A Novel Security Framework for Industrial IoT Based on ISA 100.11a

Hyunjin Kim, Sungjin Kim, Sungmoon Kwon, Wooyeon Jo,
and Taeshik Shon(✉)

Department of Computer Engineering, Ajou University, Suwon, Korea
hyunjin.infosec@gmail.com,
{ksjskyblue, tsshon}@ajou.ac.kr,
calmcombat@gmail.com, dndusdndus12@gmail.com

Abstract. This paper proposes a security assurance technology of IoT devices using their relevant standard, focusing on ISA100.11a, one of the ICS wireless communication protocols. The proposed security assurance technology is divided broadly into communication test and security function assessment. In detail, the communication test is divided into baseline operation test, resource robustness testing, and packet manipulation testing. The security function assessment conducted with the devices that have passed communication testing is proposed differing the required items, divided by the components of ISA100.11a, such as a field device, backbone router, and host so that an assessment appropriate for the hardware specifications and roles of each component is achieved. In addition, the paper seeks to facilitate the implementation and application of the proposed security assurance technology by proposing concrete methods or criteria for communication testing and security function assessment. Finally, this paper attempts to verify the conformance of the proposed security assurance by testing the security assurance technology in a testbed with a network environment where the standard ISA100.11a can work network environment.

Keywords: Industrial Control System (ICS) · Industrial IoT (IIoT) · ISA100.11a · Security framework

1 Introduction

The existing Industrial Control System (ICS) attempted to establish the reliability of security based on the isolated network through the separation from the external network, but the malicious codes, which had attacked the targets of ICS-related companies and institutions such as Stuxnet (2010), Duqu (2011), Flame (2012), Gauss (2012), Shamoon (2012), Havex (2014) and Black Energy (2014), was proven that there is a security vulnerability in the isolated network environment. Moreover, the Industrial Internet of Things (IIoT), that apply the Internet of Things (IoT) technology to existing ICS, is introduced and deployed for increasing service economically and efficiently. It means that the existing isolated network gradually gets openness and inherits security vulnerability in the existing Information & Communication Technology (ICT) environment.

T. Q. Duong et al. (Eds.): Qshine 2018, LNICST 272, pp. 61–72, 2019.
https://doi.org/10.1007/978-3-030-14413-5_5

The security vulnerabilities of ICS are increasing and can cause serious damage to economic, social, and human life, security must be considered before deploying and operating the IIoT technology in ICS.

One of the major technologies of the IIoT is the wireless communication technology, it has many advantages such as the convenience of maintenance, cost savings, scalability, interoperability, and mobility, so IIoT has been actively applied to the industrial field. According to the 2016 HMS, wireless network takes 4% in the entire market of the industrial network, but it reports that the Compound Annual Growth Rate (CAGR) amounts to 30%, so it is noted that the application of the wireless network is becoming gradually more active in the industry. For deploying and operating the wireless communication in the real industrial environment, ZigBee, WirelessHART, and ISA100.11a protocols are in the limelight, which are based on IEEE.802.15.4 Standard that has advantages in the node price and the number of nodes supported and supports low power consumption and low processing capability. Of them, ISA100.11a is a protocol with many benefits such as time management, security, interoperability and the use of open standards. But ISA100.11a was enacted lately, there are insufficient related studies and assurance systems. Therefore, this study would promote the improvement of the security of the ICS based on ISA100.11a by proposing a security assurance framework for a system using it.

First, Sect. 2 examines the overall background and present condition, such as the wireless communication network background of the ICS, representative protocols of the relevant wireless communication network and the present condition of the assurance systems of the ICS. Section 3 proposes a security framework for the ICS based on ISA100.11a. Section 4 facilitates the implementation and application of the security framework in the ICS, suggesting methods for measuring individual components of the proposed security framework and criteria for assessment and also execute framework in a testbed network to which ISA100.11a can be applied and carries out the proposed security assurance framework for the target devices. And lastly, Sect. 5 draws conclusions and introduces the follow-up studies.

2 Background

The existing ICS was mostly wire communication-based system using industrial serial communication protocols such as PROFIBUS, Modbus and CAN and industrial ethernet communication protocols such as EtherNet/IP, PROFINET and EtherCAT because of strict conditions of the characteristics of the environment of the industry, such as real-time communication, time-limited processing, high availability, functional safety and security (see Fig. 1). But nowadays wireless communication is deployed in ICS environment for reducing maintenance cost and increasing the usability of systems. To use wireless communication while satisfying requirements of the environment of the industry, ICS groups developed various technology and specification, such as Zigbee, WirelessHART and ISA100.11a [1, 2]. Among these standards, ISA100.11 was developed most recently and use open standard from physical layer to transport layer.

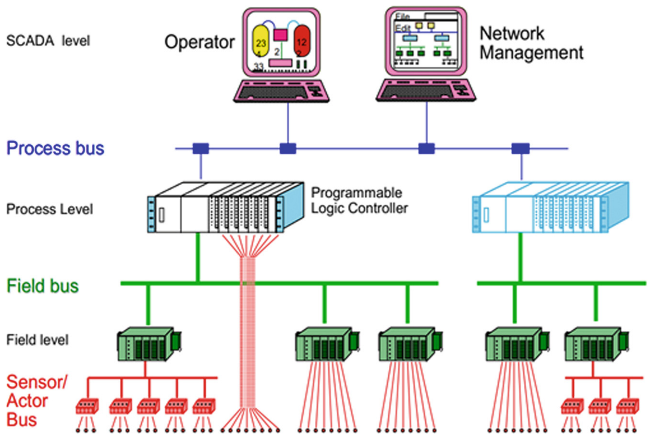

Fig. 1. Location of the field bus in the plant hierarchy [3]

ISA100.11a is a wireless communication network standard issued by the International Society of Automation (ISA), a non-profit organization in the U.S., in order to overcome the disadvantage of the wire communication protocol in the existing ICS. Reliability, security, robustness, quality, interoperability, existing system, compatibility and large network support were considered requirements, and the main characteristics include low power/low speed wireless network use, compatibility with other communication standards, open standard and IPv6 support. In 2009, ISA100.11a was officially announced, and it was approved as IEC 62734 Standard at the International Electrotechnical Commission (IEC) in 2011. The network components of ISA100.11a include adapter, gateway, network manager, security manager, handheld and field device, and it can perform communication by the composition (See Fig. 2).

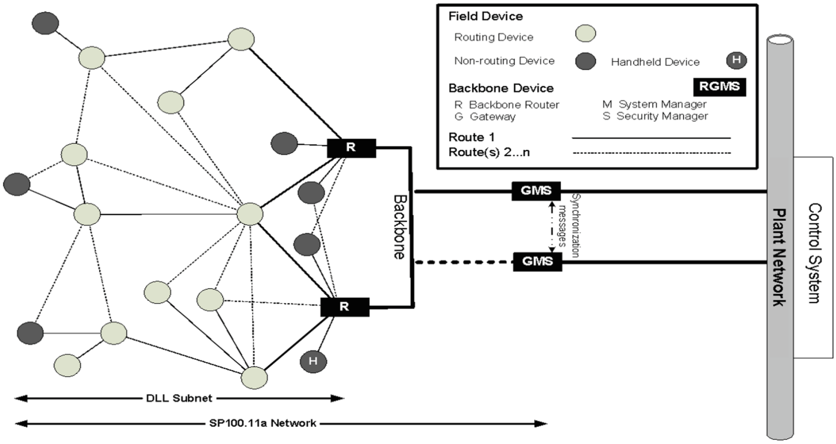

Fig. 2. ISA100.11a network configuration [4]

The ISA100.11a assurance test is conducted by ISA and two tests can be performed. The first test is stack test that ensures ISA100 wireless stack conformance prior to device interoperability testing and second test is device test that ensures ISA100 wireless device interoperability in native mode. In order to conduct two tests of Device Under Test (DUT), a gateway and system manager can be provided, which constitutes an ISA100.11a network, and an official test tool kit certified by ISA100 WCI is used. The entire test process is performed according to the ISA100 wireless communication specification. The products that have conformance and interoperability with ISA100.11a obtain a certificate. Like this, the assurance of ISA100.11a turned out to be the first step which is mostly formed by the tests on protocol stack and interoperability, and tests on stack and interoperability are performed on 6LoWPAN, one of the main referenced standards. Therefore, in order to assure the security of the ICS that uses ISA100.11a, it is necessary to draw additional security requirements and propose a security framework.

Some studies are conducted about the framework and methodology of a security vulnerability study and security test of the main protocols of ISA100.11a, 6LoWPAN and IPv6 and apply the result to the security assurance framework of this study. Studies analyzing the security vulnerability of 6LoWPAN include Le [5] and Redwan [6]. Anhtuan Le analyzed security threats that might occur in a 6LoWPAN network environment and suggested security countermeasures based on Intrusion Detection System (IDS). The study examined investigated OSI 7layers security threat in the existing WSN environment and security vulnerability that might occur in a known 6LoWPAN network and designed an IDS that could respond to a Quality of Service (QoS) attack abusing the vulnerabilities. Hassen Redwan proposed an end-to-end authentication protocol to detect a fragmentation attack method possible on a 6LoWPAN network and defend the attack. The security vulnerability of 6LoWPAN drawn from the studies is based on the wireless communication vulnerability generally known, which attacks on the integrity, availability and confidentiality of a network from eavesdropping, intercepting and manipulating packets.

The representative standard documents and guideline documents related to the methodology and evaluation of security testing include of NIST SP 800-42, SP 800-53A and SP 800-115, ISECOM OSSTMM, OISSG ISSAF and OWASP Group Testing Guide v5. These documents specify that security should be evaluated through a test, examination and interview and suggest that each method should be performed through the steps such as plan, execution and post-execution. This study proposed penetration testing related to test and examination and a security authentication framework that evaluates security through examination and analysis of the objects or functions of the target.

3 Proposed Security Frameworks

3.1 Overview of Proposed Security Framework

Similar to the Achilles certification and ISASecure certification program, which give certification about embedded device by testing procedure, this section proposed security assurance framework for device of industrial control system based on ISA100.11a protocol. This security assurance framework consists of two main categories. One is communication test; the other is security function test. All devices that use to ISA100.11a protocol must be satisfied with same communication test, but components of ISA100.11a network, such as field device, router and host, are satisfied with different number of security functions. Communication test is specific test about ISA100.11a communication and focus on transport and network protocol layer in ISA100.11a protocol. It is helpful to test other protocols that are based on these layers and to apply common test item to various component devices of ISA100.11a network (See Fig. 3).

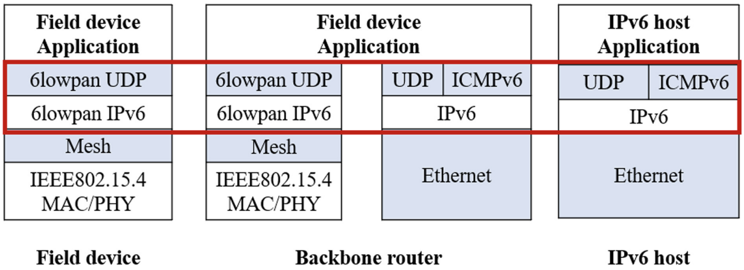

Fig. 3. Protocol stack of network component ISA

Security function test is assurance procedure to assess whether ISA100.11a devices are satisfied with requirement of security functions. As each component of ISA100.11a network, such as field device, router and host, have different purpose and H/W specification, different number of requirements are suggested for each component. Organization of proposed security assurance framework are shown in the following Fig. 4.

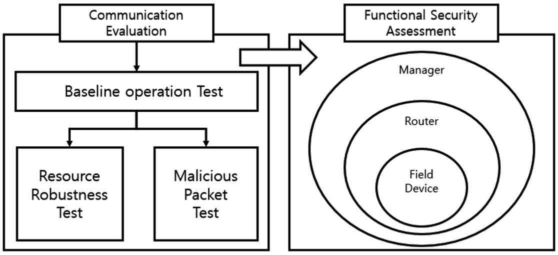

Fig. 4. Proposed security framework

3.2 Communication Test

Communication test is consisting of three test components: baseline operation test, resource robustness test, packet manipulation test. These tests are focused on network layer and transport layer of ISA100.11a communication protocol and are confirmed about maintaining normal operation of target device during test procedure. If the target device occurs following abnormal operation, it means that target device is not satisfied with related test item.

- **Program instability:** program crash or restart when test is being executed.
- **Suspension of network operation:** deny response of application program when test is being executed.
- **Abnormal exhaustion of resource:** occur abnormal CPU availability or memory leak when test is being executed.

Baseline Operation Test

Baseline operation test is basic test of packet creation and processing that is based on transport layer and network layer of ISA100.11a communication protocol. Similar to following Fig. 5, this test is focused on packet compression and fragmentation according to RFC 6282 and ISA100.11a-2010 standard documents. Derived items of baseline operation test are referred to ETST Plugtest document and draft document of Interoperability of 6LoWPAN issued by IETF.

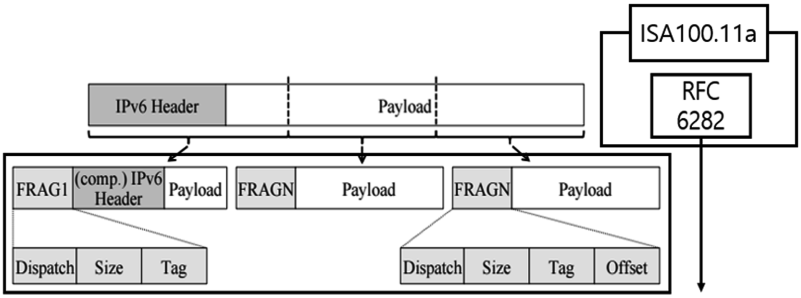

Fig. 5. Scope of baseline operation test and reference standards

Resource Robustness Test

Resource robustness test perform consumption of specific resources in target device and evaluate processing and protection capability of target device under transmission of high speed and flooding packet. This test evaluates that existing communication connection is continuously operating within the time limit. So that it assurance that target device is maintaining essential service under exhaust resource attack. Derived items of resource robustness test are referred to level 1 of Archilles communication certification that is assurance of resource robustness and are transformed into suitable ISA100.11a.

Packet Manipulation Test

Packet manipulation test evaluate processing and protection capability of target device by creating and transmitting of abnormal packet, such as non-conformed standard packet, invalid value packet, invalid sequence packet and known attack packet. This test can use fuzzing methodology (Blackbox test) and manual methodology (Whitebox test) for generating and transferring attack packet. Target device not only does not become program instability, suspension of network operation and abnormal exhaustion of resource but also executes protection action under packet manipulation test. Derived items of packet manipulation test are referred to IEC 62443 and RFC standard.

3.3 Security Function Testing

Security Function testing confirm operating and implementing of security functions for maintaining and operating target device. This test assures target device by checking function name or command of OS. Security Function testing are needed to propose appropriate requirement of security function depending on different hardware specifications and roles of device. This study divides devices of ISA100.11a network into three components: a field device, backbone router, and host. And then, it proposes three different evaluation items of security function for each component. For example, a field device is satisfied with assurance level 1 and backbone router is satisfied with assurance level 1 & 2 and host is satisfied with assurance level 1 & 2 & 3. Derived items of Security Function testing are referred to NIST SP800-53, NIST SP 800-52, NERC CIP, PP (Protection profile) for WLAN access systems/client and PP profile of an industrial wireless base-station. And then, these items are adopted about different level of assurance method in IEC 62443-4-2.

4 Measurement and Evaluation Method

Specifying evaluation method and environment about proposed items is important methodology for proving objectivity, consistency, validity and reliability in assurance program. Furthermore, this can be useful to use self-testing for finding and making up for security vulnerability in target device and to improve overall security level about related device. This section specifies method of evaluation and measurement about proposed security assurance framework and then experiment with testbed that is able to apply ISA100.11a network.

4.1 Measurement Method for Communication and Security Function Test

The ISA100.11a protocol is based on IEEE 802.15.4 standard in the physical layer and data link layer, but it defines IEEE 802.15.4 expanded for channel hopping and mesh network in the data link layer. In the network and transport layers, it uses open standard, 6LoWPAN connected to the UDP and IPv6 standard. Therefore, communication testing method and configuration are based on RFC standard document.

Baseline Operation Test

Baseline operation test is conformed about generating and processing 6LoWPAN complying with RFC standard and about derived items by analyzing response packet for transferred echo packet to target device. Configuration and process of baseline operation test is shown in Fig. 6.

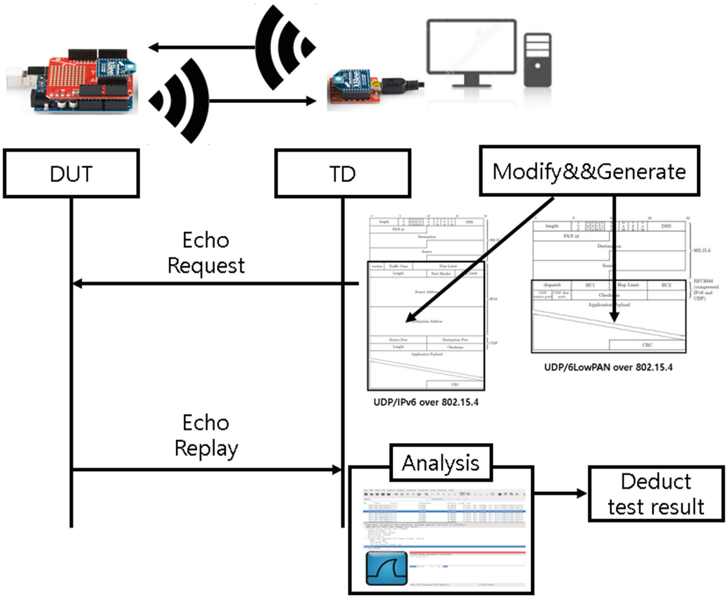

Fig. 6. Configuration and process of baseline operation test

Resource Robustness Test

Resource robustness test is exhausting specific resource of target device by transferring flood packets and evaluating capability of processing and protecting about target device. The test is checked about time interval of existing communication connection and is monitored about operation status of target device under the test. Configuration and process of resource robustness test is shown in Fig. 7.

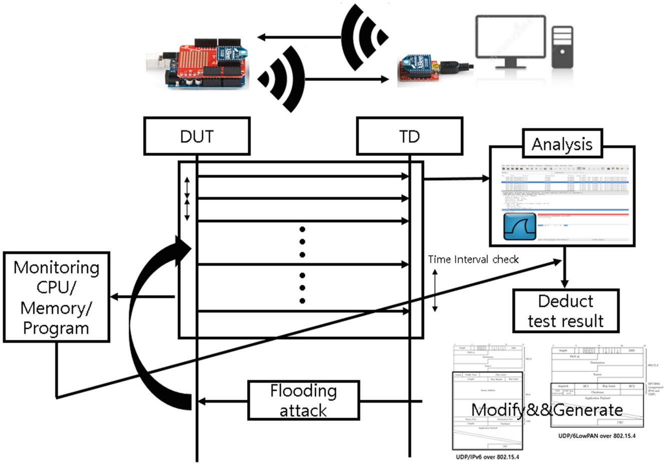

Fig. 7. Configuration and process of resource robustness test

Packet Manipulation Test

The test is checked about capability of processing and protecting in target device by transferring non-conformed standard packet, invalid value packet, invalid sequence packet and known attack packet. Configuration and process of packet manipulation test is shown in blow Fig. 8.

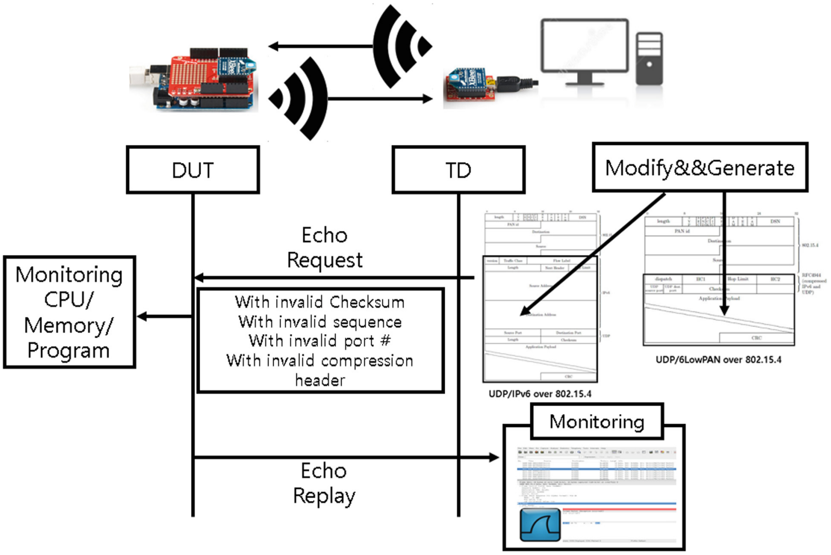

Fig. 8. Configuration and process of packet manipulation test.

Security Function Test

Security Function testing confirm operating and implementing of security functions for maintaining and operating target device. This test assures target device by checking function name or command of OS. However, same security function has various function name or command according to target OS. So, the following Table 1 briefly guides example checklist about security function test.

Table 1. Example checklist of security function test

Checklist of security function			
Role-based access	User password management	System use notification	Audit record generation
Dual authentication access	Monitor unsuccessful login attempt	Local session locking timeout	Audit record time-stamp
Least privilege default access	Record successful login	Remote session termination timeout	Non-repudiation of audit record

(*continued*)

Table 1. (*continued*)

Checklist of security function			
Administrator role	Previous login notification	Monitoring unauthorized connection	Additional content of audit record
Administrator access support	Password modification notification	Disable wireless networking	Audit fault warning
Write protection	Password strength enforcement	Basic device authentication	Basic protection of audit record
Basic protection of executable code	Unsuccessful login attempt	Session creation	Cryptographic protection of audit record
Crypto protection of executable code	Password minimum strength	Basic protection of session	Audit record of system area
Basic protection of OS	Password encryption	Cryptographic protection of session	maintenance of essential service
Crypto protection of OS	Encrypted password protection	Session termination	Backup system support
Security function verification	Basic confidentiality of system data	Session timeout	Recovery system support
Security function isolation	Cryptographic mechanism	Information flow enforcement	Incident response support

4.2 Experiment Methodology of Proposed Framework

For experiment of proposed security assurance framework, it was configured to a network environment where the standard ISA100.11a can work network environment. By using arduino Arduino XBee Artenna series 1 (802.15.4 1 mW) and arduino uno R3 board (Fig. 9).

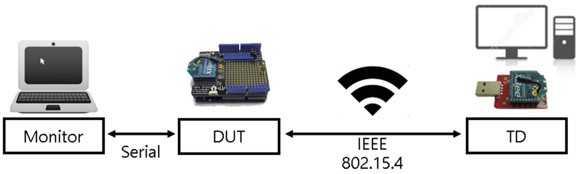

Fig. 9. Experimental configuration of proposed framework

And then for configuration of UDP/6LoWPAN stack on this H/W components, it was used to pIPv6 source code, which implement UDP/6LoWPAN for arduino uno based on Contiki OS [7, 8] (Fig. 10).

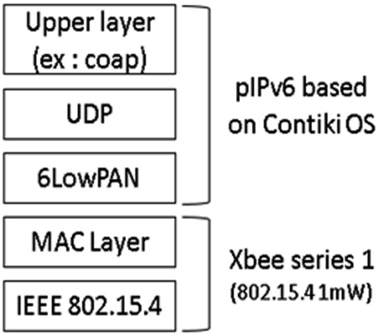

Fig. 10. Experimental configuration of protocol stack

5 Conclusion

ISA100.11a, one of the main wireless communication protocols in industrial environment, has high scalability, reliability, security, robustness, quality, interoperability, compatibility of existing system and large network support. Therefore, it is actively researching and applying in industry site. Due to wireless communication system characteristic using ICT based on main infrastructure, it is necessary to security technology and security assurance program about cybersecurity threats. However, there are lacking studies to test and evaluate the security of the wireless communication technology for ICS. Therefore, this study proposed a security assurance technology of the devices focusing on ISA100.11a, one of the wireless communication protocols for ICS. The proposed security assurance technology was divided broadly into communication testing and security function assessment, and the communication testing was divided into baseline operation testing, resource robustness testing, and packet manipulation testing. A security function assessment conducted with the devices that have passed communication testing was proposed differing the required items, divided by the components of ISA100.11a, such as a field device, backbone router, and host so that an assessment appropriate for the hardware specifications and roles of each component is achieved. In addition, this study seeks to facilitate the implementation and application of the proposed security assurance technology by proposing concrete methods or criteria for communication testing and security function assessment.

Acknowledgments

- This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2018-2016-0-00304) supervised by the IITP (Institute for Information & communications Technology Promotion).

- This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2018R1D1A1B07043349).

- This work was supported by an IITP grant funded by the Korean government (MSIT) (No. 2018-0-00336, Advanced Manufacturing Process Anomaly Detection to prevent the Smart Factory Operation Failure by Cyber Attacks).

References

1. Lennvall, T., Svensson, S., Hekland, F.: A comparison of WirelessHART and ZigBee for industrial applications. In: IEEE International Workshop on Factory Communication Systems (WFCS 2008) (2008)
2. Nixon, M., Round Rock, T.X.: A comparison of WirelessHART and ISA100.11a. Whitepaper, Emerson Process Management, pp. 1–36 (2012)
3. Kirrman, H.: Industrial communication systems-field bus: principles. https://web.fe.up.pt/~asousa/sind/acetat/AI_EPFL/AI_3xx_Field_bus_OSI_MVB.pdf. Accessed 17 Oct 2018
4. Analysis of wireless industrial automation standards: ISA-100.11a and WirelessHART. https://www.isa.org/standards-publications/isa-publications/intech-magazine/2012/december/web-exclusive-analysis-wireless-industrial-automation-standards-isa-100-11a-wirelesshart/. Accessed 17 Oct 2018
5. Le, A., Loo, J., Lasebae, A., Aiash, M., Luo, Y.: 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. Int. J. Commun. Syst. **25**(9), 1189–1212 (2012)
6. Redwan, H., et al.: SAKES: secure authentication and key establishment scheme for M2M communication in the IP-based wireless sensor network (6L0WPAN). In: 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE (2013)
7. A small CoAP implementation for microcontroller. https://github.com/1248/microcoap. Accessed 17 Oct 2018
8. Arduino pico IPv6 stack. https://github.com/telecombretagne/Arduino-pIPv6Stack. Accessed 17 Oct 2018