CHEMICAL ENGINEERING TRANSACTIONS
VOL. 66, 2018
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Songying Zhao, Yougang Sun, Ye Zhou

ISBN 978-88-95608-63-1; **ISSN** 2283-9216
DOI: 10.3303/CET1866152

Chemical Production Process Monitoring System Based on Embedded Trusted Computing Platform

Yuxiang Lin[a], Huiting Wang[b]

[a] Nanyang Institute of Technology, School of Software, Nanyang 473000, China
[b] Beijing University of Posts and Telecommunications, Institute Of Science and Technology Development, Beijing 100876, China
yuxianglin27361@126.com

The purpose of this study is to design the chemical production process monitoring system by using an embedded trusted computing platform. To this end, with reference to a large number of domestic and foreign literatures, various aspects of the trusted computing platform were analysed and understood, with particular emphasis on TPM. Then an embedded platform system was constructed. The results show that in the chemical production process monitoring system designed in this paper, the historical data can be consulted on the basis of related given reference conditions, and the monitoring points can be customized. Besides, this monitoring system can stop in time if it's tampered with the application program. Finally, it's concluded that the monitoring system of the chemical production process designed in this paper has a simple structure and can be well protected against external attacks, which can thus be better applied in practice.

1. Introduction

With the development of information technology and communication technology, the embedded system has been generated and developed. This has also given birth to the embedded trusted computing platform. The embedded trusted computing platform involves many disciplines, mainly including computer technology and microelectronics technology etc., and has been widely used in various fields in China. At present, the embedded trusted computing platform is gradually moving towards diversification and intensification. The production of chemical companies has certain risks. Therefore, most chemical companies have constructed chemical production process monitoring system. Through this system, the monitoring personnel can grasp the chemical production status of the company in real time, and timely detect the safety hazards. Also, it can play a certain role in regulating the operation process of the workshop staff so as to reduce the production safety accidents of chemical companies and improve the safety of chemical production. Now, the production technology of chemical companies is updated faster and the production process is becoming increasingly complex, thus, the conventional monitoring system of chemical production process cannot meet actual needs. To effectively solve the above problems, the embedded trusted computing platform was applied in this paper to analyse and understand all aspects of the trusted computing platform, and then an embedded platform system was constructed to design the chemical production process monitoring system. It's of great significance to apply the embedded trusted computing platform to the chemical production process monitoring system, which can effectively monitor the production and meet its actual needs of chemical companies.

2. Literature review

Compared with traditional industrial instrument control, DCS (Distributed Control System) is a modern intelligent computer automatic control system. It is a new generation of automation control system after the base regulator, pneumatic/electric unit combination meter, direct digital control system (DDC) and supervisory computer control system (SCC). DCS enhances the processing capability of information by centrally controlling multiple computers, and facilitates monitoring and management. Each computer controls the different regions to facilitate the decentralization of risk. With the advantages of powerful decentralized control, simple centralized management, solid reliability, fast configuration software, rich control algorithms, and open

Please cite this article as: Lin Y., Wang H., 2018, Chemical production process monitoring system based on embedded trusted computing platform, Chemical Engineering Transactions, 66, 907-912 DOI:10.3303/CET1866152

networking capabilities, DCS is playing an increasingly prominent role in the field of industrial automation control and gradually become the mainstream of application. The main application of DCS system and most markets are concentrated in petrochemical industry and other complex processes. In the petrochemical and other industries, the collection and monitoring of on-site signals such as pressure, flow, and temperature account for the absolute proportion. The predecessor of DCS, the direct digital control system, has mature monitoring technology. DCS is easy to meet the data acquisition and control functions of chemical field. In addition to analog quantities, digital or switching sequence control is also very important. In the process of chemical production, large equipment such as towers, slots, axes and cans can be run. At the same time, when these equipments are working, there is no need for monitoring the switch quantity of all electrical and mechanical equipment (such as pumps, fans, compressors, etc.) and valves. The advantage of DCS in digital control is that it can meet the functional requirements of chemical production. The simple analog digital quantity is not enough to complete the whole process flow, such as reactors and other equipment. Their working characteristics are intermittent. The equipment does not work continuously. After the first raw material is put into the reaction product, it has to undergo a period of intermittence and then put into the raw material for second times. In view of the working characteristics of this kind of production device, the petrochemical industry uses mass control methods to effectively solve it. According to the batch control form, the analog and digital phases are required to be combined for acquisition and control, so that the petrochemical industrial control system is now referred to as a hybrid control system. In fact, it is the DCS control system (Lukin and Rubin, 2015). In addition, the DCS control system also has features such as easy installation, safe and reliable performance, friendly man-machine interface, easy use and maintenance, and easy expansion and upgrade. It can better meet the requirements of industrial control (Dou, 2017).

In the late 20th century, with the development of large-scale integrated circuits, the degree of integration became higher and higher. It can integrate more electronic components and is more powerful. 8-bit microprocessors are commonly used. This technology makes a qualitative change in the industrial automation instrumentation industry (Stabile, 2017). Among them, Guney et al. developed an overall decentralized control system for microprocessors based on the combined microprocessor technology of a centralized computer control system, namely a microcomputer distributed system (Guney et al., 2017). On this basis, in 1975, Honeywell of the United States took the lead in publishing the TDC2000 overall decentralized control system (Solnechnyi, 2017). The system can complete the 8-loop control separately, and the basic controller of each loop can be set independently. The communication system is served by the data highway's bus as a network medium. Several basic controllers and CRT (Cathode Ray Tube) operating stations are connected together to ensure that each node has computer decentralized control and centralized display management at the operating platform (Zhang et al., 2017). At the same time, the United States, Japan, Britain, France, and Germany have also started to develop corresponding products. It is mainly used in systems based on analog control loops, including public utilities such as chemical, power, petroleum, and metallurgy. Such products are collectively referred to as DCS (Kubo et al., 2015). At present, the DCS control system plays an irreplaceable role in the field of industrial control. Although fieldbus technology has gradually emerged, the company has introduced its own bus technology because there is no unified standard so far. Openness and interoperability are difficult to unify. The cost is high and the technology is not mature enough. It does not win a wide market (Tao et al., 2017). In the future and even for a long period of time, the status of DCS in petrochemical and other special industrial controls is beyond any doubt. However, its functions are more perfect. The transparency of the new technology compatibility, the improvement of the application service level and the reduction of the price of the product market are also urgent.

In summary, the above research work mainly describes a large number of distributed control systems. DCS enhances the processing capability of information by centrally controlling multiple computers, and facilitates monitoring and management. Each computer controls the different regions to facilitate the decentralization of risk. With the advantages of super strong decentralized control, simple centralized management, solid reliability, fast configuration software, rich control algorithm, open network ability and so on, the role of DCS has become increasingly prominent in the field of industrial automation control, and gradually become the mainstream of application. Therefore, based on the above research status, the monitoring platform of embedded system platform is studied. New functions are developed. Market share is allocated and new technology is improved.

3. Methods

3.1 Architecture of embedded platform

SoCs, based on application-specific integrated circuits (ASICs), are lack flexibility, not reusable, and take huge development time and costs, so it’s only suitable for large-volume market fields that do not need to be upgraded in the future. Obviously, there is a need for more flexible solutions, and there emerges the

programmable chip system. The Xilinx Zynq all-programmable SoC-series device implements a high-performance, dual-core ARM Cortex-A9 processor subsystem (PS) and a rich memory, configuration, and interconnect interface. With flexibility retained and all the advantages of other traditional FPGAs in the FPGA logic, the FPGA is connected to the PS terminal through multiple high-performance interfaces, realizing high-bandwidth communications between ARM and FPGAs. In this design, FPGA+ARM combination of Xilinx's ZYNQ series was used. The essential feature of ZYNQ is that it combines a dual-core ARM Cotex-A9 processor and a traditional field programmable gate array logic. Although there have been dedicated processors bundled with FPGAs before, there has not been a completely identical solution. On ZYNQ, the ARM Cortex-A9 is an application-level processor that can run a complete operating system like Linux, and the programmable logic is based on the FPGA architectures of Xilinx7 family. This architecture implements the industry-standard AXI interface, enabling high-bandwidth, low-latency connections between the two parts of the chip. This means that both the processor and the logic portion can each be used optimally without the interface overhead between the two discrete chips. At the same time, the benefits of simplifying the system to a single chip can be obtained, including the reduction in physical size and overall cost. Each product in Zynq7000 embedded processor platform family uses a dual-core ARM Cortex-A9 MPCore processing system with NEON and a double-precision floating-point engine that is hard-wired to achieve the full integration of L1, L2 caches, memory, controllers, and common peripherals.

The hardware with security protection features was used to ensure certain physical protection capability of the platform. Besides, the trusted computing environment was built on this platform through a combination of hardware and software. Embedded system software is necessary for the embedded platform in operation. The software architecture of the embedded platform is mainly composed of the basic input/output system (BIOS), boot program, operating system, and application program, as shown in Figure 1.

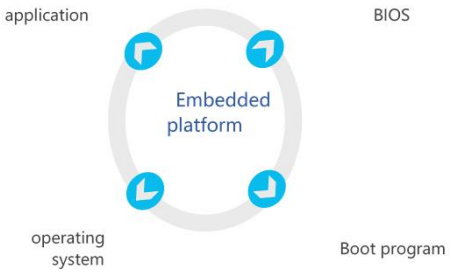

Figure 1: Embedded Platform Software Architecture

After the computer is powered on, it first starts with the BIOS. The BIOS is usually stored in the read-only memory ROM. The code will not disappear even if it is shut down or powered off. The BIOS code deals directly with the hardware. It provides the operating system with the basic functions of hardware control. The boot process of the computer is performed under the control of the BIOS. The BIOS detects the hardware, mainly including the CPU, memory, and plug and play devices. Then the boot program is started to boot the operating system, which firstly boots the kernel, and then make the system initialization, mainly to complete the reading of machine state data, the switch from real mode to protected mode, data segment register loading, and interruption of descriptor table setting etc. Finally, the operating system loads the application

3.2 The core function of TPM

After embedding the TPM in hardware of ordinary computing platform, one trusted computing platform with security and secrecy features can be constructed. The credibility of the trusted computing platform is ensured by the internal functions of the TPM. The core functions of the TPM include security metrics and reports, key management, remote certification, and data protection, as shown in Figure 2.

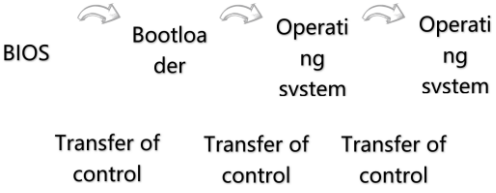

Figure 2: The establishment of the trust chain when the operating system starts

Based on the TPM structure, the key generation component is used to generate keys, including the symmetric key and asymmetric key. The random number generator serves as an important input parameter to the key generation unit. The TPM's cryptographic coprocessor is used to implement cryptographic operations, as well as symmetric cryptographic operations and asymmetric cryptographic operations.

4. Research results and discussions

In this paper, the open source U-Boot of 2013.07 version provided by one foreign company was used as the bootloader, and the 4.0.0-version Linux kernel was adopted, to mainly verify the TPM working status and make the U-Boot measurement. After the XC7Z015 chip was powered on, the TPM was activated but has not yet started. A TPM_Startup command was issued by the BIOS to reset the PCR register and start the TPM. Figure 3 shows the information of the TPM module loaded at system start-up, indicating that the TPM module was successfully started.

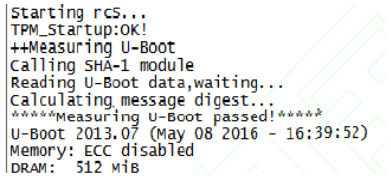

Figure 3: System Loading TPM Module

The TPM first called the SHA-1 module to measure the U-Boot integrity, and then performed integrity verification on the digest value. U-Boot could be started only if the verification passes. Similarly, U-Boot read the Kernel into RAM, and then called the SHA-1 module to measure the integrity of the Kernel. After the measurement was successfully made, the kernel was started.

To generate the DLL dynamic link library (DLL), VC++ should be used for data acquisition, because VB does not support the hardware operation. By compiling the data acquisition part into dynamic link library, the dynamic link library function was called in the VB application program to complete the access to the hardware port. The following example simply shows how to generate and call a DLL. One simple DLL project sample was generated in VC, to read the contents of port 300H, and add the content at the end of sample.cpp, as shown in Figure 4.

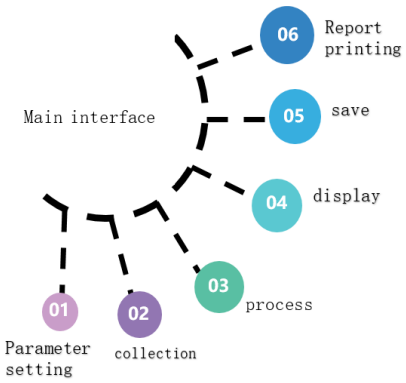

Figure 4: Chemical production monitoring system control interface

At the same time, DEF defined the exit of the function in the file, that is, to define the function that can be called by other applications. The module definition file was created by entering the following:

LIBRARY sample
DESCRIPTION“sample.dll0”
CODE PRELOADMOVEABLE DDSCARDABLE
DATA PRELOAD SINGLE
EXPORTS
ReadByte @1

Before describing the design of the codec module, it is necessary to specify the format of the TPM command, because the main function of the codec module is to parse out the specific TPM command requested by the application and encode the results executed by the software TPM back to the application program. Thus, the data communication becomes more secure. After describing the TPM command format, this chapter presents the TPM command design method, and also illustrates the coding and decoding design methods in the codec module.

TPM commands are divided into input command and output response. In terms of the structure, the TPM commands are divided into three parts: request/response header, request/response parameter, and authorization trailer. Authorization trailer is sub-divided into authorized trailer 1 and authorized trailer 2. It is mainly used to verify the legitimacy and validity of TPM commands. The TPM command structure is shown in Figure 5.

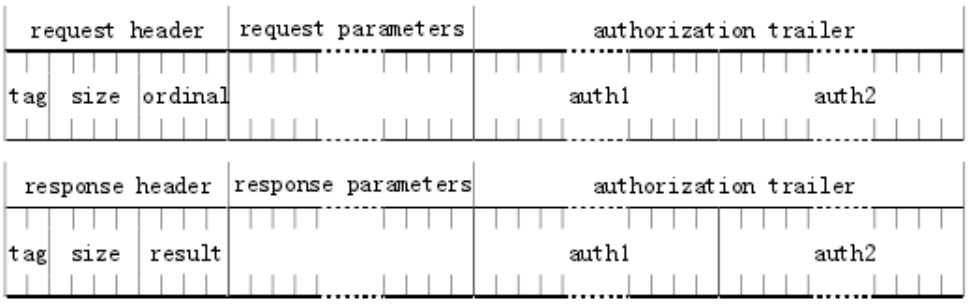

Figure 5: TPM command structure (the figure above shows the input command structure, the figure below shows the output response structure)

In the TCG specification, TPM commands generally include the request/response header and request/response parameters. The authorization trailer is optional. It varies according to the command. Some TPM commands have no authorization trailer, some have one, and others have two. All TPM commands have the same format of header, with the length fixed at 10 bytes.

If the TPM command fails to be executed, its execution failure information will also be returned to the command caller by the result field in the output response header. The caller can know the specific error information according to the TPM command execution status code in the result field.

According to the TCG specification, the number of bytes returned when the TPM command is successfully executed can be calculated, and the number of bytes returned when the execution fails is undefined. Therefore, when receiving the TPM return value, the caller first receives 10 bytes of the output response header and parses out the size field and the result field; if the result is TPM_SUCCESS, then the caller reads the remaining return words according to the size; if result is not TPM_SUCCESS, then simply discard (do not receive) the remaining bytes, or make the appropriate processing based on the specific result value.

In this way, when the TPM command is parsed, only the corresponding parameters need to be read; when the TPM returns data, only the corresponding parameters need to be filled.

In order to better verify the security of the trusted embedded platform based on TPM design, this paper simulates the kernel forgery attack test. For the integrity attack test of the kernel, an untrusted kernel similar to the secure legal kernel was forged. By illegally tampering the mandatory access control functions of the legitimate boot kernel, this kernel could achieve arbitrary destruction of the operating system kernel code and data integrity. The kernel forgery attack test results are shown in Table 2.

Table 1: Forgery Attack Test Results

	PCR value	Measurement time
Forgery before the attack	0x81, 0x34,	Sun Jan 15
	0xB5, 0x51,	09:13:17
	0x4E, 0xF4,	2017
After forging an attack	0x2A, 0x09,	Sun Jan 15
	0xC1, 0xB2,	09:30:09
	0x8C, 0x3F,	2017

The experimental results show that during the boot process of the XC7Z015 embedded platform, the Os kernel is found timely to have been tampered before the Bootloader transfers control to the Os kernel. That is, the Os kernel metric is different from the standard PCR value. Thus, it's judged that the integrity of the Os Kernel is destroyed and then the system automatically terminates.

5. Conclusion

With reference to a large number of domestic and foreign literatures, various aspects of the trusted computing platform were analysed and understood. Then an embedded platform system was constructed to design the monitoring system of chemical production process. The research results show that for the chemical production process monitoring system designed in this paper, the historical data can be consulted on the basis of related given reference conditions, and the monitoring points can be customized. Besides, this monitoring system can stop in time if the system is tampered with the application program. Finally, it can be seen form the results above that the monitoring system of the chemical production process designed in this paper has a simple structure and can be well protected against external attacks, which has a higher promotion and application value.

In this paper, one chemical production process monitoring system was successfully designed, but the layered structure of the system may result in too many instances, which is not conducive to its practical application in the chemical companies. It can be said that the design of the chemical production process monitoring system based on the embedded trusted computing platform should take the user application and development requirements as the design core, providing users with personalized and simplistic services, which is trend for the design of the future chemical production process monitoring system.

Reference

Dou J., 2017, Human-machine interface evaluation of cnc machine control panel through multidimensional experimental data synchronous testing analysis method, International Journal of Performability Engineering, 58(6), 153-157, DOI: 10.23940/ijpe.17.08.p3.11951205.

Guney O.F., Bozkurt A.F., Erkan K., 2017, Centralized gap clearance control for maglev based steel-plate conveyance system, Advances in Electrical & Computer Engineering, 17(3), 101-106, DOI: 10.4316/aece.2017.03013.

Kubo M., Taniguchi J., Kato M., 2015, Howling reduction by analog phase-locked loop and active noise control circuits, Applied Acoustics, 87, 174-182, DOI: 10.1016/j.apacoust.2014.07.004.

Lukin N.A., Rubin L.S., 2015, Use of nonlinear functional analog-to-digital conversion in precision measurements of small electrical quantities, Gyroscopy & Navigation, 6(2), 149-155, DOI: 10.1134/s2075108715020078.

Solnechnyi E.M., 2017, Conditions for stability and roughness of the distributed plant control system with a controller close to the degenerate system, Automation & Remote Control, 78(7), 1243-1250, DOI: 10.1134/s0005117917070062.

Stabile R., 2017, Towards large-scale fast reprogrammable soa-based photonic integrated switch circuits, Applied Sciences, 7(9), 920, DOI: 10.3390/app7090920.

Tao F., Cheng Y., Zhang L., Nee A.Y., 2017, Advanced manufacturing systems: socialization characteristics and trends, Journal of Intelligent Manufacturing, 28(5), 1079-1094, DOI: 10.1007/s10845-015-1042-8.

Zhang M., Ortega R., Liu Z., Su H., 2017, A new family of interconnection and damping assignment passivity-based controllers, International Journal of Robust & Nonlinear Control, 27(1), 50-65, DOI: 10.1002/rnc.3557.