerability of the measurement system itself allows an attacker to infiltrate the OA network with a measurement system or device. On the other hand, in the measurement of numerical control system may be installed wireless devices, as a springboard, an attacker can maliciously tamper with the machine measurement program information, steal logs, theft of OA network classified information.

Risk analysis of measurement control systems

China's precision geometric measurement market is almost monopolized by foreign manufacturers to the aviation enterprises, for example, a large number of OEMs to buy the Swedish HEXAGON's Global series, the German Zeiss Prismo series and Germany's Wenze white measuring machine, these companies control the control system , Software, all the core probe technology, firmly in control of the measurement data.

Domestic manufacturers only in the machinery manufacturing has its own technology, control systems and measurement software has been monopolized by foreign manufacturers. Domestic manufacturers work is almost Zanji, measurement software is basically purchasing the United States External-Array Software's Rational DMIS, the United Kingdom DELCAM's PowerINSPECT or British IMS's Virtual DMIS measurement software; control system or purchase British RENISHAW, or purchase Swiss PANTEC Of the control system; probe system is usually purchased RENISHAW probe or TESA probe. The measurement data are obtained by the data fusion of the probe data and the control system, and finally the measurement software is processed. The loss of control of the key technology of the domestic manufacturers leads to the more fragility of the measured data.

Overview of Industrial Control Information Security Technology

Canada's Tofino (Tofino) are designed for industrial networks, a dedicated firewall. The firewall consists of three main components: the " Tofino " Safety Equipment Module (TSA), the Dorneno Loadable Security Plug-in (LSM), and the Configuration Software-Central Management Platform (CMP). The Tofino Loadable Security Plug-in (LSM) is a technical core. Each LSM plug-in is downloadable to the Tofino safety device module, which enables it to provide configurable safety functions, depending on the requirements of the control system. Tofino central management platform (CMP) Centralized configuration, management and monitoring of all Tofino security device modules (TSA) and the network; built-in controller model, to the known controller vulnerability protection; built-in industrial communication protocol; real-time monitoring network alarm, Accurately locate the fault point.

Wurldtech of Canada has also provided solutions to prevent the industrial control system from sustained and dynamic network attacks. The proposed solutions include three parts: assessment, protection, verification. In addition, Canada's ICS Sandbox test platform uses penetration testing to simulate the vulnerability of critical infrastructure in SCADA systems by simulating real-world cyber-attacks. Codenomicon Defensics Industrial Robustness / Security Testing Platform, based on the robustness assessment and management scheme of active vulnerability exploiting, cooperates with ISA Secure and conforms to IEC 62443 standards.

In the field of data machine tools, Beijing Aerospace CNC System Co., Ltd. has developed China's first information security products for the protection of CNC machining: "HT706-CNCP CNC system terminal information security protection equipment" and "HT706-CISP border security gateway" [6].

After analyzing the status quo of research at home and abroad, we found that the domestic and foreign companies for the petroleum, chemical, municipal and other areas of industrial control system security solutions, discrete manufacturing can learn a lot of protection techniques and methods. As the specific situation facing each field is different, so the characteristics of the industry need to carry out extensive and in-depth study put forward more applicable solutions.

Information security protection module design

Requirement of Protection for NC System of CMM

Through a survey of the industry's mainstream brands of measuring machine CNC system, learned that the last 5 years of measuring machine CNC systems are used as a communication interface Ethernet port, the previous communication interface with RS232 and USB, USB as a debug interface due to the stability of the owe Good, so the use of USB interface, measuring machine CNC system is relatively small, quickly out of the market.

Communication protocol aspects for compatibility considerations, the Ethernet communication interface also uses the RS232-level application layer protocol. By capturing packet analysis, we can see that the agreement is broadly divided into three categories, the first category is manually operated instructions, the second type is sent from the CNC system to the computer coordinate position, the third category is sent to the computer control system computer control instructions. Through these analyzes, the form of hardware interface is determined and a list of application layer protocol keywords is established for the design of information security protection module of CNC system.

Protection module design

The whole system is divided into two parts: the information audit module and the client, the former is the core; the latter only provides a user interface.

As shown in Fig.4, the external communication interface of the industrial control panel will be controlled by the audit software module. The network interface, serial port and USB interface communicate with each other through the audit module. For the network interface 1, the serial port and USB communications are used from the physical layer bypass monitoring mode to ensure that the efficiency and stability of the industrial host; on the internal LAN and host interface between the

network 2 transparent agent to monitor the way, To ensure the control of internal communications and security.

Fig.4 CNC system information security protection module design of the overall program Fig.4 CNC system information security protection module design of the overall program.

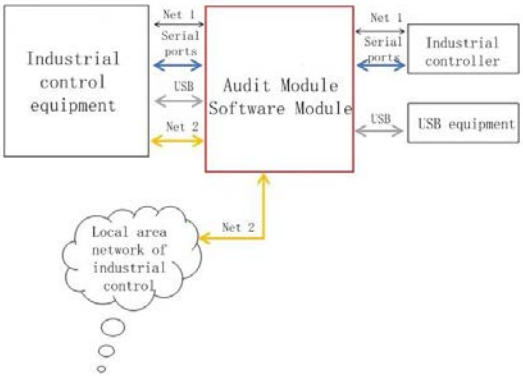

Fig.4 security protection module design

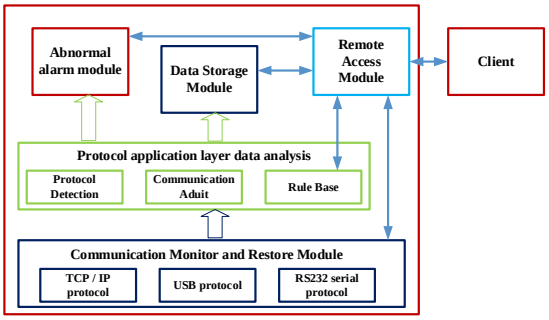

Fig.5 information audit module structure

In the monitor at the same time real-time communication protocol to restore, according to the type and content of the agreement to restore the audit, testing, as shown in Fig.5. In order to ensure the stability of industrial hosts in the network interface 1, serial port and USB communication is detected only when abnormal records and alarm; for network interface 2 disconnect the LAN and the host connection between to ensure the security of the host.

Communication Monitor and Restore Module

The module mainly from the physical layer of the TCP / IP network, USB interface and 232 serial port three types of communication bypass monitoring, while real-time transmission protocol storage and restore, and restore the application layer data submitted to the upper audit module . The module consists of the following three parts.

TCP / IP protocol:

This module mainly needs to monitor the communication between two network environments, namely the communication between the industrial controller and the industrial host and between the LAN and the industrial host. To ensure the efficiency and stability of industrial equipment, the network between the industrial controller and the host directly from the physical layer to monitor the bypass; for LAN network connections are transparent proxy approach to ensure the safety of industrial hosts.

USB protocol:

The module from the physical layer of the USB communication interception, with three USB ports, two of which are USB communication device connection side, the third for the data read side. USB communication does not affect the original case, the module through the data reader to monitor the USB communication.

RS232 serial protocol:

The module needs to monitor and restore the serial communication data. In order not to affect the efficiency of serial communication and function, the same bypass monitoring.

Protocol application layer data analysis

The module is called by the communication monitoring module, which mainly deals with the application layer data submitted by the monitoring module and analyzes and audits it according to the predefined rules according to the application layer protocol.

The analysis of the application protocol in the module is mainly based on the predefined rule base. The rule base is provided in the form of black / white list, and the secondary development interface is provided so that users can add their own rules according to the actual requirements.

After the data analysis is complete, the module stores the results in the data center for later analysis, and calls the exception alarm module for an alarm when the exception occurs.

Abnormal alarm module

This module mainly responds to and responds to an exception, and this module is called when

the application layer data abnormality detection result is abnormal. Response is based on the different sources of abnormal processing, such as local area network communication is the exception of the host and LAN to interrupt the connection, and provide secondary development interface to define the response to different anomalies the way.

Data Storage Module

Data storage module is mainly used for data access management, mainly used to store traffic data, the protocol content after the restore (including test results) and the log data.

Remote Access Module

The module mainly implements the access to the audit module and encapsulates the local secondary development interface into a remote access form. Encapsulation of the local secondary development interface, including authentication, real-time data acquisition, alarm information acquisition, rule base customization and monitoring control.

Conclusions

With the advancement of intelligent manufacturing, the interconnection of devices becomes an inevitable trend. The network of equipment lacking information security is extremely fragile, and it is urgent to carry out research on information security protection for various ICS. In this paper, the security risk of the measuring machine numerical control system is analyzed. Then, according to the security risk of the communication protocol of the measuring machine numerical control system and the requirement of the high availability of the industrial control system, the design of the information security protection scheme of the measuring machine numerical control system is given. The measuring system of NC is protected. The advantage of this external protection will not affect the original communication to ensure the high availability requirements; the disadvantage is not fundamentally improving the robustness of communication. China should further promote the standardization of related fields to improve the industrial control equipment, information security protection for intelligent manufacturing escort.

References

[1] ZHANG Yan. Research on the Information Security of Industrial Control Systems in China[J].Electronic Product Reliability And Environmental Testing,2012, 30(6):48-53.

[2] WANG X S, YANG A, SHI Z Q, et al. New Trend of Information Security in Industrial ControlSystems [J]. Netinfo Security, 2015(1):6-11

[3] PENG Yong,JIANG Changqiong, XIE Feng, et al. Industrial control system cybersecurity research. J TsinghuaUniv(Sci&Tech), 2012, 52(10):1396-1408.

[4] YU Li-ye, XUE Xiang-rong, ZHANG Yun-gui, et al. Solutions of industrial control systems security[J]. Metallurgical Industry Automation, 2013, 37(1):5-11.

[5] NIST SP800-82. Guide to Industrial Control Systems (ICS) Security[S]. Gaithersburg, USA:National Institute of Standards and Technology(NIST),2011.

[6] WANG Qi-kui, LI Xin, ZHAO Fu. Research on Information Security for Industrial Control System and the Solution for Numerical Control Network[J].Netinfo Security, 2014(1):120-122.