International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.155-164
http://dx.doi.org/10.14257/ijsia.2015.9.1.17

A Systematic Review of Studies on Cyber Physical System Security

Peiyuan Dong[1], Yue Han[1], Xiaobo Guo[1] and Feng Xie[2]

[1]*School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing, 100876, China*
[2]*China Information Technology Security Evaluation Center, Beijing, 100085, China*
dongpeiyuan@bupt.edu.cn, pz_han@bupt.edu.cn

Abstract

Cyber-Physical System (CPS) is a system of systems which integrates physical system with cyber capability in order to improve the physical performance [1]. So far, it is being widely applied in areas closely related to national economy and people's daily lives. Therefore, CPS security problems have drawn a global attention and an appropriate risk assessment for CPS is in urgent need. According to the researches and discussions in recent years, we believe that most researchers have already established a comprehensive understanding about CPS. This paper systematically introduced CPS's conception, development and applications assisted. In addition, concerning about its aspects of safety and security, we also analyzed CPS's risks and new requirements as an up-to-date technique brings. We elaborate the existing work and propose a research focus that has not been paid enough attention to, and proposed a security framework for CPS. At last, after providing a classic modeling and simulation method of CPS, we bring forward a new idea for accessing the experimental results into existing systems.

Keywords: *CPS; safety; security; risk assessment; simulation*

1. Introduction

A Cyber-physical System (CPS) is a system of systems which tightly couple the computing components between the physical components, governed by the underlying processes and policies [2]. So that, CPS integrates networked computational resources into physical processes in order to add new capabilities into the original system and realize real-time perception, dynamic control, information services in large-scale projects.

In CPS, components are networked at every scale. You can find the applications of CPS everywhere. In the contemporary time, CPS is being applied in nuclear facilities, steel industries, chemical engineering, electric power and many other areas closely related to national economy and people's livelihood. Earlier in 2007, U.S. President's Council of Advisors on Science and Technology (PCAST) has ranked CPS as a national priority for Federal R&D [3].

As with all communication and computer networks, information, security is a big problem which can't be ignored during CPS network development process. CPS system inherits the advantage of wireless sensor networks, next-generation networks and network control system. However, it brings the defect into the network at the same time. CPS is being faced with a series of new security issues, such as security protocols seamless, global trust assessment, collaborative process of privacy protection, etc. Meanwhile, as a physical system, it requires safety and real-time property.

ISSN: 1738-9976 IJSIA

According to the researches and discussions in recent years, we already have a comprehensive understanding about CPS. But for the researchers who are not familiar with this subject, it's extraordinary difficult to understand this subject systematically without going through a large number of research work. Aims to provide a guide, in this paper we elaborate the existing work and proposes a research focus that has not been paid enough attention to. Therefore, people can get a general understanding about CPS in the least time.

This paper comes up with a CPS conceptual model, which systematically introduced CPS's conception, development and applications. In addition, concerning about its safety and security aspects, we analyze CPS's risks and emerging requirements. Through the elaboration of the existing work, we propose a neglected research focus. And then we proposed a security framework on CPS based on the threat analysis, which takes consideration of risk assessment from four angles: assets, threat, vulnerability and damage. At last, we provide a classic modeling and simulation method of CPS. With a discussion of the significance of the simulation, we propose a new idea for accessing the experimental results into existing systems.

2. Conceptual Model for CPS

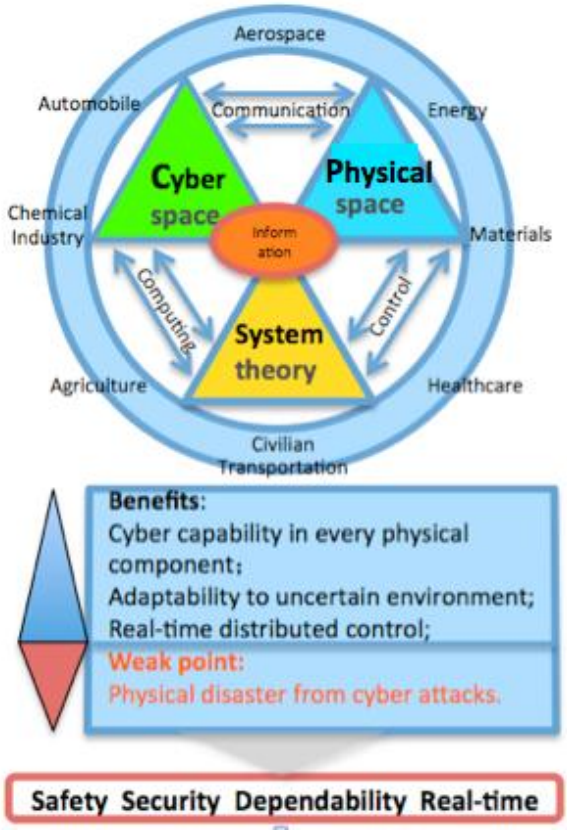


Figure 1. Conceptual Model for CPS

As shown in Figure 1, a Cyber-Physical System merges the physical space with the cyber space by information according to the system theory. It integrates the capabilities of

computing and communication with the monitoring and controlling of the entities in the physical world, so that builds a bridge attaching the cyber space to the physical space.

CPS is applied in every scale and every area, which contain aerospace, automobiles, energy, chemical industry, materials, civilian transportations, agriculture and healthcare [4]. The examples include micro- and nano-scale cyber and physical materials, controlled components, cooperating medical devices/systems, next-generation power grid, future defense systems, next-generation automobiles, intelligent highways, flexible robotic manufacturing, next-generation air vehicles, airspace management, and so on.

In a CPS, each physical component has cyber capability. Computing is deeply embedded into every physical component. The behavior of a CPS is a fully integrated hybridization of computational (logical) and physical action [5]. Moreover, the complete system has an excellent adaptability to the uncertain environment [6-7]. Its real-time distributed controlling used in large scale network also achieved good results [8].

We believe that the new technology will bring us wonderful life. But when we enjoy the benefits of it, do not forget about the risks and the additional requirements of it. However, the truth is, highly integrated system has brought new risks to us. People can easily affect the physical facilities from the cyber space. If the physical environment can be taken over by malicious entities, serious damage can occur. The utilization of CPS may provide a more convenient opportunity for terrorists to destroy the critical infrastructures. Therefore, we have to ensure that a CPS is dependable, safe, secure, efficient and real-time [9].

3. Security and Safety Framework for CPS

In the process of the integration between cyber space and physical space, the use of the general software, hardware, interfaces and protocols, the access to the Internet, all theses may bring about a large number of risks that we have to consider about.

As shown in Figure 2, we are not just focus on the security of CPS. Furthermore， the significance of the safety is even higher than the security. The functional safety and the physical safety must be dependable. Certainly, do not forget its real-time requirement. Compared to the traditional IT systems, the demands for CPS have occurred considerable changes. The traditional IT systems' requirements for security are Confidentiality, Integrity and Availability. However, CPS put the Availability first, followed by Integrity.

To make CPS systems more resilient, the research must integrate the knowledge of cyber security, human interaction and complex network design to address the threats. Aim to maintain survive with no loss of critical function after natural disasters, human errors, or intentional cyber attacks, we need to accomplish the risk analysis with the classification (software/ hardware/ human being). Although each physical node contains software in it. As an integrated system, we cannot analyze it simply classified into software and hardware. We focus on the information streams flow through the whole system and the physical entities.

Except the physical interferences, attacks, destructions to the physical components, what else can be attacked is the information. An attacker could eavesdrop and tamper the sensor information, the store information or the control information, and even modify the logic of control algorithms. These will cause unexpected delays of the system, and even denial of service (DOS), which can pause the system's stable operation. These common defect or failure in IT systems are not been allowed happening in CPS. For instance, the brief outages for critical infrastructure may cause immeasurable losses and impacts. The suspension of a medical CPS is even fatal.

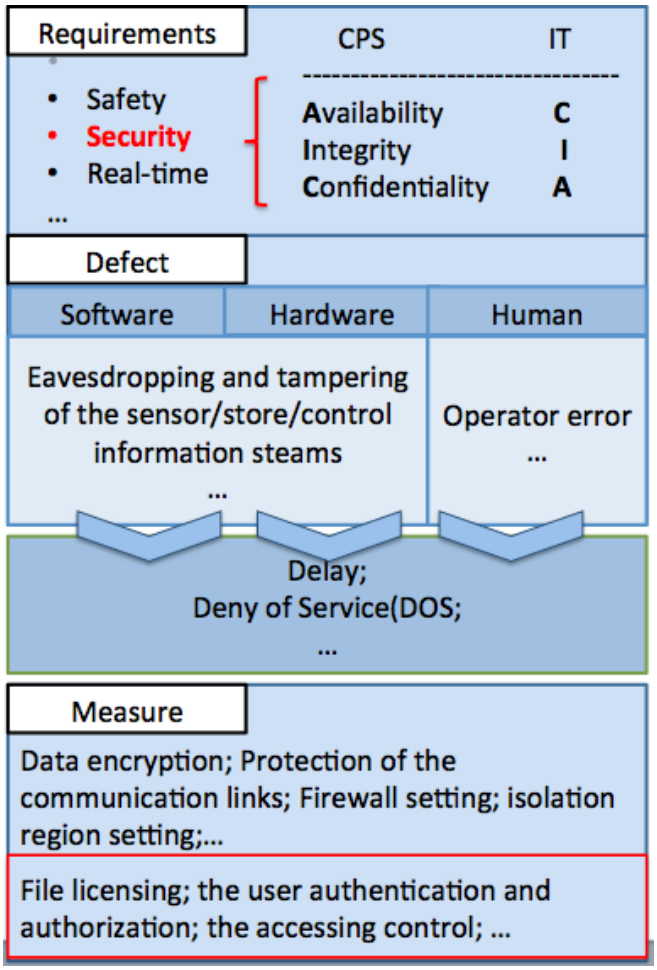


Figure 2. Security and Safety Framework for CPS

Then what measures would always been taken? Data encryption, protection of the communication links, firewall settings, isolation region settings and so on. Here comes a question. We focus too much on the information tamper of the sensor or the analog-digital conversion components in the past.

So, in this paper, what we would like to emphasize is that, we should make some efforts to perfection the file licensing, the user authentication and authorization, and the accessing control on the critical physical nodes, which have not arouse adequate attention in the research among recent years. Attacks on the critical physical nodes will bring more serious damage. If an attacker has the ability to access to the PLC (Programmable Logic Controller), he could gain authorities to launch more deadly attacks. Penetration testing in the critical nodes can also make efforts to improve the dependability of a CPS.

4. Security Framework for CPS

4.1. Security Framework

Now the security research of CPS is focused on the security of information and controlling. Information security solves the problems of information collection, processing and sharing nondestructively in large-scale, high-mix, collaborative autonomous network environment. Its

key point is enhancing existing security mechanisms, user privacy protection, efficient processing of massive data encryption, etc. The controlling security solves the controlling problems in the networked systems with open interconnection and loosely-coupled architecture. It focuses on overcoming the influence from attacks on system estimation and control algorithms.

As shown in Figure 3, it is a CPS security architecture proposed by this paper. In the cyber filed, multiple security mechanisms for a same security problem is set to realize the defense in depth, using hierarchical network structure and from and starting from each logical hierarchy. In the control field, security threats is analyzed by means of traditional delay, interference, and fault model and security control can be achieved with the use of tolerant control, distributed estimation, robust estimation and etc.

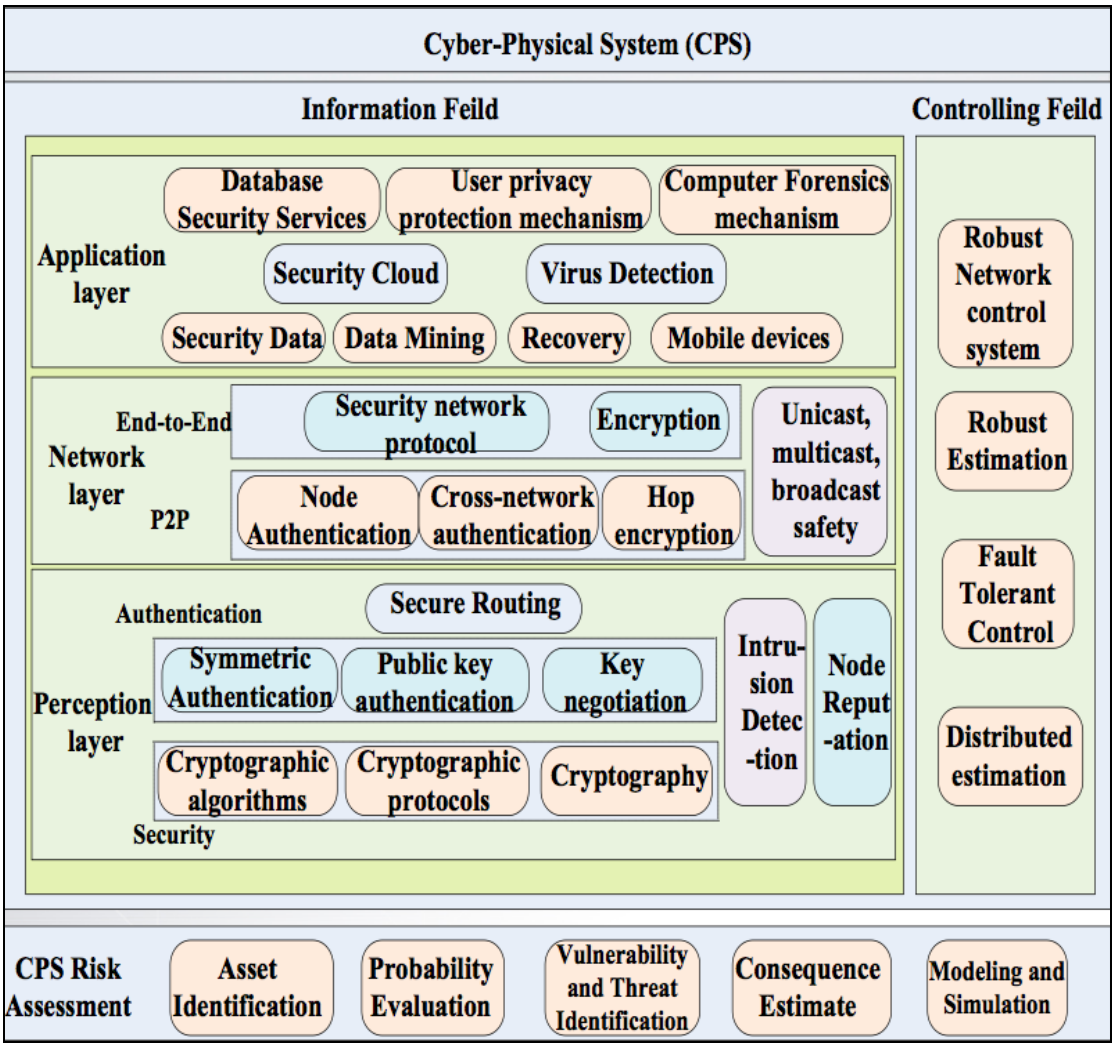


Figure 4. Security Framework for CPS

4.2. Security Structure in the Framework

4.2.1. Security Architecture in Perception Layer: In perception layer of CPS, a closed system composed of sensor network, whose all communication with external networks must depends on the gateway node, the security issues of the sensor network itself is the unique

factor to be considered in the design of security architecture. In CPS environment, perception layer is more vulnerable to external cyber-attacks, so establishing intrusion detection and intrusion recovery mechanisms and improving the system robustness is another important issue in perception layer. And establishing a credibility model, making a behavioral assessment on suspicious nodes and reducing the impact of malicious behavior are important tasks in perception layer. In addition, a mutual trust mechanism between sensor nodes and external networks to ensure the secure transmission of sensory information should be taken into consideration.

4.2.2. Security Architecture in Network Layer: In network layer, both the sensory data and controlling commands are time sensitive, and a large number of heterogeneous networks with different performance and defense capability against cyber-attacks make special security protocols aiming at network specificity an urgent demand. Security architecture can be divided into two sub-layers: point- to-point security sub-layer and end-to-end security sub-layer. The point-to-point security sub-layer could ensure the data security during the hop transmission. Its corresponding security mechanisms include: mutual authentication between nodes, hop encryption and across-network certification. The end-to- end security sub-layer could ensure the end-to-end confidentiality and protect the network availability. Its corresponding security mechanisms include: the end-to-end authentication and key agreement, the key management and cryptographic algorithm selection, the detection and prevention of Dos and DDoS attacks. Further, special security mechanism for unicast, broadcast and multicast should be designed according to the different network communication modes.

4.2.3. Security Architecture in Application Layer: The design of security architecture in application layer must follow the principle of differentiated services. As there is a wide variety of applications of CPS, security requirements are different. Even for the same security service, there may be completely different definition for different users. Therefore, providing targeted security services according to the users' needs is the core idea of the design. The main challenges in the application layer include: hierarchical access to the sensory data and the privacy protection in the user authentication process.

4.3. Risk Assessment for CPS

CPS is being exposed to various kinds of risks and a well- designed risk assessment for CPS will provide an overall view of CPS security status and support efficient allocations of safeguard resources. When making risk assessment for CPS, 4 elements should be taken into consideration: asset, threat, vulnerability and damage. Asset and damage is positively related and they should be banded together. The final risk value is positively related to the four elements.

Assets are tangible or intangible presence, which have a direct value for business or organization and need to be protected. Assets quantization can be considered from three aspects: direct economic losses, indirect economic losses and casualties. Threat is factors or events that can be a likelihood of potentially damaging from the outside for the assets of enterprises or institutions. The quantification of threat can be conducted through the threat matrix, which have seven angles includes intense, stealth, time, technical personal, information knowledge, physical knowledge and access, proposed by US Sandia Lab [10]. Vulnerability is a kind of condition or environment which exists as corporate or institutional assets and can be utilized by threat to cause a loss to the assets. Vulnerability quantification can be quantified through expert evaluation method or comparison with best practices in

industries. Methods can be adopted to simulate the real components, data stream and entity stream of CPS to anticipate what will happen to the whole system and to obtain the possible damage [11].

5. Modeling and Simulation

5.1. Modeling and Simulation Method

In CPS simulation, a combination of physical real components and software simulation components can be adapted.

According to our proposed framework, we can simulate the physical components and use an emulation testbed based on Emulab (or Opennet++) to recreate the cyber components with networked industrial control systems such as SCADA servers and corporate networks.

The models of the physical systems are developed using Matlab/Simulink, from which the corresponding C code can be generated using Matlab Real Time Workshop. The generated code is executed in real time and can interact with the real components in the emulation testbed. PLC can be a good representative for interaction. From an operational point of view, PLCs receive data from the physical layer, elaborate a "local actuation strategy", and send back commands to the actuators. PLCs execute also the commands that they receive from the SCADA servers (Masters) and additionally provide, whenever requested, detailed physical layer data [11].

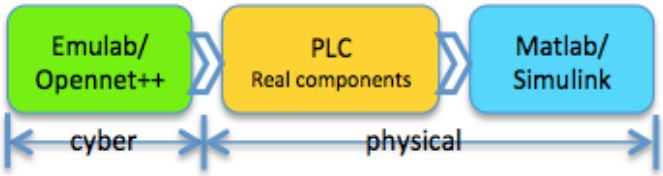


Figure 4. Simulation framework for CPS

5.2. The Meaning of Simulation

The experimental work for CPS has been done for a lot. Obviously, we all have verified that a disturbance of a cyber attack could impact the whole system. Is the significance of the simulation just a test for the practical application of the system? In fact, we can do more.

When a node is under attacking, several associated nodes may generate a data drift. We can regard the group of drifted data as a feature and use it to enrich the database of intrusion detection. Through this work, we believe that we will do efforts to perfect the self-repair logic of CPS and improve the dependability.

6. Conclusion

Although after several years of development, the research and application of CPS is still worth to be further in-depth inquired. The cross study of computing, communication, controlling and other disciplines brought a broad application prospects and more benefits to CPS, but it also brings a lot of new difficulties, such as designing of connection between different components. Through the description of two frameworks about CPS in this paper, we can better understand the conception and meaning of CPS, clarify the research content and developing direct. And provide guidance to more researchers for entering the CPS study area, therefore, more scientific areas will be integrated with the CPS design ideas. With the

progress of related technologies, I believe CPS will change our life and change our world as the developing direction of the next generation network.

Acknowledgements

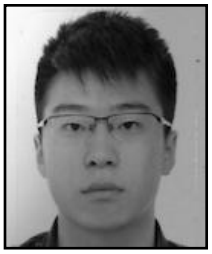
This work is supported by the following programs: the National Natural Science Foundation of China under Grant No.61170273; the China Scholarship Council under Grant No.[2013]3050; Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China (NO. CAAC-ITRB-201201); 2010 Information Security Program of China National Development and Reform Commission with the title "Testing Usability and Security of Network Service Software".

References

[1] T. Lu, "A New Multilevel Framework for Cyber-Physical System Security", TerraSwarm, (**2013)**.
[2] R. Baheti and H. Gill, "Cyber-physical systems", The Impact of Control Technology, Washington D. C.: IEEE, (**2011),** pp. 161−166.
[3] National Institute of Standards and Technology, Cyber-Physical Systems: Situation Analysis of Current Trends, Technologies and Chanllenges, (**2012)**.
[4] R. Rajkumar, I. Lee, L. Sha and J. Stankovic, "Cyber-physical systems: the next computing revolution", In Proceedings of the 47th ACM/IEEE Design Automation Conference, Anaheim, USA: IEEE, (**2010)**, pp. 731−736.
[5] E. A. Le, "Cyber-physical systems-are computing Foundations ad-equate? [C]", Position Paper for NSF Workshop on Cyber- Physical Systems: Research Motivation, Techniques and Roadmap, Austin, TX: Cyber-Physical Systems Workshop, National Science Foundation, (**2006).**
[6] National Science Foundation of the United States, Cyber Physical System (CPS) Program Solicitation [EB / OL], [**2011**-05-08]. http: //www.nsf.gon/pubs/2010/nsf10515/nsf10515.html
[7] CPS Steering Group. Cyber - physical Systems Executive Summary [EB/OL].[**2011**-05-08], http: ‖varma. ece. cmu. edu / CPS-Forum / CPS - Executive-Summary.pdf
[8] E. A. Lee, "Cyber Physical Systems: Design Challenges[C]", 2008 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), (**2008**), pp. 363-369.
[9] K. Wan, D. Hughes and L. Man, "Composition challenges and approaches for Cyber Physical Systems [C]", 2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications,Suzhou, (**2010),** pp. 1-7.
[10] X. Feng and T. Lu, "Security Analysis on Cyber-Physical System Using Attack Tree", The Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, (**2013**).
[11] Y. Peng and T. Lu, "Cyber-Physical System Risk Assessment", The Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, (**2013)**.

Authors

Pei-Yuan Dong, she is a lecturer in School of Software Engineering, Beijing University of Posts and Telecommunications, China. Her research interests include network security and Cyber Physical System.



Yue Han, he was born in Tianjin, China, 1992. He received his Bachelor Degree in Information Engineering from Beijing University of Posts and Telecommunications in 2013. At present he is studying for his master degree of Software Engineering in Beijing University of Posts and Telecommunications and will graduate in 2016. His technical interests include information and network security and anonymous communication.

Xiao-Bo Guo, she was born in February 1990, at present studying for her master degree of Software Engineering in Beijing University of Posts and Telecommunications and will graduate in 2015. During her postgraduate, she had participated in the security research on Information and Communication Supply Chain and Cyber Physical Systems. Up to now, she had published 1 paper indexed by SCIE and 3 papers indexed by EI.

Feng Xie, he was born in 1977. He obtained his PhD from Chinese Academy of Science. His technical interests include information and network security, risk assessment.