Researches Based on Subject-Oriented Security in the Cyber-Physical System

Caixia Zhang[1](✉), Hua Li[1], Yuanjia Ma[2], Xiaoyu Wang[3], and Xiangdong Wang[2]

[1] Foshan University, Guangdong 528000, China
zh_caixia@163.com
[2] Guangdong Provincial Key Lab of Petrochemical Equipment Fault Diagnosis,
Guangdong, Maoming 525000, China
[3] The Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China

Abstract. The security research of Cyber-physical system is a dynamic development process. Because no single technique could ensure the absolute safety of CPS, so its safety problem must be considered from the overall and systematic researches. Based on the structure of CPS, CPS is here divided into some subjects, and various subjects are then discussed in face of security threats in the design of subject oriented CPS security model. This model is supplied with the WPDRRC security system model as a protective layer. With the technology oriented CPS system, subject oriented system security will have superiorities such as initiative, systemic, portability and simplified.

Keywords: Cyber Physical System (CPS) · Security researches · Subject-oriented · The WPDRRC security model

1 Introduction

The technologies in computers, wireless communication, the network control, sensor and embedded technologies are rapidly developed. The physical system emerge. Once the concept was put forward by the literature [1], it is widely intentioned in the domestic and foreign fields in computers, communication, control, health, and so on, because it has wide application prospects and commercial values [2].

In a broad sense, the cyber-physical system is physical network equipment which can be controlled and trusted. At the same time, it can deeply integrate the computation, control and communication. Through the calculation process and physical process of interacting feedback, it can achieve fusion depth and real-time interaction to increase or expand with new functions and CPS monitors, or it can control a physical object entirely in a safe, reliable, efficient and real-time style. The ultimate goal of CPS will surely realize the complete integration of the information and physical worlds, build a controllable, reliable, scalable, secure CPS network, and it will ultimately change the human construction in engineering physics system [3].

Xiangdong Wang: Prioject Supported the National Natural Science Fundation of Guang dong (S2013010014485) and Technology Project of Guangdong Province (2013B020314020).

V.C.M. Leung et al. (Eds.): TridentCom 2014, LNICST 137, pp. 351–359, 2014.
DOI: 10.1007/978-3-319-13326-3_33

At present, the CPS system research is mainly focused on the concept of CPS, CPS architecture, CPS modeling, CPS application and CPS challenges [4–6]. Like all traditional network, security and reliability are very important. For the large information and physical component, interaction has more freedom and equality than the traditional network. Therefore the CPS system will face a series of new security problems. How to construct the CPS security architecture, the completion of the safety communication and security control is an important and challenging problem.

For the security of CPS, scholars at home and abroad have launched a series of discussions from the angle of technology. The security problem about the congestion and tampering with CPS perception data in the CPS system has been discussed [7], which will cause the error of the network state estimation and the error control command. Privacy protection, security controls and security vulnerability assessment technology of CPS have preliminarily been studied. Based on semantic models in CPS, the security analysis of information flow was put forward through information flow tracking and automated analysis process algebra specification [8].Starting from the structure of the CPS, the CPSlayers of security threats and solutions are analyzed in literature [9]. Fine-grained model of CPS was presented [10] in order to ensure the safety of CPS system.

However, the research of CPS security is a dynamic development process. Any single technique is too difficult to guarantee the absolute security, so the safety problem must be considered from the overall and systematic angle. This paper segments subject-oriented and discusses various subjects to solve security threats from the CPS system structure. Based on the theme of the CPS system security, the subject-oriented security model has more advantages than the technology-oriented security model.

2 CPS System Structure

The structure is the most fundamental contents in CPS system, and the scientific and reasonable system structure is the base of the realization of overall safety performance, and it plays an important role in the system safety analysis.

Considering the various definitions of CPS system and the need of completing the various functions, the CPS system is divided into physical layer, network layer and dynamic control execution layer in-depth analysis on the basis of [11–13].

1) Physical Dynamic Layer: The physical dynamic layer refers to the CPS system and the physical environment in close connection with the large number of isomorphic or heterogeneous physical components.

2) The Communication Network Layer: The communication network layer which controls the execution layer provides the real-time and effective multidimensional perceptual information, data and so on..

3) To Control the Execution Layer: The executive control layer in the real-time acquisition is the integrated perception information under premise according to the specific control demands of the semantic rules and the control logic in order to realize the large-scale entity in the real-time control and the global optimization control.

3 CPS System Topic Partition

CPS is a complex dynamic system. From a technical point of view to study the security of the system, and from the technical details of a starting solution which is the emergence of CPS security issues, it will make the CPS system security in a passive position. Facing the new emerging safety concerns, the security must be studied through the analysis to obtain a solution. Then it will enhance the CPS system security research in a chaotic state, and a passive defense situation.

In view of the above analysis, from the angle of technology on CPS system security passive study, the proposed subject oriented CPS system design idea and purpose are the security problems of CPS which is also subject to study, so that CPS system security will break up the whole into parts.

In the depth study of CPS function, on the basis of the system structure and the operation mechanism, the abstract is divided into perceptual systems, storage systems, communications equipment, intelligent network, distributed computing, control system and the implementation of the system. The seven themes are shown in figure 1.

3.1 CPS Theme Connotation and Technical Support

1) CPS system, perception system of dynamic physical layer in various physical components, which track location, condition, environment and other kinds of real time information access, needs a lot of sensing devices. The technical support can be provided by RFID, GPS global positioning technology, sensor technology, image capture apparatus, laser scanning, mobile terminals and other technology development for the perceptual system.

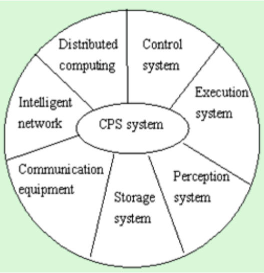

Fig. 1. 7 subjects of CPS system

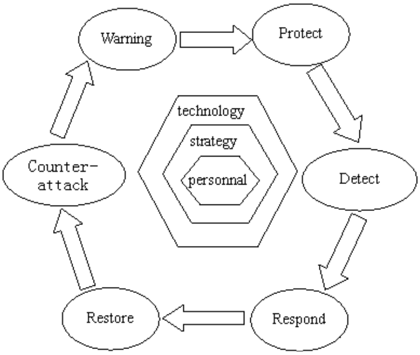

Fig. 2. The WPDRRC security model

2) Storage system: the perception system generates a large amount of real-time information of data stream, and the control system which produces a large number of parallel control instructions requires powerful storage support. NAS storage technology, cloud storage technology, direct attached storage, network attached storage, storage area network and discs [11] can server storage scheme for CPS system storage system with some technical support;

3) CPS system of communication equipment in dynamic physical layer and application layer is connected to the calculation of a variety of communications equipment for the CPS system in material objects, so people, objects and other information can provide hardware support.

4) CPS intelligent network in real-time communication and the information interaction require a certain transmission pathway of CPS intelligent communication network. CPS intelligent communication network is required in the transmission of information in the course of the digital / analog converter.

5) CPS distributed computing systems require real-time processing massive information system to realize a large number of physical devices with optimal control. The powerful computation and information processing ability are the keys of realizing this goal. Distributed computing, grid computing[14] or cloud computing, distributed computing technology for CPS system are all provided to calculate the theme of technical support.

6) Control system: according to CPS function target and control requirements, the collection and analysis of all kinds of information systems, real-time monitoring and integrated simulation are all generated by applying the control command.

7) Execution system: the implementation system is the control system which generates instruction execution mechanism. CPS system is involved in all walks of life, the performing system also differs in thousands of ways according to different applications.

3.2 CPS System Subject Facing Security Threats

The CPS system is large and complex because it has many hidden security dangers, vulnerable to various attacks, combined with the structure of CPS system, CPS system from themes, and analysis of CPS system potential security threats.

1) Sensing system: it includes hardware, node capture, attack, denial of service, collision attack, energy depletion attack, perception data destruction, tapping, illegal access and other security threats; 2) Storage system: it includes database attack, privacy disclosure, unauthorized access, virus, Trojan horse attacks and other security threats; 3) Communication equipment: it includes physical destruction, Hello flooding attacks, tapping, virtual attacks; 4) Intelligent network: it includes network attack, routing attacks, malicious network, response to selective forwarding attack, tunnel, misleading, direction, black hole attack against security threats; 5) Distributed computing: it includes cloud computing services such as security threat; 6) Control system: it includes unauthorized access, vulnerability, control command forgery attacks, malicious code attacks, denial of service attacks, blocking, tampering with CPS data and other security threats; 7) Execution system: it includes equipment failure, node control, physical destruction, and denial of service attacks, unfair competition and other security threats.

3.3 CPS Security Service Demand

Different from the traditional communication network, computer network, Internet, CPS information in the system and the physical component interaction are more convenient than traditional network. And the frequent, intelligent component can enjoy more freedom and equality. Therefore, the CPS system security problems put forward higher requirements to the social service.

1) Confidentiality: the unauthorized person cannot obtain the content of the message, but CPS system complex network composed of the information is easy to leak, so it must ensure that the system information transmission will not be tapped.

2) Integrity confidentiality guarantees the information safe, but it cannot guarantee that the information is to be modified. CPS system information from emergence to application process is due to transmission network openness, vulnerable to attackers tamper, add, resulting in the loss of information and the data is damaged. The packet message authentication mechanism, data monitoring and other means to identify can ensure data integrity and transfer command.

3) Identity authentication of identity authentication is the most important one of all the security properties; other security services are dependent on the service implementation, the node which can confirm the communication node identity.

4) Access control determines who can access the system, who are able to access the resources system and how to use these resources. The appropriate access control can protect CPS system of massive terminal information from unauthorized physical access.

5) CPS system adaptability to dynamic characteristics of the physical entity must be able to target the change of the external environment, rapid response to the intelligent selection, adaptive adjustment of the balance state, to ensure that the system can adapt the changes in safety.

6) In providing personalized privacy of user experience, CPS can, at the same time, master more user privacy. On the other hand, CPS tasks are normally performed by distrust of the entity in the process of collaboration. The entity output information may cause privacy.

7) Real-time, or timeliness [14]:Once the network delays, the actuator can receive controller command, and the system will not enter into a stable state. The availability of the CPS requirements is more stringent real-time environment than traditional information system.

4 Subject Oriented CPS System Security Model

CPS system security model formulation can be achieved in CPS overall system security protection system, overall, plan and normative, which makes CPS system control flow and data flow information confidentiality. The integrity and availability are comprehensive, reliable protections.

At the beginning of the design, due to the OSI reference model and TCP/IP reference model without consideration of the security problems in network communication, the reference model of any dimension to find security vulnerabilities will be enemy attack. In order to avoid similar situations, the subject oriented CPS system security model design, this paper uses the WPDRRC security system model for the CPS security model of protective layer.

WPDRRC security system model is considering the safety aspects, technology, management, strategy, project the respect such as the process, the design and construction of the security side case strong basis is closely guided here. As is shown in figure 2.

4.1 Subject Oriented CPS System Security Model

In the CPS system security service demand as the basis, the CPS system as the basis, the WPDRRC security system model is introduced into the CPS system security model design, design subject oriented CPS system security model.

1) The Model Center. The model center in perceptual systems, storage systems, communications equipment, intelligent network, distributed computing, control system and the implementation of the system of the seven-theme service requirements of security as the core, in accordance with the overall, systematic thinking, combined with its own characteristics and needs of each subject and theme between interaction design requirements.

2) Model of the System. CPS system architecture consists of physical layer, network layer and dynamic control execution layer, in the design of security model, the three layers require both interrelated and need depend on each other. Therefore, this paper in the CPS system security model design puts forward the interlayer with protective layer of train of thoughts. When a layer of security threats passes through the isolating layer isolation effect, prevents the spread to other levels of security threats. On the other hand, between layers needed to have the cooperation function, as an organic whole, one layer of problems needs the other layer to provide the appropriate security measures, and the CPS system has become an organic whole security defense.

3) Model of the Protective Layer. The security of CPS system needs its own security policy, at the same time, needs protection. Therefore, in the CPS system security model, the WPDRRC security system model is introduced. WPDRRC warning, protection, detection, response, recovery, counter functions of six parts can all complement each other, so that the security of CPS system come into a flow entity.

4) Model, Validation of Safety Standards. Subject oriented CPS system security model in the outer layer is the safety management standard and verification system. The safety standards include CPS security and verification of the lack of universal recognized standards, safety management of security techniques, global trust degree evaluation, collaborative process of privacy protection, system validation considerations from system scheduling capability, system energy consumption, the speed of the system, the system memory usage, deadlock and privacy aspects of the research.

4.2 Oriented CPS Model Comparison

The technology of secure CPS system work flow as is shown in Figure 3.

Along with the rapid development of CPS, new technology also changes rapidly, and a kind of any new technology is not completely safe. Technically oriented research strategy will also need continue to carry out new technology of safety research, to meet a variety of technical and safety requirements.

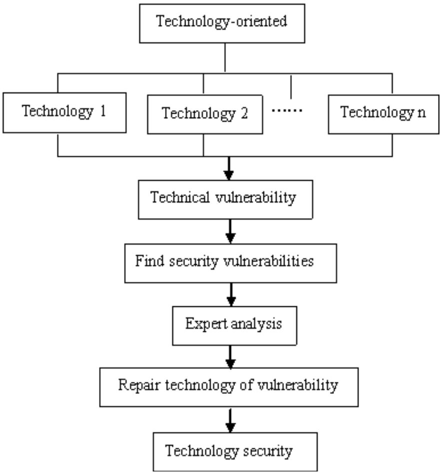

Fig. 3. Subject oriented CPS safety research process

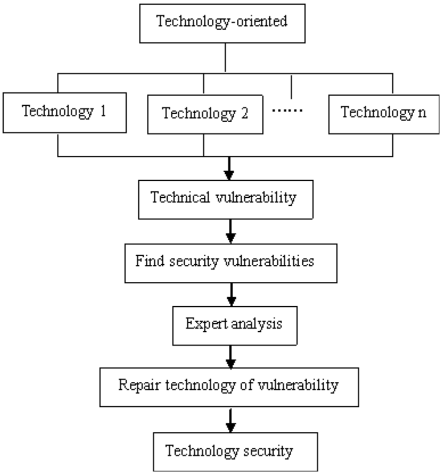

Fig. 4. Technology oriented CPS safety research process

Subject oriented CPS system security research process as is shown in Figure 4.

Researches can be active from each subject's own security needs, forming a closed loop security defense system, and can fundamentally change the CPS system security research in the passive position of state.

Subject-oriented study of safety design strategies leads to themes of safety demand as the research object, and leads to the theme of their own needs as the starting point, so it is relatively stable and oriented with respect to the technical security researches.

Subject-oriented security design research strategy has a better system. Each subject was a safety research. The importance of the theme, the connection and cooperation make it become an organic whole. And in the technical security research, it lacks the whole CPS system security planning, and ignores the CPS system sex.

Subject-oriented study of safety design strategies leads to themes of safety property as the object of study, and it has good portability..

To sum up, subject-oriented CPS system security research is better than the technology research of CPS security initiative, and its changes are numerous for their advantages are brief, systemic, and portable.

5 Summary

In the system, safety is one of development process problems which cannot be ignored. In the Internet design in the initial stage, because of the single attention to the practical application, ignoring the consideration of the system safety, the current Internet has many defects. Internet dependence of TCP/IP protocol has the bigger hidden safety trouble, and it makes Internet security in a passive position. Although active defense has got certain development, Internet security will not be able to reach the ideal state over a period of time.

As a global information technology and information industry's new development trend, the CPS system will be the information world and the physical world, which includes fusion and development of the computer system, embedded systems, industrial control systems, networked control systems, networking, wireless sensor network, hybrid system, permeability and economic life. In all areas of production it can produce far-reaching effect. Therefore, in the initial stage of development, the system security cannot be ignored.

This paper proposes the subject-oriented CPS system security model for CPS security research, and provides a good idea to effectively promote the development of CPS system.

References

1. CPS Steering Group. Cyber-physical systems executive summary (July 2011). `http://precise.seas.upenn.edu/events/iccps11/doc/CPS-Executive-Summary.pdf`, Smith, T.F., Waterman, M.S.: Identification of Common Molecular Subsequences. J. Mol. Biol. 147, 195–197 (1981)
2. Wang, Z., Xie, L.: Cyber-physical Systems: A Survey. ACTA AUTOMATICA SINICA **37**(10), 1157–1165 (2011)
3. He, J.: Cyber-physical Systems. Communications of China Computer Federation **6**(1), 25–29 (2010)
4. Tan, Y., Vuran, M.C., Goddard, S.: Spatio-Temporal Event Model for Cyber-Physical systems. In: Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Work shops, pp. 44–45 (2009)
5. Zhang, F.M., Szwaykowska, K., Wolf, W.: Task. scheduling for control oriented requirements for cyber-physical systems. In: IEEE Proceedings of the Real Time Systems Symposium, Barcelona, Spain, pp. 47–56 (2008)
6. Dillon, T., Potdar, V., Singh, J., Talevski, A.: Cyber-physical systems: Providing Quality of Service (QoS) in a hetero-generous systems-of-systems environment. In: Proceedings of 5th IEEE International Digital Ecosystems and Technologies Conference (DEST), Daejeon, USA, pp. 330–335. IEEE (2011)
7. Cardenas, A.A., Amin, S., Sastry, S.: Secure Control Towards Survivable Cyber-Physical Systems, In: The 28th International Conference on Distributed Computing Systems Workshops, pp. 495–500 (2008)
8. Akella, R., Tang, H., McMillin, B.M.: Analysis of information flow security in cyber–physical systems. International Journal of Critical Infrastructure Protection, 157–173 (2010)

9. Tang, H., Tan, F., Song, B., Li, N.: Cyber-Physical System Security Studies and Research, Multimedia Technology (ICMT), Beijing, 4883–4886 (2011)
10. Codella, C., Hampapur, A., et al.: Continuous Assurance for Cyber Physical System Security (2011). `http://cimic.rutgers.edu/positionPapers/CPSSW09%20_IBM.pdf`
11. Tan, Y., Goddard, P., Rezl, C.: A prototype architecture for cyber-physical systems. SIGBED Review, pp. 51–52 (2008)
12. Kang, W., Son, S.H.: The design of an open data service architecture for cyber-physical systems. ACM SIGBED Review **5**(1) (2008)
13. Tan, P., Shu, J., Wu, Z.: An Architecture for Cyber-Physical Systems. Journal of Computer Research and Development, 47 (2010)
14. Wu, M., Ding, C., Yang, L.: Research on Security Architecture and Key Technologies in Cyber-Physical Systems. Journal of Nanjing University of Posts and Telecommunications (natural science) **30**(4), 52–56 (2010)