Short Communication
Volume 10:6, 2021

International Journal of
Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

More Attention to the Cybersecurity of Industrial Internet of Things (IIoT)

Chih-Wei Chang*

Department of Management Information Systems, National Chengchi University, Taipei, Taiwan

Abstract

In the case of Taiwan Semiconductor Manufacturing Company (TSMC) who was forced to shut down several factories after revealing is being attacked by a malware in August 2018. The incident caused attention on the security of smart manufacturing industry whilst in the past, management issue of cybersecurity for Operational Technology (OT) were rarely discussed. As such if we are unable to provide good defense for information security among sensor networks and OT environment, the development of smart application system and industry 4.0 will be potentially precarious.

Keywords: Operational Technology • IoT • Sensors • IIoT

Introduction

Many sensors and IoT have been integrated into the Industrial Control Systems (ICS) and Industrial Automation and Control Systems (IACS) in the rapid developing smart factory or Industry 4.0. Yet most of IoT devices and existing ICS are vulnerable due to the inadequate physical security protection mechanism. In August 2018, TSMC was plagued by a ransomware and immediately lost operation revenue approximately USD $171M [1]. Similarly, researcher observed a situation occurred that at Iran where the hacker attacked one nuclear plant with mimic method [2]. Consequently ICS-CERT continuously reported threats among OT network environment. These incidents explain the consequence is dire once an OT environment or smart factory system is hacked thus failed functioning. Therefore, we shall take the safety of ICS and the cybersecurity threat into account. First, we have to build adequate information security protection capability, resorting for Industrial Internet of Things (IIoT), to ensure those systems can function continuously, and thus achieve their purposes and expect benefits.

In addition, some scholars recently have started to study IoT security via threat taxonomy, and others have highlighted the defense solution for cybersecurity of Industrial Internet of Things (IIoT) [3-12]. The examination discloses establishing dynamic security protection mechanism in variant industrial fields.

Enhance the cybersecurity of industry IoT system

It is universally reckoned that cyber security shall be thoroughly considered in the new system where initially planning, design, processing, and implementation to final operation shall be catered for. Furthermore, in-service IIoT and ICS systems must be able to assess security risk and manage information security. Purdue Enterprise Reference Architecture (PERA) provides a basic operating structure of an industrial control system [13]. Industrial Automation and Control System Security Committee purposes an ISA-99 standard with a framework to provide cybersecurity assessment tools in the OT field. Base on this framework, we can project multiple layers of defense to protect IIOT, or existing IACS systems.

***Address for Correspondence:** Chih-Wei Chang, Department of Management Information Systems, National Chengchi University, Taipei, Taiwan; E-mail: 107356509@nccu.edu.tw*

Received: July 02, 2021; **Accepted:** July 16, 2021; **Published:** July 23, 2021

Initially, network segmentation and the established access policies will effectively ensure data safety in whole system that includes device connection, senor network and Manufacturing Execution Systems (MES), and information exchange between OT and IT. Secondly, improve the smart application environment in order for enhancing security protection and prevent hacking events in each individual subsystem. Last, strengthen security management to achieve requirement of confidentiality, integrity and availability in IT systems, and to comply human health, facility safety, and environment control in OT fields (Figure 1).

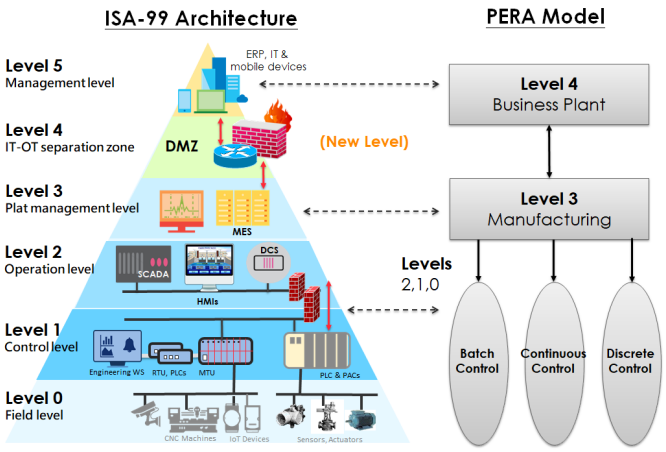

Figure 1. ISA-99 Architecture and PERA model.

Conclusion

Despite the lack of a physical protection mechanism for IIOT and IACS, we can analyze data exchange safety through system architecture, information requirement of subsystem functionality and simulation of protection intrusion detection, rechecking the entire network environment. Furthermore, apply multi-layer defense to enhance OT field security, protection, and renovation, in order to build-up cybersecurity mechanism, and sustain the whole chain functioning well to achieve the goal of IIoT and smart factory. The ISA-99 work has been utilized by the International Electro-technical Commission (IEC) to develop the multi-standard ISA/IEC 62443 series. The importance of evolving cybersecurity for IIoT and IACS are crucial. Topics about the latest standard for IACS and the related IIoT research examination are of our major attention.

References

1. Harkins, Malcolm and Anthony M. Freed. "The Ransomware Assault on the Healthcare Sector." *J Law Cyber Warfare* 6 (2018): 148-164.
2. Maglaras, A. Leandros, Ki-Hyung Kim, Helge Janicke and Mohamed Amine Ferrag, et al. "Cyber Security of Critical Infrastructures." *ICT Express* 4 (2018): 42-45.
3. Ray, P. P. "A Survey on Internet of Things Architectures." *J King Saud Univ Comput Inf Sci* 30 (2018). 291-319.
4. Ammar, Mahmoud, Giovanni Russello and Bruno Crispo. "Internet of Things: A Survey on the Security of IoT Frameworks." *J Inf Secur Appl* 38 (2018): 8-27.
5. Kouicem, Eddine Djamel, Abdelmadjid Bouabdallah and Hicham Lakhlef. "Internet of Things Security: A Top-Down Survey." *Comput Netw* 141 (2018): 199-221.
6. Alaba, Ayotunde Fadele, Mazliza Othman, Ibrahim Abaker Targio Hashem and Faiz Alotaibi. "Internet of Things Security: A Survey." *J Netw Comput Appl* 88 (2017): 10-28.
7. Yu, Xingjie and Huaqun Guo. "A Survey on IIoT Security." *IEEE VTS Asia Pac Wirel Commun Sym* 1 (2019): 1-5.
8. Sfar, Riahi Arbia, Enrico Natalizio, Yacine Challal and Zied Chtourou. "A Roadmap for Security Challenges in the Internet of Things." *Digital Commun Netw* 4 (2018): 118-137.
9. Boyes, Hugh, Bil Hallaq, Joe Cunningham and Tim Watson. "The Industrial Internet of Things (IIoT): An Analysis Framework." *Comput Ind* 101 (2018): 1-12.
10. Panchal, C. Abhijeet, Vijay M. Khadse and Parikshit N. Mahalle. "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures." *IEEE Global Conf Wirel Comput Netw* 1 (2018): 124-130.
11. Byres, Eric. 7 Steps to ICS and SCADA Security Plus White Paper. Tofino Security, (2012).
12. Mahmoud, Rwan, Tasneem Yousuf, Fadi Aloul and Imran Zualkernan. "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures." *Int Conf Int Technol Secured Trans* 1 (2015): 336-341.
13. Williams, J. Theodore. "The Purdue Enterprise Reference Architecture." *Comput Ind* 24 (1994): 141-158.

How to cite this article: Chang, Chih-Wei."More Attention to the Cybersecurity of Industrial Internet of Things (IIoT)."*J Sens Netw Data Commun* 10 (2021): 130.