Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 13, no. 8, December 2017, pp. 1336-1346
DOI: 10.23940/ijpe.17.08.p15.13361346

Security Framework based on Trusted Computing for Industrial Control Systems of CNC Machines

Shanshan Tu[a,b,*], Guojie Liu[a,b], Qiangqiang Lin[a], Li Lin[a,b], Zedong Sun[c]

[a]*Faculty of Information Technology, Beijing University of Technology, 100124 Beijing, China*
[b]*Beijing Key Laboratory of Trusted Computing, 100124 Beijing, China*
[c]*Army Aviation Institute, 101123 Beijing, China*

Abstract

With the deepening of the integration of information technology and industrialization, industrial control systems of computerized numerical control (CNC) machines is gradually changed from the original isolated closed mode into the Internet model. It is not only facing the internal threat, but also facing the threat from the Internet. The existing industrial control system of CNC machine is due to long-term in a closed environment. The system cannot be updated in time; it is difficult to defend against the threat of industrial networks from the Internet. In view of the above problems, this paper firstly puts forward the security and trusted framework for CNC machine control system based on trusted computing technology, and elaborates the frame composition and function principle in detail. Then, the module of the trusted communication monitoring and control for the control system of CNC machine is presented; it can realize the scalability of the CNC machine system and the correlation of the equipment, while satisfying the trusted measurement function. Finally, this paper analyzes the reliability of the traditional CNC machines by means of experimental simulation. The performance shows that in the controllable range, the proposed framework can effectively enhance the CNC machine computing environment security.

Keywords: CNC Machine; industrial control systems; trusted computing; trusted measurement

(Submitted on September 29, 2017; Revised on November 12, 2017; Accepted on November 23, 2017)

1. Introduction

Due to the continuous progress of the integration of informatization and industrialization, the German government has proposed industry 4.0 in "German 2020 high-tech strategy"[10]. Global manufacturing enterprises are moving towards advanced manufacturing and intelligent manufacturing, and using industrial control systems as network entities to access the Internet. As an important part of intelligent manufacturing, computerized numerical control (CNC) machines are used widely in the manufacture of automobiles, locomotives, engines, aircraft, ships, and electronics and in many other fields [3]. The industrial control systems (ICSs) of CNC machines are the core of such machines, and are vulnerable to attacks; this is because these systems were initially closed, and not updated in a timely manner. For example, the "STUXNET" [4] virus that appeared in 2010 attacked the Iranian nuclear power plant system and caused serious damage; this was a warning that a great deal of attention needed to be paid to ICS security. Moreover, on December 23rd, 2015, the Ukrainian electric power network was attacked by BlackEnergy, which eventually led to system paralysis [5]. In other countries, their ICSs also face security problems.

Existing ICS solutions are basically based on measures such as firewalls, intrusion detection, and virus killing; however, it is difficult to deal with unknown system threats using these existing solutions. Wallace et al. [11] used the Metasploit framework, which is an intrusion detection technology, to observe attacks, and ascertained that active defense was impossible. Genge et al. [2] adopted a network traffic anomaly detection method for critical infrastructure based on a connection mode to detect intrusions, but discovered it was unable to discern unknown threats. Huang et al. [1] used a framework of policy-based integration into a role-based access control for mandatory access control. However, as there was

* Corresponding author.
E-mail address: sstu@bjut.edu.cn.

no trusted root, this method could not resist attacks from within the system. Yüksel et al. [12] suggested reading the neighborhood information, which was useful for finding an unknown industrial control virus and malicious instructions, but found that the false positive rate was higher, and the method had little actual application value. Yang et al. [13] detected and found potential intrusion behaviors for ICSs having taken account of misuse manipulation and command behaviors; however, whilst this provided a certain level of industrial safety protection, it could not fundamentally solve the problem. Zhang et al. [15] obtained data characteristics through the daily collection and analysis of the input and output data of industrial networks in order to establish a model, and then compared this model with the subsequent input and output to find whether the characteristics had changed. It was ascertained that certain threats could be detected using this approach, but it could not fulfill the role of active defense. Yi et al. [14] proposed an intrusion detection method based on the nonparametric cumulative sum (CUSUM), which improved the detection accuracy. However, this was also a passive detection method, which was unable to prevent malicious attacks effectively. In this study, a great deal of safety research on the ICS of CNC machines (CNC-ICS) was conducted, and its main contributions are as follows.

- The application scenarios and their special structures of various types of CNC-ICS are analyzed, and the security problems of CNC-ICSs are summarized. Having focused on these problems, a CNC machine security framework is proposed, which achieves an in-depth industrial network defense.
- Based on the trusted computing 3.0 technology [7], a trusted security framework of the CNC-ICS is proposed, which can automatically recognize “self instructions” and “non self instructions”, in order to guarantee that the CNC-ICS network is not interfered with.
- Based on this framework, a trusted communication monitoring and control scheme is proposed to monitor and control the CNC-ICS, and check the encryption of any instructions. When problems occur, the CNC machines can be controlled in real time, so that any losses are minimized.
- The scheme has been constructed following experiments, and can guarantee the communication reliability of CNC machines effectively without affecting the performance of the original CNC-ICS, thereby guaranteeing that the whole CNC-ICS is safe and reliable.

2. Security problem analysis

2.1. The CNC-ICS framework

Having analyzed and summarized the CNC-ICS, the framework of an ordinary CNC-ICS is shown in Fig. 1. A CNC-ICS framework is composed of a number of features, including an enterprise management computing environment, enterprise management network, production monitoring computing environment, production monitoring network, and CNC machine computing environment. Most of the enterprise management computing environment is an ERP system, which is responsible for all of the enterprise resource planning. The enterprise management network manages the communication network between the enterprise computing environment and the production monitoring environment, and delivers information such as that relating to tasks and feedback. The main function of the production monitoring and computing environment is to decompose the tasks according to those issued by the enterprise management computing environment, and distribute them to the CNC machine computing environment for execution. The security for the framework is now analyzed, and the existing potential security hazard will be outlined.

2.2. Security problem analysis

With an increasing number of CNC-ICSs connected to the Internet, a CNC-ICS is threatened not only by internal local networks, but also by the Internet itself. Having analyzed the framework composition of the CNC machines’ application scenarios, it was found that there are four aspects of risks to CNC machines, which are outlined below.

- The risk of operating systems. For example, a part of a CNC PCU uses Windows XP platform. When the system is online, users upgrade the operating system. Meanwhile, Microsoft has stopped its technical services for Windows XP, making it more vulnerable to attacks. Once the system is hacked, user data, HMI application data, the PLC processing code, and system log files in the system could all be stolen.
- The risk of application software. A large number of CNC machines use various application software, and it is difficult to form a unified defense standard. If an application port is opened, an ordinary IT firewall cannot guarantee its security. Once the security hole of the application software is obtained by hackers, any control of the equipment will be lost. For example, attackers in internal networks can easily, remotely and fully control CNC machines.

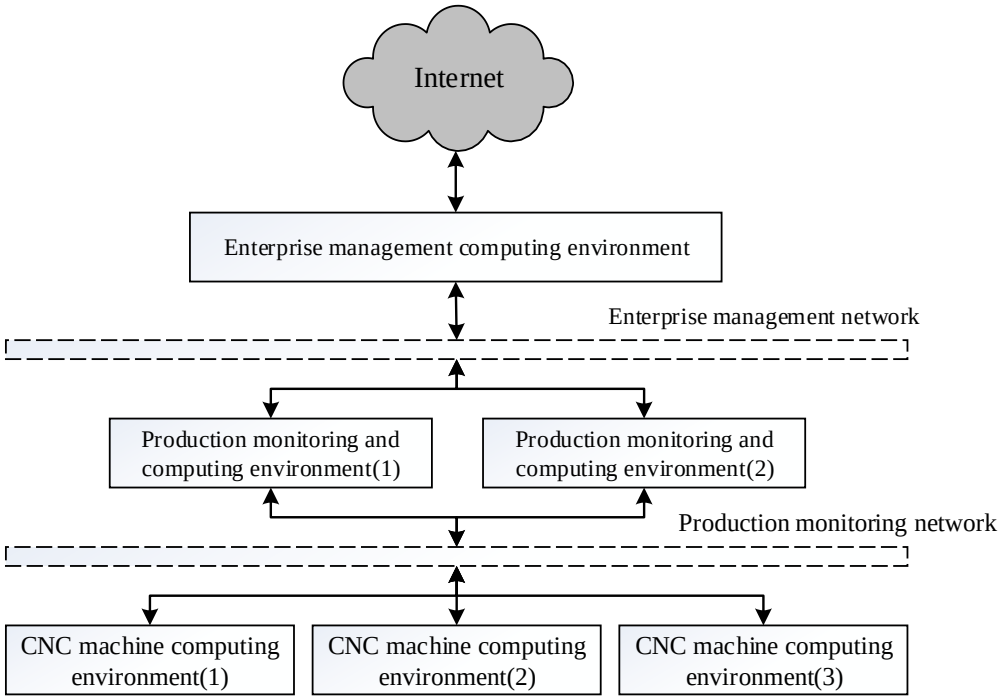

Figure 1. CNC Machine Tool Control System

- The risks of communication protocols. At present, the communication protocol of CNC machines is not uniform, and a private protocol or open protocol is adopted for communication. For example, the SIEMENS 840D uses SIEMENS MPI for communications, but its MPI protocol is not open. Its G code uses a TCP/IP protocol-based custom protocol for plaintext transmission, which is prone to being stolen.
- Security risks that exist in DNC networks. DNC servers use traditional databases installed on Windows systems, and FTP is widely used, making it possible to permeate the operations. The field processing equipment is connected to the management network MES system, and a series of protective measures, such as isolation between industrial control networks, malicious code monitoring, abnormal monitoring, and access control, are not carried out. Therefore, the system is vulnerable to a virus or other attacks, which will affect the whole workshop or company.

In this study, the literature is referred to in order to analyze current defense technologies for the above security threats to CNC machines. Current CNC-ICS defense technologies are based mainly on firewall technologies and intrusion detection technologies[6]. Firewall and intrusion detection can only defend known security holes, and are therefore ineffective for unknown, new security holes. Furthermore, current intrusion detection technologies only act after a system breach. In this paper, the main focus is an analysis of a CNC-ICS based on an active defense.

3. Introduction of trusted computing 3.0 technology

The main focus of the core technology of trusted computing 3.0 is to realize the trusted platform control module (TPCM), trusted software base (TSB) for active monitoring and trusted measurement of the system startup environment and operating environment by building a dual system architecture, thus realizing the system;s active defense, as shown in Fig. 2. The function of the TPCM is that of a trusted root, which takes an active measure of the hardware layer. The TSB undertakes the underlying hardware trust chain, actively monitors the system operating environment, and uses the cryptographic function provided by the TPCM to actively measure the system running environment. From the start of the system, the TPCM is used as the trusted root, and the active measurement verification is implemented step-by-step through the trust chain transfer mechanism. The credibility of the computing nodes and network environment is guaranteed due to the trusted network connection mechanism.

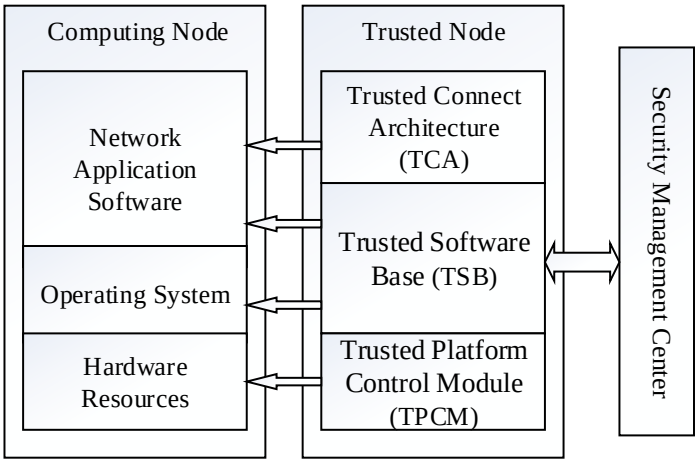

Figure 2. Double System Architecture of Trusted Computing Nodes

3.1. The TPCM

The structure of the TPCM is shown in Fig. 3[8, 16]. The TPCM is the physical trusted root of a trusted computing platform, which provides three trusted roots for the system and application, namely, a trusted measurement root, trusted storage root, and trusted report root. On the basis of the TPCM, the trusted measurement function, trusted report function and trusted storage function of a trusted computing platform can be extended. The TPCM adopts a trust chain transfer model based on a multi-metric agent, and defines the extended metric proxy module (EMM) based on different strategies for different stages of a platform start-up[8]. From the start of the system, the TPCM starts before the CPU, constructs a trust chain using the TPCM as the root of the trust, and uses the metric proxy nodes' EMM to measure the trust of the main board, system boot, system kernel and application step-by-step, thereby realizing the transfer and extension of the trust.

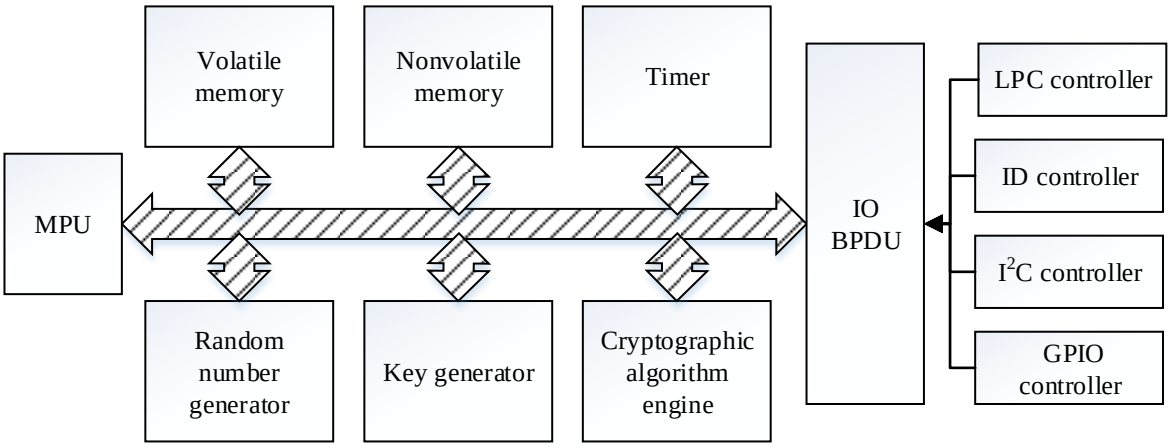

Figure 3. Structure of Control Module on Trusted Platform

3.2. TSB

The TSB forms a connecting link between the preceding and following stages in a trusted computing system, which protects the preceding stages, manages the TPCM and continues the transfer of the TPCM trust chain; moreover, it is the extension of the TPCM. The TSB parallels host base software by building a dual system architecture, and carries out active interception and measurement protection in the host base software under the support of the TPCM, thereby realizing the security function of an active immune defense, as shown in Fig. 4[9].

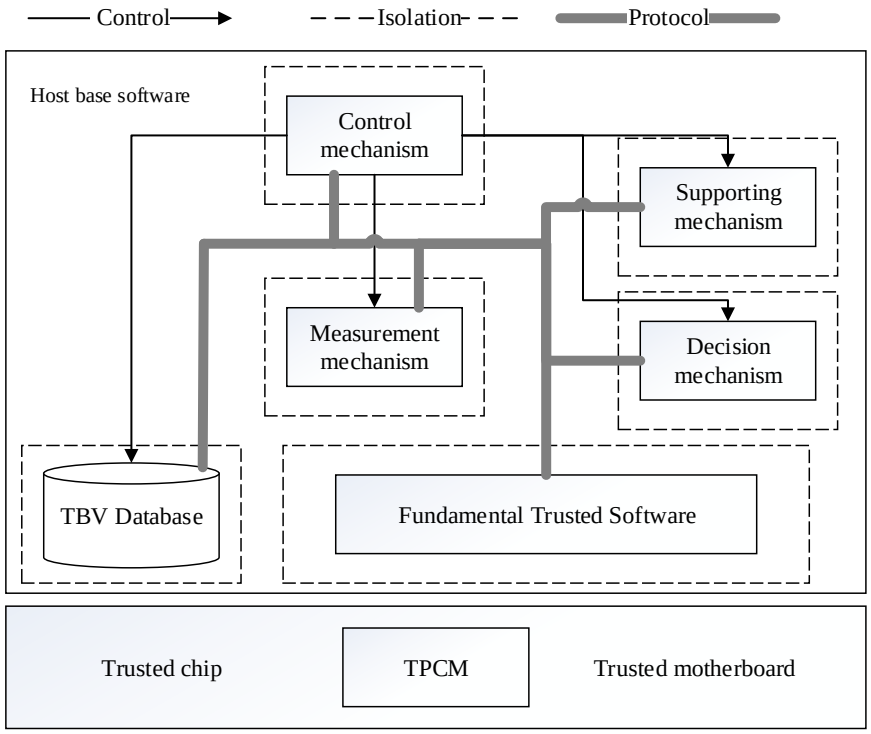

Figure 4. Function Framework of Trusted Software Base

3.3. The trusted connection architecture (TCA)

The TCA defines the trusted network connection between terminals with a TPCM and computer networks, and its essence is three layers of ternary equilibrium. The triplex control and discrimination are both realized among the access requester, access controller and strategy arbiter. Centralized control by servers improves the security and manageability of the architecture. The unified strategy management is implemented for the access requester and access controller to improve the overall credibility of the system, and overcome the insecurity of the traditional dualistic structure such as a collusion attack. The framework is shown in Fig. 5.

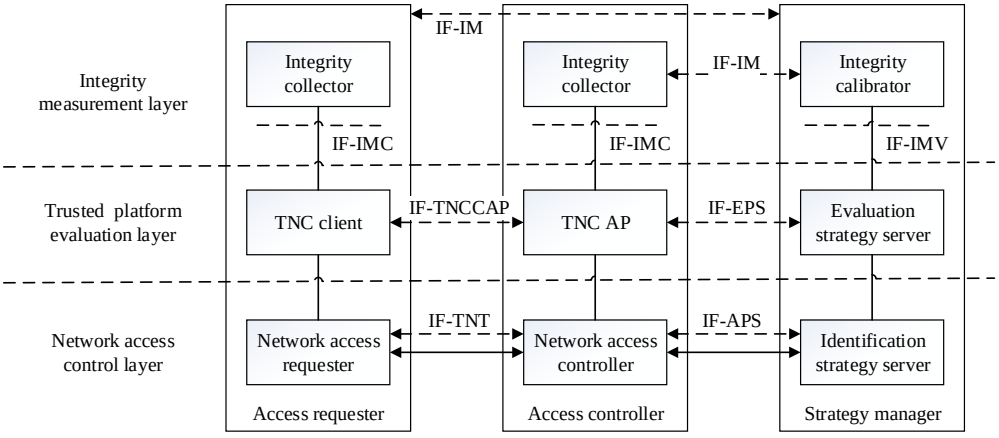

Figure 5. Architecture of Trusted Network

4. The security framework of a CNC-ICS based on the trusted computing 3.0

According to the characteristics of the CNC-ICS and the analysis of its security problems, a new security framework of a CNC-ICS based on trusted computing 3.0 is proposed. The functions of the framework are now described.

4.1. The security framework

In this study, having taken into account the special environment of a CNC-ICS, a security framework suitable for a CNC-ICS is designed based on the trusted computing 3.0 technology. It includes mainly a trusted security management center, trusted computing environment for CNC machines, field boundary protection, trusted computing for production monitoring, trusted computing environment for enterprise management, and boundary isolation, as shown in Fig. 6.

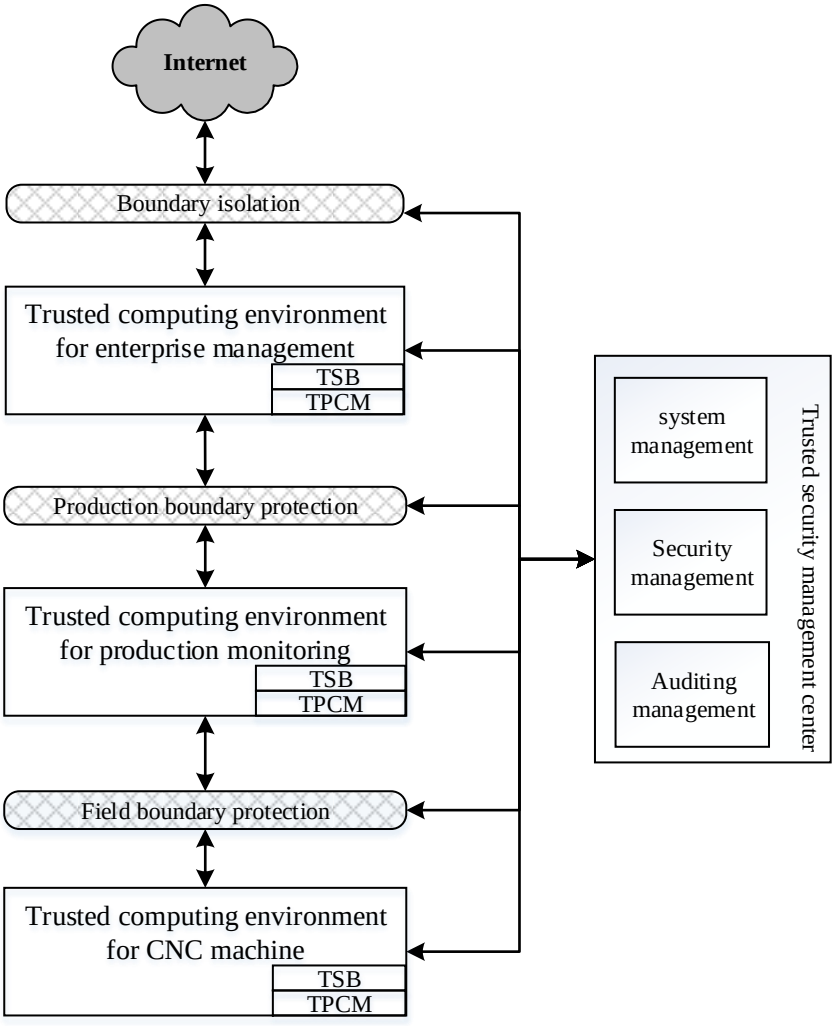

Figure 6. Control System of CNC Machine Tool Security Framework Based on Trusted Computing 3.0

4.2. The function description

4.2.1. The trusted security management center

The trusted security management center is the control core of the trusted computing environment, including the system management subsystem, security management subsystem and audit management subsystem. The system management subsystem is responsible for the centralized management and maintenance of three computing environments, three security boundaries and the safety communication network in a CNC-ICS. It also manages all kinds of user identity, various resources and emergency handling methods, amongst other things, thereby providing a basic guarantee for the safe operation of an information system. The safety management subsystem is the security control center of the information system. It mainly implements the key information marking management, the security authorization management and the security policy management. Through the establishment of corresponding security strategies, according to the security policy, it controls the access of three classes of a trusted computing environment, three classes of boundary protection and a communication network system, in order to realize the centralized management of the whole CNC-ICS. Thereby, it provides a strong guarantee for the safety of a CNC-ICS. The audit management subsystem is the supervision and audit center of the

system. By formulating corresponding audit strategies, auditors enforce the execution of the strategies of the security management subsystem, system management subsystem, three kinds of regional boundary subsystem, and communication network subsystem. This is carried out in order to realize the audit of the behavior record of the whole CNC-ICS, ensure that the calculation node cannot deny the behavior of violating the corresponding security policy, and provide the basis for the emergency treatment.

4.2.2. The trusted computing environment for CNC machines

There are many CNC machine manufacturers and various CNC-ICS operating systems; therefore, it is difficult to design a unified security system. Thus, according to the characteristics of the CNC-ICS and its actual operation, a trusted computing environment for CNC machines is designed in this study, and the concept of a trusted communication monitoring controller is proposed, which is also the unique character of the trusted computing environment for a CNC-ICS.

The trusted communication monitoring and control module is installed directly on a CNC machine, and connected directly with the control network interface of the ICS, without any other devices between them, in order to ensure the confidentiality and reliability of any communication. Moreover, active protection instructions can be issued when the system is attacked. The main functions of the trusted communication monitor controller are as follows. First, to perform an integrity measurement of the CNC machine system to prevent tampering. Second, to implement the corresponding safety control according to the safety control strategy. Third, to receive the instructions' task scheduling and other encrypted data of the production monitoring system, and send the CNC machine the decrypted data. Finally, to encrypt the log information generated by the CNC machine, and send it to the production monitoring environment and audit subsystem. In this way, the safety, credibility and safety control communication of a CNC-ICS are guaranteed.

4.2.3. The field boundary protection

The main function of the field boundary protection of a CNC-ICS is the security monitoring and control of the trusted computing environment and production monitoring environment data of a CNC-ICS, according to the data security strategies of the trusted security management center, in order to prevent the inflow and outflow of illegal data.

4.2.4. The trusted computing environment for production monitoring

The main function of the trusted computing environment for production monitoring of a CNC-ICS is to receive the production tasks of the enterprise management subsystem, and report the completion of the production tasks to the enterprise management subsystem. The trusted computing environment for production monitoring will measure the integrity of the system when it is started, and prevent a malicious program from running in the system. The data of the industrial control system of the CNC machine are received, decrypted and analyzed in real time.

4.2.5. The production boundary protection

The main function of the production boundary protection of a CNC-ICS is the security detection and control of the production monitoring environment and data of the enterprise management computing environment, according to the security strategies of the trusted security management center, in order to prevent data leakage and the running of malicious software, and prevent the inflow and outflow of illegal data.

4.2.6. The trusted computing environment for enterprise management

The trusted computing environment for the enterprise management of a CNC-ICS is the same as the traditional trusted computing environment. Its main functions include the management of the enterprise production process and production tasks; interacting with the Internet, and upgrading the system update. The trusted computing environment for the enterprise management will measure the integrity of the system when it is started, and prevent a malicious program from running in the system. It also interacts with the trusted computing environment of security monitoring, and can use the network's white list strategy to prevent illegal access and malicious attacks

4.2.7. The boundary isolation

The main function of the industrial boundary isolation system of a CNC machine tool is based on the security policy of the safety monitoring of communication data, and through data encryption and other measures achieves the protection of confidentiality and data integrity, and prevents leakages and illegal external or internal data streaming into other data.

5. The trusted communication monitoring and control framework for CNC-ICS

5.1. The trusted communication monitoring and control framework for CNC-ICS

Through a statistical analysis of the current ten prevalent CNC-ICSs, the CNC-ICSs are categorized into two classes: dedicated systems and general purpose systems. The communication interfaces of a CNC-ICS including RS232, Profibus,field bus, and Ethernet are listed in Table 1.

Table 1. Top Ten Popular Industrial Control Systems

System name	Communication interface	Classification
FANUC CNC system	RS232	Dedicated system
SIEMENS CNC system	Profibus	Dedicated system
MITSUBISHI CNC system	Profibus	Dedicated system
HEIDENHAIN CNC system	Ethernet	Dedicated system
REXROTH CNC system	Profibus	Dedicated system
NUM CNC system	RS232	Dedicated system
FAGOR CNC system	Ethernet	PC Converged system
MAZAK CNC system	Ethernet	PC Converged system
HuaZhong CNC system	NCUC bus	Dedicated system
GSK CNC system	Field bus	Dedicated system

As the operating systems of CNC-ICSs are different, and many of them are dedicated systems with non-uniform communication interfaces, it is very difficult to install a TPCM and TSB for trusted computing transformation. Therefore, the following trusted monitoring communication scheme for CNC machine is proposed, as shown in Fig. 7. The scheme consists mainly of two parts: the CNC machine computing environment, and trusted communication monitoring and control module. The latter of the two parts is the trusted monitoring function communication control module customized according to the working environment of CNC machines.

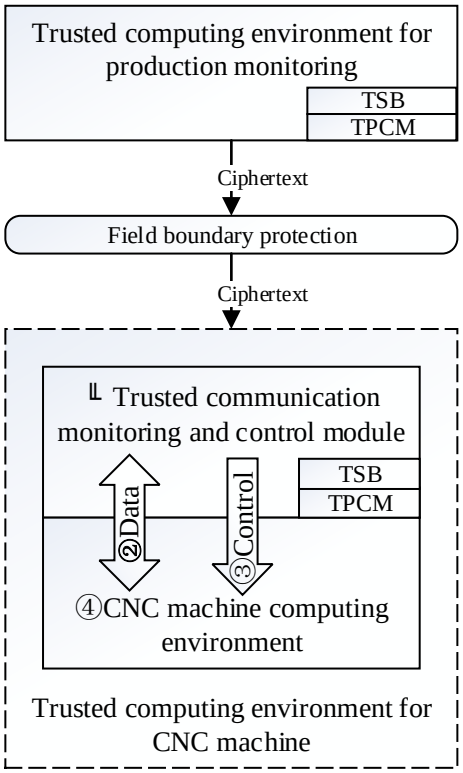

Figure 7. Framework for Trusted Monitoring Communication Scheme for CNC Machine

5.2. The function description

5.2.1. The trusted communication monitoring and control module

In Fig. 7 ①, the trusted communication monitoring and control module is embedded in the TPCM trusted platform control module. Moreover, the TSB that is installed in the embedded system ensures the trustworthiness of the trusted communication monitoring and control module. The trusted communication monitoring and control module is responsible for the following. First, decrypt the data of the trusted environment for production monitoring, then convert the data into plaintexts and send them to the CNC machine computing environment. Second, audit and encrypt the data of the CNC machine computing environment, and then forward the data to the trusted environment of production monitoring. Third, monitor the operation of a CNC machine, and take certain protective measures when errors occur in the running process of a CNC machine, such as sending standby, hibernate, shut-down, and restart instructions.

According to the control strategy, the trusted communication monitoring and control module can implement the white list mechanism of CNC-ICS instruction system in order to prevent the execution of malicious instructions. The security checks of the response data and logs of CNC-ICS prevent hidden malicious information from being transmitted to the trusted computing environment for production monitoring, and effectively prevent the CNC-ICS from attacking the entire ICS.

5.2.2. Data transmission

In Fig. 7 ②, the data transmission includes two parts. One part contains the data transmitted from the trusted communication monitoring control module to the CNC machine computing environment, and the other part contains the log data and error information generated by the CNC machine computing environment and transmitted to the trusted communication monitoring and control module. Since the CNC machine manufacturers' specifications and models are inconsistent, the trusted communication monitoring and control module needs to be compatible with RS232, ProfiBus and other CNC machine data interfaces, and enables the appropriate interface as needed.

5.2.3. The control command

In Fig. 7 ③, the control command mainly refers to the active control over the computing environment of the CNC machine by the trusted communication monitoring and control module. When a threat is detected, different control signals such as standby, sleep, shut-down, and restart instructions, can be sent out according to the different threats, and the CNC machine can be controlled in different ways.

5.2.4. The CNC machine computing environment

In Fig. 7 ④, the CNC machine computing environment is the object of monitoring and protection, i.e., all of a CNC-ICS. After installing the trusted communication monitoring and control module, the CNC machine computing environment cannot directly communicate with the trusted computing environment of production monitoring. Therefore, the trusted communication monitoring and control module must be used to access the whole industrial control network to ensure that the industrial control network is not subject to malicious attacks while protecting itself from such attacks.

6. Security and performance analysis

6.1. Security analysis

Since the framework adopts the trusted computing 3.0 technology, the general trusted computing nodes have a high level of security. The security of the trusted communication monitoring and control framework of a CNC-ICS is now analyzed.

Start with the trusted measurement. The trusted communication monitoring and control module starts before the CNC machine, and measures the CNC machine's system files. If the measurement result is inconsistent with the reference value stored in the trusted communication monitoring control module, the startup is terminated, and error alarm information is sent to the trusted computing environment for production monitoring to prevent the tampering from malicious programs.

Prevent the running of a tampered program on a CNC machine. Before the update of a CNC machine program by the trusted computing environment production monitoring, the signature of the CNC machine is updated, and then a trusted

computing environment is sent to the CNC machine. After the trusted communication monitoring and control module receives the updated instructions of the CNC machine's production procedures, it verifies the security of the update packages, and whether the digital signature information is correct. If incorrect, it prevents the execution, and sends an alarm command to the trusted computing environment for production monitoring, in order to prevent malicious instructions from running.

The trusted link for CNC machine communication. When the trusted computing environment of a CNC machine is connected to an ICS, the CNC machine's system environment is measured by the trusted communication monitoring and control module. If it is inconsistent with the reference value, the module prevents the CNC machine from connecting to the ICS.

Prevent the potential threat of a CNC-ICS. When the CNC machine sends data to the trusted computing environment of production monitoring, it must pass the trusted communication monitoring and control module. The trusted communication control and monitoring module performs a security review for data. If the data do not conform to the specification, they are blocked, and the data and alarm signal are sent to the trusted computing environment for production monitoring. If the trusted computing environment for production monitoring receives the alarm data, it will analyze the data in real time and determine whether there are malicious codes operating in order to ensure the safety of the ICS and prevent attacks.

6.2. Performance analysis

After setting up the security framework of a CNC-ICS based on the trusted computing 3.0, there are mainly the following two influential aspects on the original system. The first is the effect of adding the TPCM and TSB on the system, with the exception of the CNC's computing nodes, for trust measurement purposes. The second is the effect of adding the trusted communication monitoring and control module on CNC machine's program update and streamlined production.

In this study, the updated process and cycle of CNC machine program are analyzed and shown in Fig. 8. After adding the trusted communication monitoring and control module, due to the data encryption and integrity measurement, there will be some kind of impact. However, taking into consideration the update cycle of CNC machines, the impact is negligible. Generally speaking, CNC-ICS will write a control program according to business requirements, update data machine tools, and then start a long-term streamlined production, until the current task is completed, and new business requirements are received. This process is repeated and lasts weeks, months, or even years. The time of a program update for CNC machines (normally several seconds) is negligible for this period. After the CNC machine program is updated, it operates independently without being affected.

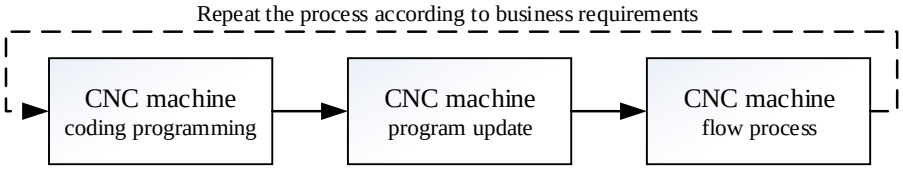

Figure 8. Updated Process and Cycle of CNC Machine Program

7. **Conclusions**

This paper analyzed the security problem of a CNC-ICS and existing ICS security protection technology. A CNC-ICS security framework was proposed based on the trusted computing 3.0, and the framework was described in detail. Specifically, the trusted component, "trusted communication monitoring and control module", was designed in an innovative manner. Without changing the existing CNC-ICS, the minimized resources were used to realize the trusted computing environment of all kinds of CNC-ICSs, thereby solving the problem that the special characteristics of a CNC-ICS are difficult to reform, and effectively protecting the safe operation of a CNC-ICS without interference. Meanwhile, the attacks to the entire ICS by a CNC-ICS were also effectively prevented. Finally, the experiments demonstrated that the proposed security framework for a CNC-ICS has an acceptable impact on the original system, and can be deployed for implementation.

Acknowledgements

This work is supported in part by the Beijing Science and Technology Planning Project (Z171100004717001), National Natural Science Foundation of China (No. 61671030, 61502017, U1536115, U1536207), the Scientific Research Common Program of Beijing Municipal Commission of Education (KM201710005024).

References

1. J. Huang, D. Nicol, and R. Bobba,"A framework integrating attribute-based policies into role-based access control," *the 17th ACM symposium on Access Control Models and Technologies*, pp. 187-196, 2012
2. B. Genge, D. Rusu, and P. Haller, "A connection pattern-based approach to detect network traffic anomalies in critical infrastructures," *European Workshop on System Security*, pp. 1-6, 2014
3. M. Keinert, A. Lechler, and A. Verl, "Concept of a computerized numerical control kernel for execution on multi-core processors," *2016 IEEE 14th International Workshop on Advanced Motion Control (AMC)*, pp. 581-586, 2016
4. S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," *IEEE Industrial Electronics Society*, pp.4490-4494, 2011
5. N. Paxton, D. Jang, and S. Russell, "Utilizing Network Science and Honeynets for Software Induced Cyber Incident Analysis," *2015 48th Hawaii International Conference on System Sciences*, pp. 5244-5252, 2015
6. Y. Peng, C. Jiang, and F. Xie, "Industrial control system cybersecurity research," *J Tsinghua Univ (Sci & Technol)*, no. 10, pp.1396-1408, 2012
7. C. Shen, D. Zhang, and J. Liu, "The Strategy of TC 3.0: A Revolutionary Evolution in Trusted Computing," *Engineering Sciences*, vol. 18, no. 6,pp. 53-57, 2016
8. C. Shen, and X. Chen, "Construction of the Information Security Infrastructure Based on Trusted Computing," *Journal of Sichuan University (Engineering Science Edition)*, vol. 46, no. 1, pp .1-7, 2014
9. Y. Sun, and Y. Wang, Y. Hong, "Research and application of trusted software base," *Journal of Information Security Research*, vol. 3,no. 4,pp. 316-322, 2017
10. M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17-27, 2017
11. N. Wallace, and T. Atkison, "Observing industrial control system attacks launched via metasploit framework," *ACM Southeast Conference*, no. 22, 2013
12. Ö. Yüksel, J. Hartog, and S. Etalle, "Reading between the fields: practical, effective intrusion detection for industrial control systems," *ACM Symposium on Applied Computing*, pp. 2063-207, 2016
13. A. Yang, L. Sun,and X. Wang, "Intrusion detection technique for industrial control systems," *Journal of Computer Research and Development*, vol. 53,no. 9,pp. 2039-2054, 2016
14. S. Yi, C. Zhang, and F. Xie, "Security analysis of industrial control network protocols based on Peach," *J Tsinghua Univ (Sci & Technol)*,no. 1,pp. 50-54, 2017
15. Y. Zhang, H. Zhao, and L. Wang, "A non-parametric CUSUM intrusion detection method based on industrial control model," *Journal of Southeast University (Natural Science Edition)*, vol. 42, no. s1, pp. 55-59, 2012
16. X. Zhang, and C. Shen, "A novel design of trusted platform control module," *Geomatics and Information Science of Wuhan University*, vol. 33, no. 10, pp. 1011-1014, 2008

Shanshan Tu is an associate professor in Faculty of Information Technology, Beijing University of Technology, China. He worked in the Department of Electronic Engineering at Tsinghua University as a postdoctoral researcher from 2014 to 2016. He received his PHD degree from Computer Science Department at Beijing University of Post and Telecommunication in 2014. He visited University of Essex as joint doctoral training from 2013 to 2014. His research interests are in the areas of cloud computing security and information hiding analysis technology.

Guojie Liu is a PHD student in Faculty of Information Technology, Beijing University of Technology, China. His current research interests fall within the general area of trusted computing technologies.

Qiangqiang Lin is a graduate student in Faculty of Information Technology, Beijing University of Technology, China. His current research interests are in the areas of mobile cloud computing security.

Li Lin is an associate professor in Faculty of Information Technology, Beijing University of Technology, China. Her research interests include cloud computing, multimedia network and next generation Internet.

Zedong Sun is a lecturer in Army Aviation Institute, China. His current research interests are in the areas of digital signal processing.