RESEARCH ARTICLE | MAY 08 2017

Security analysis of cyber-physical system FREE

Bo Li; Lichen Zhang

AIP Conf. Proc. 1839, 020178 (2017)
https://doi.org/10.1063/1.4982543

Security Analysis of Cyber-Physical System

Bo Li [a)], Lichen Zhang

School of Computer, Guangdong University of Technology, Guangdong 510006, China

[a)] Corresponding author: 460374381@qq.com

Abstract. In recent years, Cyber-Physical System (CPS) has become an important research direction of academic circles and scientific and technological circles at home and abroad, is considered to be following the third wave of world information technology after the computer, the Internet. PS is a multi-dimensional, heterogeneous, deep integration of open systems, Involving the computer, communication, control and other disciplines of knowledge. As the various disciplines in the research theory and methods are significantly different, so the application of CPS has brought great challenges. This paper introduces the definition and characteristics of CPS, analyzes the current situation of CPS, analyzes the security threats faced by CPS, and gives the security solution for security threats. It also discusses CPS-specific security technology, to promote the healthy development of CPS in information security.

Key words: Cyber-Physical System; security threat

INTRODUCTION

The 21st century is the era of rapid development of information technology industry, such as mushrooming technology breakthroughs and innovation, and the environment and the way of human life has undergone enormous changes, especially in the embedded computing device as the main body of the information system in all aspects of social life applications. Traditional embedded devices are often one-step molding, is closed to the outside world, far from being able to meet the current physical equipment to be controlled, interactive, communication, scalability and many other application needs. Therefore, on the basis of environmental perception, the Cyber-Physical System (CPS), which integrates the interconnection and deep integration of people, machine and material, has not only become an important research and development direction at home and abroad, will also be a priority area for the development of enterprises priority investment. At the same time, it is of great significance to accelerate the integration of industrialization and informationization in China.

This paper analyses the security threats faced by CPS from the security requirements of CPS, and gives the security solutions. The key technologies are researched to promote the healthy development of CPS in information security.

CPS Definition

CPS is the next generation of intelligent systems that combine the integration of computing resources with physical resources by combining the organic and deep integration of communication, control and control technologies.

At the micro level, CPS integrates computational processes and physical processes by embedding computing and communication kernels in physical systems. The calculation process interacts with the physical process through the feedback loops [1], which realizes the reliable, real-time and efficient monitoring, coordination and control of the physical process of the embedded computer and the network.

At the macro level, CPS is a dynamic hybrid system consisting of distributed, asynchronous heterogeneous systems running in different time and space ranges, including various types of resources and programmable components such as sensing, decision making and control. Each network through the wired or wireless communication technology,

Materials Science, Energy Technology, and Power Engineering I
AIP Conf. Proc. 1839, 020178-1–020178-6; doi: 10.1063/1.4982543
Published by AIP Publishing. 978-0-7354-1509-6/$30.00

relying on the network infrastructure to coordinate with each other to achieve real-time perception of physical and engineering systems, remote coordination, precision and dynamic control and information services.

CPS Features

CPS is called "human-machine-material" fusion system, its essence is to achieve human time and space in the extension of control.

1) Compared with the embedded system, CPS as a physical device and computing technology integration, making the calculation of the object from digital to analog, from discrete to continuous, from static to dynamic, from distribution to unity of the transition, PS as a fusion of physical equipment and computing technology, making the calculation of the object from digital to analog, from discrete to continuous, from static to dynamic, from distribution to unity of the transition, the same network, control and embedded system dynamic reorganization and integration.

2) Compared with the Internet of Things, CPS in the physical entity after the realization of the perception on the basis of more attention to the physical equipment for real-time, dynamic information control and information services.

3) Compared with the software system, CPS focuses on the real-time control and feedback of each physical process, emphasizing the dynamic response of information processing and interaction.

Research Status at Home and Abroad

Foreign research and development on the physical integration of information system began earlier, first of all, the United States in 2006, and as one of the important research projects. After a lapse of one year, the US President's Science and Technology Advisory Council puts CPS at the top of the eight key information technologies with software, data, data storage and data flow, networking, high-end computing, network and information security, man-machine interfaces, NIT and social life. At the same time, the National Natural Science Foundation of China (NSF), perennial commitment to funding research and development for the CPS research group, has reached as many as dozens. In Europe, the EU plans to invest 6 billion euros in 6 years to become the world's leading electronic systems.

In China, although relative to the current voice of the Internet is relatively high, CPS also seniority is still shallow. But the country has been in the "12.5" plan will be put forward as the future of China's information technology industry, one of the important direction of development. Correspondingly, "973", "863" and the National Natural Science Foundation have also put forward the corresponding scientific research program to adapt to the country's future strategic tendencies.

CPS SECURITY REQUIREMENTS

CPS has changed the way of human and natural physical world, it can be applied to smart grid, traffic control, environmental control and other key areas of national economy. GPS applied to the smart grid, the key is how the sensor technology and power system organically combined, that is, the physical system and information systems for the integration of new industrial systems. In the process of information fusion, information security is the prerequisite for CPS to be applied. Therefore, CPS puts forward higher requirements for information security. According to the information security characteristics of the CPS security system security requirements are summarized as follows [2-6]:

A) Data confidentiality refers to the ability to maintain confidentiality of information during data transmission and storage and to prevent unauthorized access to information by unauthorized third parties.

B) Information integrity refers to the modification of data or other resources that cannot be authorized by a third party, and the lack of integrity of the information results will result in fraud.

C) Availability means that the CPS system can provide the necessary services when needed. High availability CPS system needs the following characteristics: the physical layer can automatically deal with hardware failure, system updates, power load and other emergencies, to provide the correct service; information layer to deal with denial of service attacks, to provide the right information processing services.

D) Authentication, refers to the communication process, the mutual communication between the two sides must confirm the true identity of each other to prevent the fake node access to important resources and information, especially in cross-domain authentication and cross-network authentication, to ensure that data communication during the calculation and communication process is real.

E) Non-repudiation, refers to the communication process, all participants cannot deny or deny the operation and commitment has been completed. The use of information source evidence to prevent the sender does not really deny the information has been sent, the use of evidence to submit to accept the recipient to accept the information has been accepted.

F) privacy protection, privacy and security mainly refers to the user privacy and security, in the CPS system, the user's personal information and their participation in the behaviour can be divided into two aspects of privacy and privacy for different groups need to use different privacy protection technology, to avoid the user's information disclosure, by lawless elements to obtain.

POTENTIAL THREATS TO CPS SECURITY

Due to the inherent high sensitivity, high reliability and high connectivity of CPS, the safety performance of CPS is much higher than that of ordinary Internet. Especially in the network information layer, the communication process may involve heterogeneous networks, need to consider the security risks of different network connections, when the background network for the cloud computing network, but also need to take into account the corresponding cloud computing security risks. In general, CPS security from the perspective of information and infrastructure can be divided into two categories: infrastructure security and information security.

Infrastructure Security Threats

In different CPS systems, there are a number of infrastructure: sensors, routers, servers, protocols, etc., which provide critical services for the normal operation of the CPS system. Accordingly, there are the following security threats: physical damage, equipment failure, line failure, electromagnetic interference, and internal threats. As the CPS system is highly sensitive to the physical environment, in the physical process to prevent these security risks at the same time, the need to design CPS system when the use of high security and physical entities.

Information Security Threats

According to the three levels of CPS system, information security threats can be divided into three aspects: physical layer (perceptual layer) threat, information layer threat and application control layer threat. Physical layer threats include node capture, denial of service attacks, node control, passive attacks, clock synchronization attacks, crash attacks, exhaustion attacks, unfair competition, eavesdropping, tampering, and interference. Information layer threats include denial of service attacks, authentication attacks, cross-network attacks, routing attacks, malicious code, distributed denial of service, user privacy disclosure, control network Dos attacks, flood attacks, error path selection, tunnel attacks. Application control layer threats include control command forgery attacks, perceptual data tamper attacks, control network DOS attacks, resonant attacks, viruses, Trojans, cloud computing service threats, and vulnerability attacks.

CPS SECURITY SOLUTION

CPS solutions can be stratified discussion, respectively, to introduce the solution of each layer, see Table 1.

Sensing Layer Solution

The sensor of the sensing layer acquires the external entity information, which is constructed by these wireless sensors into the wireless sensor network. The sensor layer needs to consider the safety of the sensor network. The perceived layer of node computing, storage capacity is weak, cannot use complex encryption algorithm, so the need to design lightweight password algorithms and protocols. In order to prevent the node from being controlled, steal or tampered with, it is necessary to perform node authentication and data integrity verification. Through the expansion of the spectrum, the message priority and other security means to prevent the perception of the frequency interference. Using intrusion detection and intrusion recovery mechanism as a passive attack security measures to improve the robustness of the system.

Network Layer Solution

The network layer consists of a large number of heterogeneous networks, different networks to resist security threats in different ways, so the design of the network layer security structure need to consider the network layer compatibility and consistency. Network layer security tasks include network layer identity authentication, network resource access control, data transmission confidentiality and integrity, remote access security, routing system security. The security structure of the network layer has two layers: point-to-point security sub-layer and end-to-end security sublayer. Among them, the point-to-point security sub-layer guarantees the security of the data in hop-by-hop transmission. The corresponding security mechanism includes mutual authentication between nodes, hop-by-hop encryption, and cross-network authentication and so on. The end-to-terminal layer primarily implements end-to-end confidentiality and protects network availability. The corresponding security mechanisms include end-to-end authentication and secret key negotiation, secret key management and cryptographic algorithm selection, denial of service and distributed denial of service attack detection and defense, hierarchical architecture, broadcast radius limit, port interception and so on.

Collaborative Solution Solutions

The task of the collaborative processing layer is to collect useful data and then analyse and process the data. Therefore, the security task of this layer is to identify and delete the malicious information in the data source, collect the effective information and keep it on the basis of security. In addition, the collaborative processing layer of the synergy of the information obtained can have different sources, there may be different receivers, so in order to ensure the confidentiality and integrity of the data, the recipient and the sender need to be certified, and the information content and information sources are separated to protect the privacy of users. The security measures of the collaborative processing are as follows: virus detection, good confidence in data sources, access control box disaster recovery, secure multi-party computing and secure cloud computing, and efficient data mining for encrypted data.

Application Control Layer Solution

The application layer service is different because of the application of CPS system, and the corresponding security requirements are different. Therefore, it is necessary to provide targeted security service according to the specific application. In general, the protection of user privacy is the most common security services, such as in the medical system, the need to protect the patient's personal privacy, the patient's personal information and medical records of the contents of the need to be separated to prevent user privacy theft by outsiders. In addition, unauthorized access is prohibited, and can be secured by computer security measures to ensure this. Application control layer security measures are mainly differentiated database security services, user privacy protection mechanism, access control, security software, patches, upgrade systems.

CPS SAFETY KEY TECHNOLOGY

Large-Scale Entity Identification and Authentication Technology

Identity and addressing structures include identity identification, location and exchange labels. The identity of the node is determined by the relationship between the node and other network organization; the location address is determined by the location of the nodes in the network and the topology of the network. The structure of the exchange tag is similar to a transmission mode and virtual path identifier, providing connection-oriented services for both parties. IN the CPS, the sensor network authentication mechanism is an important part,

CPS wireless sensor network authentication technology mainly includes based on lightweight public key encryption authentication technology, pre-shared key authentication technology, based on one-way hash function authentication [7]. In literature [8], the author introduces the authentication between high-level application and terminal network entity, and analyzes the large-scale entity identification and authentication technology. Due to the limited resources of the terminal network entity, the authentication mechanism must be efficient, and the calculation and communication costs should be as small as possible to leave a certain operating space to meet the CPS certification requirements.

TABLE 1. CPS security solutions

	Security threats	Security measures
Sensing layer	Node control Node steal Node tampering Frequency interference	Authentication Data integrity verification Spread spectrum Message priority Intrusion Detection and Intrusion Recovery
Network layer	Network layer authentication Access control of network resources Confidentiality and integrity of data transmission Remote access security The security of the routing system	Mutual authentication between nodes Hop-by-hop encryption Cross-network authentication End-to-end authentication and key negotiation Key management and password algorithm selection Denial of service and distributed denial of service attack detection and defense Hierarchical architecture Broadcast radius limit Port blocking
Collaborative processing	Data confidentiality Data integrity	Virus detection The reliability of the data source is good Access Control Box Disaster Recovery Secure multi-party computing and secure cloud computing Efficient data mining of encrypted data
Application control layer	User privacy	Differentiated database security services User privacy protection mechanism Access control Security software Patch Upgrading the system

Safety Control Technology

CPS introduces the control system into the information network and brings new security problems. At present, the research on the control system has not yet formed the mature model and strategy. The existing research mainly focuses on two aspects: attack behavior pattern analysis and robust network control system construction.

Privacy Protection Technology

Privacy protection is also an important issue for CPS security. Users who enjoy CPS services may also disclose their own information. PS tasks are usually completed by a number of nodes to collaborate, the process of communication nodes may also cause privacy disclosure. The current research on CPS privacy protection focuses on the encryption of video privacy data in wireless sensor networks, and protects the confidentiality of data through the concealment, encryption and multipath transmission of multimedia information. At present, privacy protection technology can be divided into two technical routes: user anonymous and safe multi-party calculation. User anonymity refers to the use of data transformation, randomization and other means to achieve the hidden information of user information. The classical algorithm is the k-anonymous algorithm (the algorithm [9, 12] has a detailed analysis). Safe multi-party calculation refers to the participation of parties can only participate in collaborative computing with private data. At the end of the calculation, each party only knows its own input data and the final result, but cannot get other people's privacy data. In fact, SMC is a distributed protocol. In this protocol, n members m 1, m 2, ., m n. Respectively, to hold the secret data D 1, D 2, D n, attempt to calculate the given function F (D 1, D 2, , D n). In this calculation, each member m i (i = 1, 2, , k) knows only its own input data D i and the final result F (D 1, D 2, , D n). SMC security is effective, but its operation efficiency is low, so in the field of privacy protection applications need to be further improved.

CONCLUSION

Security is a problem that cannot be ignored in the development of CPS. Due to the particularity of CPS network, it will face great security challenge. This paper analyses the security threats faced by CPS and gives the solution of security. Finally, it analyses the large-scale entity identity and authentication technology, security control technology and privacy protection technology. CPS in the prevention of attacks outside the system and the protection of user privacy and other aspects of security technology remains to be further studied in order to make it more perfect.

ACKNOWLEDGMENT

This work is supported by the national natural science foundation of China under grant (No.61572142, 61370082), natural science foundation of Guangdong province under grant (No.2015A030313490).

REFERENCES

1. Lee E A Cyber-Physical Systems-Are Computing Foundations Adequate[C]}} Position Paper for NSF Workshop on Cyber Physical Systems Research Motivation, Techniques and Roadmap. 2006
2. Cardenas a, Amin S, Sastry S. Secure control: Towards survivable cyber-physical systems. System, 2008, 1(a2):9.
3. Tang H [, Tan F, Song Bet al. Cyber-physical system security studies and research//Multimedia Technology (ICMT), 2011 International Conference on, Zurich, 2011:4883-4886.
4. Venkatasubramanian K. Security solutions for cyber-physical systems [PhD Dissertation]. Tempe: Arizona State University, 2009.
5. Reed T C. At the Abyss: An Insider's History of the Cold War. New York:presidio,2004
6. Govindarasu M, Hann A, Sauer P. Cyber-Physical Systems Security for Smart Grid. New York:PSERC publication ,2012
7. YANG Geng, XU Jian, CHEN Wei, et a1. Security Characteristic and Key Technology of the Internet of Things [J]. Journal of Nanjing University of Post and Telecommunications Natural science, 2010, 30(4):20-29.
8. WU Chuankun, First Exploration for Security Consumption of the Internet of Things [J]. Strategy and Decision Research, 2010, 25(4):411-419.
9. DING Chaoyang Lijun, wu Meng, Security system structure and Key Technology of IoT / CPS [J], zhongxing Communication Technology, 2011, 17(1):11-16.
10. WU Chuankun, First Exploration for Security Consumption of the Internet of Things [J]. Strategy and Decision Research, 2010, 25(4):411-419.
11. BAO Lei, ZHANG Dai yuan, the Internet of Things and Privacy Protection Technology [J], Electronic Technology, 2010, 23(7):110-112.
12. ZHOU Shuigeng, LI Feng, Tao Yufei, et a1. Privacy Protection Review Oriented Database Application [J]. Chinese Journal of Computers, 2009, 32(5):847-861.