Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.4, Aug. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.4.757

산업용 무선통신기기 사이버 보안위협 및 보안요구사항에 관한 연구

이 지 섭,[1†] 박 경 미,[2] 김 신 규[3‡]
[1,2,3]ETRI 부설연구소(연구원, 선임연구원, 팀장)

A Study on Cyber Security Threat and Security Requirements for Industrial Wireless Communication Devices

Jiseop Lee,[1†] Kyungmi Park,[2] Sinkyu Kim[3‡]
[1,2,3]The Affiliated Institute of ETRI(Researcher, Senior Researcher, Team Leader)

요 약

산업제어시스템(ICS)은 분산된 다양한 자산을 측정, 감시, 제어하는 시스템으로 에너지, 화학, 교통, 수처리, 제조 공장 등의 산업 시설 및 국가기반시설에서 사용된다. 산업제어시스템의 특성상 보안위협에 노출되면 오동작, 중단 등으로 인해 막대한 인명, 자산 피해 등이 발생할 수 있어 산업제어시스템의 보안위협을 예방하고 최소화하기 위한 연구가 필요하다. 기존의 산업제어시스템의 경우 보안위협을 고려하여 무선통신기기의 사용을 제한하였으나 최근에는 유지보수의 용이성 및 비용의 장점으로 인해 산업용 무선통신기기 도입이 점차 증가하고 있다. 이에 본 논문에서는 WirelessHART와 ISA100.11a를 지원하는 산업용 무선통신기기의 보안위협을 분석하고, 분석 결과를 기반으로 산업용 무선통신기기의 도입 및 운영에 필요한 보안요구사항을 제시하였다. 본 연구에서 제시한 보안요구사항을 활용하여 국가기반시설을 포함한 다양한 산업분야의 산업용 무선통신환경 구축 시 보안위협을 완화할 수 있을 것으로 기대한다.

ABSTRACT

Industrial Control System(ICS) is a system that measures, monitors, and controls various distributed assets, and is used in industrial facilities such as energy, chemical, transportation, water treatment, and manufacturing plants or critial infrastructure. Because ICS system errors and interruptions can cause serious problem and asset damage, research on prevention and minimization of security threats in industrial control systems has been carried out. Previously wireless communication was applied in limited fields to minimize security risks, but the demand for industrial wireless communication devices is increasing due to ease of maintenance and cost advantages. In this paper, we analyzed the security threats of industrial wireless communication devices supporting WirelessHART and ISA100.11a. Based on the analysis results, we proposed the security requirements for adopting and operating industrial wireless communication devices. We expect that the proposed requirements can mitigate security threats of industrial wireless devices in ICS.

Keywords: Industrial Control System, WirelessHART, ISA100.11a

Received(06. 15. 2020), Modified(07. 21. 2020), Accepted(07. 21. 2020)

† 주저자, shayete@nsr.re.kr
‡ 교신저자, skkim@nsr.re.kr(Corresponding author)

I. 서 론

산업제어시스템(ICS, Industrial Control System)은 분산된 다양한 자산을 측정, 감시, 제어하는 시스템으로 에너지, 화학, 교통, 수처리, 제조 공장 등의 산업 시설에서 사용된다. 기존의 산업제어시스템은 일반적으로 외부망과 분리된 폐쇄적인 환경에서 운영되었으며[1], 기기 간의 통신을 위해 전용 산업용 통신 프로토콜을 사용 중이다. 또한 최근에는 초고속 무선 통신 기술의 발달로 인해, 산업제어시스템 내에서 위험하거나 장비설치가 어려운 지역에 유지보수가 용이하고 비용이 저렴한 산업용 무선통신기기 사용이 전 세계적으로 증가하는 추세이다. 국내 기반시설의 경우, 현재 무선통신기기의 사용률은 낮으나 해외의 산업용 무선통신기기 적용 증가 추세에 따라 무선기기 사용에 대한 필요성 및 요구가 증가하고 있다.

그러나 산업제어시스템의 특성상 보안위협에 노출되면 범용 IT 시스템과 달리 오동작, 중단 등으로 인해 거대 규모의 물리 피해가 발생할 수 있고[2], 이로 인해 막대한 인명, 자산 피해 등으로 이어질 수 있어 산업제어시스템의 보안위협 예방 및 최소화 연구의 중요성이 부각되고 있다. 또한 무선 통신 환경의 경우, 유선 환경보다 공격 표면이 넓어 더 많은 보안위협이 발생할 수 있으므로[3] 산업용 무선통신 환경의 신뢰성 및 보안성 확보가 필요하다.

이에 본 논문에서는 산업용 무선통신 중 높은 시장 점유율을 차지하고 있는 WirelessHART, ISA100.11a 표준 네트워크를 선정하여[4], 이를 지원하는 산업용 무선통신기기 전반의 보안위협을 분석하였다. 이러한 보안위협을 바탕으로 산업용 무선통신기기의 도입 및 운영에 필요한 보안요구사항을 제시하였다.

본 논문은 다음과 같이 구성된다. 1장의 서론에 이어 2장에서는 산업제어시스템의 무선 통신 보안에 관한 연구 동향을 알아본다. 3장에서는 산업제어시스템의 무선 통신 운용환경을 설명하며, 4장에서는 관련 산업용 무선통신기기의 보안위협을 식별·분석한다. 5장에서는 4장의 연구 결과를 기반으로 대응방안을 도출한 후 이를 공통평가기준(CC, Common Criteria)에 맞춘 보안요구사항으로 작성하였고, 국내 산업제어시스템의 보안 표준문서와 비교·분석하였다. 마지막으로 6장에서는 결론을 맺는다.

II. 관련 연구

기존 연구는 IEEE 802.15.4 표준에 기반한 무선 센서 네트워크(WSN, Wireless Sensor Network) 환경에서 발생할 수 있는 전반적인 보안위협을 식별하는 것에 중점을 두어 진행되었다.

Cristina Alcaraz, Javier Lopez는 무선 센서 네트워크 환경에서 발생 가능한 보안위협을 무결성(Integrity), 기밀성(Confidentiality), 가용성(Availability) 관점으로 분석하고 산업 인프라의 보안성, 안전성을 보장하도록 대응방안을 제시하였다[5]. 본 연구의 특징은 Tsao의 보안위협 분류[6]를 참고하여 메시 네트워크 기반 Zigbee Pro, WirelessHART, ISA100.11a에 발생할 수 있는 보안위협을 분석한 것이다. 그러나 Tsao의 보안위협은 잘 알려진 위협을 일부 참고하여 도출한 것으로, 무선 센서 네트워크 환경의 모든 공격 표면(Attack surface)에 대해 전반적인 위협 분석이 이루어지지 않았다.

Erwin Patermptte, Mattijs van Ommeren은 IEEE 802.15.4 표준인 WirelessHART, ISA100.11a 네트워크를 사용하는 현장장치의 조인키(Join key)가 기본 값으로 설정되어 있을 경우, 스니핑 공격에 취약할 수 있다고 강조하였다[7]. 슈퍼프레임(Superframe), 채널 호핑 주기를 계산하면 프로비저닝(Provisioning), 조인(Join) 과정의 현장장치 전송 패킷이 어느 채널로 전송되는지 확인할 수 있고, 기본 조인키를 이용하여 외부의 공격자가 게이트웨이, 현장장치 간 송·수신 패킷을 가로채어 스니핑할 수 있다는 것을 실제 시연을 통해 보여주었다. 하지만 무선통신기기의 전반적인 보안성을 고려하지 않고, 특정 취약점에 대한 완화책만 제시해주는 한계를 가지고 있다.

Duijsens는 WirelessHART 네트워크를 사용하는 현장장치에서 발생할 수 있는 보안위협을 연구하고, 테스트베드를 구축하여 취약점 공격을 일부 수행하였다[8]. 공격자의 조인키 유무에 따라 가능한 취약점 공격을 구분하여 설명하였으며, 관련 공격을 실제로 수행한 결과 총 11개의 취약점을 발견하였다. 본 연구는 실제 공격 환경과 유사한 테스트베드를 구축해 다양한 통신 공격을 수행하는 등 실제 공격을 통해 산업제어시스템의 보안위협 발생가능성을 증명한 점이 특징이다. 그러나 조인키 유무를 기준으로 보안위협을 구분하는 등 특정범위에 한정하여 취

약점 연구를 수행하였다.

IEEE 802.15.4 표준에 기반한 무선 센서 네트워크 환경의 보안 연구는 주로 게이트웨이나 현장장치의 프로비저닝, 조인 단계에서 발생할 수 있는 보안위협을 식별·분석하였다. 그 결과, 네트워크 프로토콜의 자체적인 취약점이 다수 발견되는 등 산업제어시스템에 무선 센서 네트워크 도입 시 발생 가능한 위험성이 많은 연구를 통해 증명되고 있다. 하지만 이러한 연구들은 분석가의 지식 범위 내에서 수행되고 있어 산업제어시스템 무선 네트워크 환경의 전반적인 보안성 향상을 기대하기 어렵다는 한계점이 존재한다.

산업제어시스템의 보안위협에 대응하기 위해, GE Digital의 Achilles 인증[9], TÜV SÜD의 IEC 62443 인증[10], exida의 사이버보안 인증제도[11], 프랑스의 CSPN 인증[12] 등이 운영 중이며 산업제어시스템의 가용성, 보안성을 시험 및 인증하고 있다. 국내에서도 산업제어시스템의 보안성 확보를 위해 'TTAK.KO-12.0307-part2(산업제어시스템 보안요구사항 - 제2부: 현장장치 계층)'[13]과 'KS X IEC 62443-4-2(산업제어시스템 컴포넌트의 기술적 보안요구사항)'[14] 등의 표준을 마련하여 기기의 안전성 확보 방안을 강화하고 있다.

그러나 현재의 보안요구사항 및 시험 항목은 대부분 유선 환경에 초점을 맞추고 있어 산업용 무선통신기기 도입 시 보안위협에 대한 분석 및 요구사항의 개선이 필요하다. 이에 본 논문에서는 산업용 무선통신기기의 보안위협을 체계적으로 분석하고 보안요구사항을 도출하여 기존 연구 및 시험, 인증제도의 한계점을 보완하고자 한다.

III. 산업제어시스템 무선 통신 운용환경

일반적인 산업제어시스템의 데이터 흐름은 Fig.1.과 같으며, 구성요소로는 현장장치, 제어 H/W, 제어 S/W 등이 있다. 이 중, WirelessHART, ISA 100.11a 네트워크 기술은 현장장치 계층의 센서, 액추에이터, 게이트웨이 등에 적용된다. 센서, 액추에이터는 상태를 모니터링하거나 특정한 요청에 대한 동작을 수행한 다음 그 결과를 게이트웨이로 전송하고, 게이트웨이는 전송받은 현장장치의 상태 값을 PLC 등의 제어 H/W로 전송해준다.

이 장에서는 이러한 산업용 무선통신기기의 운용환경에서 발생할 수 있는 보안위협을 분석하기에 앞서 WirelessHART, ISA100.11a 네트워크의 특징을 알아본다.

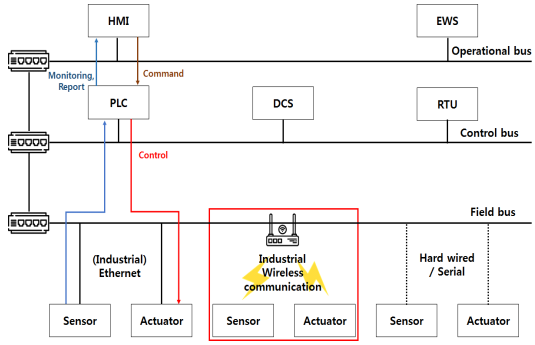

Fig. 1. Service scenario of industrial control system[15]

3.1 WirelessHART

WirelessHART는 제어시스템에서 널리 사용 중인 HART(Highway Addressable Remote Transducer) 장비를 기반으로 개발된 표준 네트워크이다. 이는 센서 및 액추에이터, 안전 샤워 장치, 상태 모니터링 장비 등 기반시설에서 사용하는 특정 제품에 대해 유연성을 제공할 목적으로 설계되었다[16]. WirelessHART 프로토콜 스택은 물리 계층, 데이터링크 계층, 네트워크 계층, 전송 계층, 응용 계층으로 구성된다. 물리 계층은 IEEE 802.15.4에 기반하여 2.4GHz 주파수 대역의 통신을 수행하며, 데이터링크 계층은 IEEE 802.15.4의 MAC에 10ms 타임 슬롯, TDMA 및 채널 호핑 기능을 제공한다. 네트워크 계층은 라우팅과 보안 기능을 제공하고, 응용 계층에서는 기존의 HART 시스템을 확장하여 사용할 수 있도록 HART 응용 계층을 제공한다. Fig.2.는 WirelessHART 프로토콜 스택 구조를 보여준다.

WirelessHART는 네트워크 환경에서 보안성을 제공하기 위해 조인 세션(Join Session), MIC(Message Integrity Code), AES-128 CCM 암호화 방식 등의 보안 기능이 포함되어 있다. 조인 세션은 기기 인증 과정으로, 현장장치가 WirelessHART 네트워크에 처음 진입할 때 수행한다. 이 때, 현장장치는 게이트웨이와 동일한 조인키가 필요한데 사용자가 올바른 조인키를 가지고 있지 않을 경우, 현장장치는 네트워크에 진입할 수 없

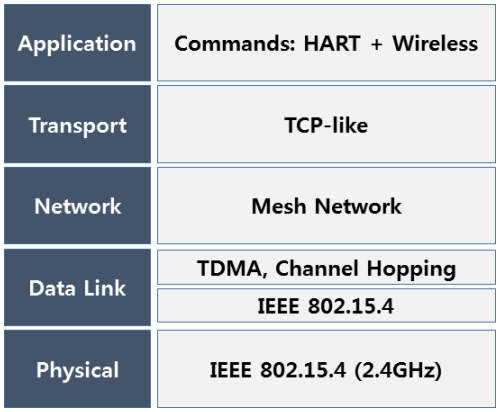

Fig. 2. WirelessHART protocol stack

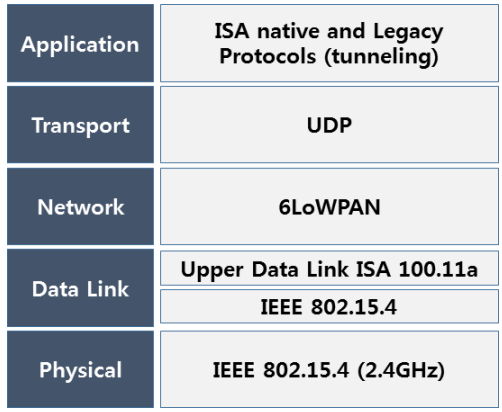

Fig. 3. ISA100.11a protocol stack

다. MIC는 데이터링크 계층, 네트워크 계층에서 계산된 후 전송 패킷에 추가되며, 데이터의 무결성을 보장해준다. AES-128 CCM 암호화 방식은 DLPDU(DataLink Protocol Data Unit), NPDU(Network Protocol Data Unit)에 무결성, 기밀성을 제공하기 위해 사용된다.

3.2 ISA100.11a

ISA100.11a는 산업 현장에서의 안정적이고 안전한 무선 통신을 제공할 목적으로 개발된 표준 네트워크이다. 이는 프로세스 자동화, 공장 자동화 및 RFID를 포함한 광범위한 무선 산업 분야 및 중요 기반시설을 지원하도록 설계되었다[16].

ISA100.11a 프로토콜 스택은 물리 계층, 데이터링크 계층, 네트워크 계층, 전송 계층, 응용 계층으로 구성된다. 물리 계층은 IEEE 802.15.4에 기반하여 2.4GHz 주파수 대역의 통신을 수행한다. 데이터링크 계층은 IEEE 802.15.4와 ISA100.11a에 특화된 Upper Data Link 기능을 구현하여 사용한다. 네트워크 계층은 6LoWPAN(IETF RFC 4944) 기술을 사용하며, 전송 계층은 UDP(IETF RFC 768)을 사용한다. 마지막으로 응용 계층은 ISA만의 프로토콜 형식을 사용한다. Fig.3.은 ISA100.11a의 프로토콜 스택 구조를 보여준다.

ISA100.11a는 조인 세션, MIC, AES-128 CCM 암호화 방식을 제공한다[17]. 조인 세션은 기기 인증 과정으로, 현장장치가 ISA100.11a 네트워크에 처음 진입할 때 동작한다. MIC는 데이터링크 계층, 전송 계층에서 각각 DMIC, TMIC로 구분하여 계산한 후 전송 패킷에 추가되며, 데이터의 무결성을 보장해준다. 그리고 AES-128 CCM 암호화 방식은 DLPDU, TPDU(Transport Protocol Data Unit)에 무결성, 기밀성을 제공하기 위해 사용된다.

IV. 산업용 무선통신 보안위협

WirelessHART, ISA100.11a를 지원하는 산업용 무선통신기기의 보안위협을 분석하기 위해 먼저 위 2가지 프로토콜을 포괄하는 기술인 무선 센서 네트워크의 알려진 모든 공격기법을 식별하였다. 다음으로, 공격 트리(Attack tree)를 이용하여 공격기법을 세분화하여 WirelessHART, ISA100.11a에 적용되는 공격을 분석하였다.

4.1 무선 센서 네트워크 공격기법

산업제어시스템의 무선 센서 네트워크는 주로 현장장치의 값 또는 상태 모니터링을 목적으로 사용된다. 그러나 무선 센서 네트워크는 자체적인 특성으로 인해 유선 네트워크보다 보안이 취약하므로[3], 알려진 위협 및 발생 가능한 위협을 식별하고 이를 보완하는 방안이 필요하다. 이에 본 연구에서는 보안위협 식별·분류를 위한 첫 단계로, 2008년부터 현재까지 알려진 보안위협을 어택 라이브러리(Attack Library)형태로 수집한 후 분석하였다. 어택 라이브러리는 논문, 컨퍼런스, 기술문서 및 취약점 데이터베이스, 표준 등 다양한 자료를 수집하여 구축할 수 있다. Table 1.은 작성한 어택 라이브러리 중 일부를 보여준다.

Table 1. Attack Library of WSN

Type	Title	Author	Year
Paper	Vulnerability Assessment of Sensor Systems[18]	Andrzej Bialas	2019
	Assessment and enforcement of wireless sensor network-based SCADA systems security[19]	Lyes Bayou	2019
Technical report	Intrinsically Secure WirelessHART Field Device Networks and the Industrial Internet of Things(IIoT)[20]	FieldComm Group	2017
	S3-17: SUTD Security Showdown[21]	iTrust, Centre for Research in Cyber Security	2017
Conference	It WISN't me, attacking industrial wireless mesh networks[7]	Erwin Paternotte and Mattijs van Ommeren	2018
Standard	IEC 62591 - Wireless communication network and communication profiles - WirelessHART, Edition. 2.0[22]	IEC	2016

분석 결과, 무선 센서 네트워크 내 공격 범위는 물리(Physical), 소프트웨어(Software), 통신(Communication)으로 구분할 수 있었다. 물리 환경에서는 공격자가 무선통신기기에 물리적으로 접근하여 노드를 부수거나 중단, 탈취하는 등의 위협이 존재한다. 소프트웨어 환경에서는 펌웨어, 애플리케이션의 취약한 코드를 악용한 위협이 존재한다. 또한 통신 환경에서는 무선통신기기의 송·수신 데이터 변조, 제거 및 악성 데이터 삽입, 혹은 라우터 네트워크의 구조적인 취약점을 악용한 위협이 존재한다.

이러한 무선 센서 네트워크의 보안위협을 공격 트리를 이용하여 세분화하였다. 공격 트리는 대상의 보안위협에 관한 공격기법을 트리 형태로 체계화한 방법으로, 상위 노드와 하위 노드로 구성된다. 공격 방법 또는 공격 목표를 상위 노드로 작성하고, 이를 달성하기 위한 세부 공격 방법을 하위 노드로 작성한다. Fig.4.는 무선 센서 네트워크의 알려진 공격기법 41개를 식별한 결과를 보여주며, 최상단 노드인 상위 노드는 각각 물리 공격, 소프트웨어 공격, 통신 공격으로 구분하였다. 하위 노드는 무선 센서 네트워크와 관련한 다수의 논문, 기술문서를 참고하여 분류하였으며, 최하위 노드는 구축한 어택 라이브러리의 모든 공격 기법 및 보안전문가의 의견을 참조하여 작성하였다.

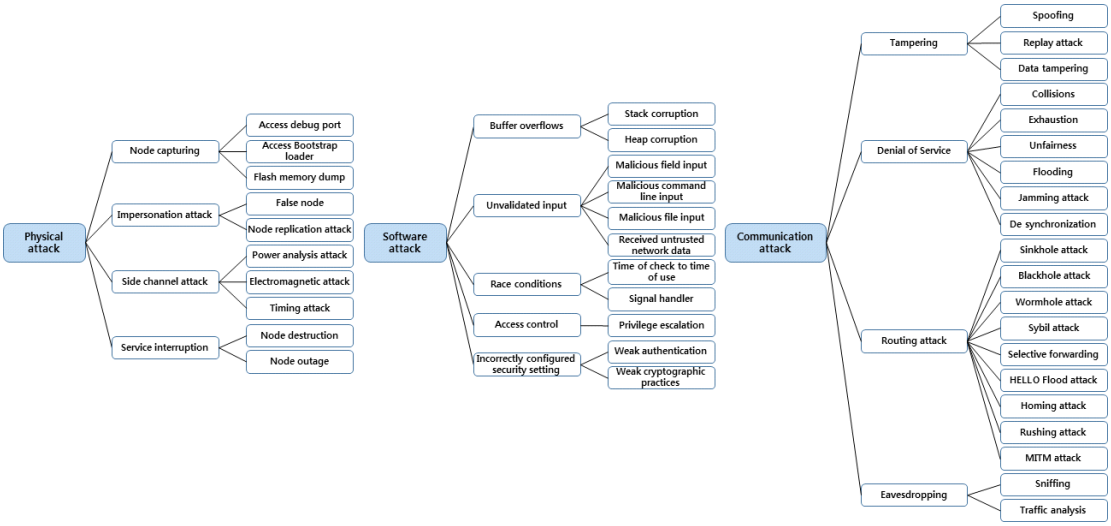

Fig. 4. Attack tree of WSN

4.2 산업용 무선통신기기 공격 기법

WirelessHART, ISA100.11a는 기기 인증을 위한 조인 세션과 무결성 검증을 위한 MIC, 패킷 무결성, 기밀성 보장을 위한 AES-128 CCM 암호화 방식 등 3가지의 보안 기능을 지원한다. 이를 고려하여 무선 센서 네트워크 공격기법 중 산업용 무선통신기기에 적용 가능한 공격기법을 분석하였다.

분석 결과, 2가지의 물리 공격기법, 15가지의 통신 공격기법을 완화할 수 있으나, 무선 네트워크 프로토콜의 보안 기능 특성상 대부분의 물리, 소프트웨어 공격에 대응하기 어려울 것으로 예상된다. 또한 통신 공격 중에서도 기술적으로 대응이 어려운 공격이 존재한다.

4.2.1 물리 공격

물리 공격은 노드 탈취(Node capturing), 위장 공격(Impersonation attack), 부채널 공격(Side channel attack), 서비스 중단(Service interruption)으로 분류되고 하위 10가지 공격이 존재한다. 이 중, 노드 탈취, 부채널 공격, 서비스 거부 공격은 공격자가 대상 기기에 물리적으로 접근하여 공격하는 방법이므로, 기술적으로 공격 위협을 완화하기 어렵다. 따라서 위 3가지 공격 분류 내의 8가지 하위 공격기법은 산업용 무선통신기기에 발생 가능하다.

그러나 위장 공격은 공격자가 임의로 제작한 노드를 정상 노드인 것처럼 위장하는 것으로, 공격자 노드를 사전에 무선 센서 네트워크에 연결해야 공격이 가능하다. WirelessHART, ISA100.11a 네트워크는 조인 세션을 통해 기기 인증을 수행하므로, 해당 네트워크를 지원하는 산업용 무선통신기기는 조인키가 유출되지 않을 경우 위장 공격으로부터 안전하다.

Table 2. Physical attack of Industrial wireless network

Physical attack method			Security features	
			Wireless HART	ISA100.11a
Node capturing	P1	Access debug port	X	X
	P2	Access bootstrap loader	X	X
Impersonation attack	P3	Flash memory dump	X	X
	P4	False node	Join	Join
	P5	Node replication attack	Join	Join
Side channel attack	P6	Power analysis attack	X	X
	P7	Electromagnetic attack	X	X
	P8	Timing attack	X	X
Service interruption	P9	Node destruction	X	X
	P10	Node outage	X	X

4.2.2 소프트웨어 공격

소프트웨어 공격은 버퍼 오버플로우(Buffer overflow), 미검증 입력값(Unvalidated input), 경쟁 상태(Race condition), 접근 제어(Access control), 잘못된 보안 기능 설정(Incorrectly configured security setting)으로 분류되고 하위 11가지 공격이 존재한다.

대부분의 소프트웨어 취약점은 개발자의 실수 혹은 논리적 오류, 기술적으로 정립이 안 된 알고리즘의 사용으로 인해 발생하므로, 이에 대한 고려 없이 소프트웨어를 개발하는 경우 11가지 소프트웨어 공격에 취약할 수 있다.

Table 3. Software attack of Industrial wireless network

Software attack method			Security features	
			Wireless HART	ISA100.11a
Buffer overflow	S1	Stack corruption	X	X
	S2	Heap corruption	X	X
Unvalidated input	S3	Malicious field input	X	X
	S4	Malicious command line input	X	X
	S5	Malicious file	X	X

Software attack method			Security features	
			Wireless HART	ISA100. 11a
		input		
	S6	Received untrusted network data	X	X
Race condition	S7	Time of check to time of use	X	X
	S8	Signal handler	X	X
Access control	S9	Privilege escalation	X	X
Incorrectly configured security setting	S10	Weak authentication	X	X
	S11	Weak cryptographic practices	X	X

4.2.3 통신 공격

통신 공격은 변조(Tampering), 서비스 거부 공격(Denial of service), 라우팅 공격(Routing attack), 도청(Eavesdropping)으로 분류되고 하위 20가지 공격이 존재한다. 이 중, 자원 고갈, 재밍, 호밍, 스니핑, 트래픽 분석 공격을 제외한 15가지 공격은 Table 4.와 같이 산업용 무선프로토콜에서 제공하는 보안 기능을 활용하여 예방, 차단할 수 있다.

자원 고갈, 재밍 공격은 주기적으로 데이터를 전송하여 배터리를 빠르게 소모시키거나 특정 통신 채널·주파수를 사용하지 못하게 하는 등 산업용 무선통신기기의 정상 동작을 방해하는 공격으로 기기의 보안 기능으로는 대응할 수 없다. 또한 호밍, 스니핑, 트래픽 분석 공격은 암호화가 적용되지 않은 패킷 영역을 도청하여 분석하고 공격할 수 있어 대응에 한계가 존재한다.

WirelessHART, ISA100.11a는 보안 기능을 이용하여 다수의 통신 공격을 차단하는 것이 특징이다. 특히 기기 간 인증 과정인 조인 세션을 통해 외부의 인가되지 않은 접근을 허용하지 않는다. 그러나 조인 세션 등의 보안 기능에 의존하는 만큼 안전한 키 관리방안을 고려해야 한다. 관련한 보안위협의 예로, 제조사가 제공하는 디폴트 조인키를 그대로 사용하거나 유추하기 쉽게 조인키를 구성한 경우, 공격자가 조인키를 획득하여 동일 네트워크에 쉽게 접근할 수 있다.

Table 4. Communication attack of Industrial wireless network

Communication attack method			Security features	
			Wireless HART	ISA100. 11a
Tampering	C1	Spoofing	MIC	MIC
	C2	Replay attack	Join, MIC	Join, MIC
	C3	Data tampering	Join, MIC	Join, MIC
Denial of Service	C4	Collisions	Backoff timer	Backoff timer
	C5	Exhaustion	X	X
	C6	Unfairness	Join	Join
	C7	Flooding	Join	Join
	C8	Jamming attack	X	X
	C9	De synchronization	MIC	MIC
Routing attack	C10	Sinkhole attack	Join, MIC	Join, MIC
	C11	Blackhole attack	Join	Join
	C12	Wormhole attack	Join	Join
	C13	Sybil attack	Join	Join
	C14	Selective forwarding	Join	Join
	C15	HELLO Flood attack	Join	Join
	C16	Homing attack	X	X
	C17	Rushing attack	Join	Join
	C18	MITM attack	Join, MIC	Join, MIC
Eavesdropping	C19	Sniffing	X	X
	C20	Traffic analysis	X	X

V. 산업용 무선통신기기 보안요구사항

4장에서는 무선 네트워크인 WirelessHART, ISA100.11a를 지원하는 산업 무선통신기기 제품 전반의 보안위협을 도출하였다. 이 장에서는 산업용 무선통신기기를 국내 산업제어시스템에 도입하는 경우 보안위협에 대응하기 위한 보안요구사항을 제안하고, 국내 산업제어시스템 보안 표준문서인 'TTAK.KO-12.0307-part2'[13], 'KS X IEC 62443-4-2'[14]와 비교·분석하였다.

5.1 보안요구사항 도출

제안한 보안요구사항 도출 과정은 Fig.5.와 같다. 4장의 산업용 무선통신기기 공격기법을 고려하여 대응방안을 도출한 다음, NIST의 산업제어시스템 보호 프로파일[23], 현장장치 보호 프로파일[24]을 활용하여 공통평가기준(CC)[25]을 반영한 보안요구사항을 작성하였다. NIST의 산업제어시스템 관련 보호 프로파일 문서는 유선 네트워크 환경에서의 보안에 중점을 두고 있어 CC의 보안기능 컴포넌트 문서의 무선 네트워크 보안과 관련한 항목을 참고하여 작성하였다.

그 결과, Table 5.와 같이 총 64개의 산업용 무선통신기기 보안요구사항을 도출하였다. 도출한 보안요구사항은 보안감사(FAU, Security audit), 통신(FCO, Communication), 암호 지원(FCS, Cryptographic support), 사용자 데이터 보호(FDP, User data protection), 식별 및 인증(FIA, Identification & Authentication), 보안관리(FMT, Security management), TSF 보호(FPT, Protection of the TSF(TOE Security Functionality)), 자원 활용(FRU, Resource utilisation), 자원 접근(FTA, TOE(Target of Evaluation) access), 안전한 경로/채널(FTP, Trusted path/channel) 등의 클래스로 구성된다.

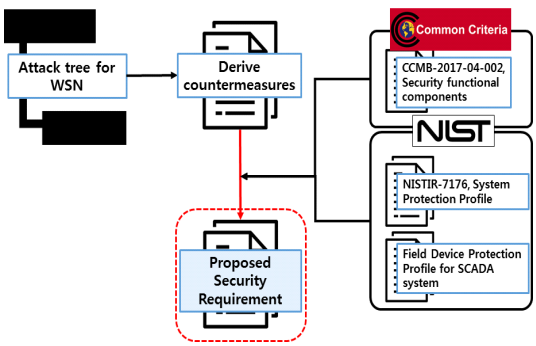

Fig. 5. Deriving proposed security requirements

Table 5. Proposed security requirements components

Class	Components	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.2	Guarantees of audit data availability
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCO	FCO_NRO.1	Selective proof of origin
	FCO_NRR.1	Selective proof of receipt
FCS	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic Operation
FDP	FDP_ACC.1	Subset access control
	FDP_ACC.2	Complete access control
	FDP_DAU.1	Basic data authentication
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ROL.1	Basic rollback
	FDP_SDI.1	Stored data integrity monitoring
	FDP_UCT.1	Basic data exchange confidentiality
	FDP_UIT.1	Data exchange integrity
FIA	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	TSF generation of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.3	Unforgeable authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
FMT	FMT_MOF.1	Management of security

		functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_REV.1	Revocation
	FMT_SAE.1	Time-limited authorization
	FMT_SMR.1	Security roles
FPT	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITA.1	Inter-TSF availability within availability metric
	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_PHP.2	Notification of physical attack
	FPT_RCV.2	Automated recovery
	FPT_RPL.1	Replay detection
	FPT_SSP.1	Simple trusted acknowledgement
	FPT_SSP.2	Mutual trusted acknowledgement
	FPT_STM.1	Reliable time stamps
	FPT_TDC.1	Inter-TSF basic TSF data consistency
FRU	FRU_FLT.1	Degraded fault tolerant
	FRU_PRS.1	Limited priority of service
	FRU_RSA.1	Maximum quotas
FTA	FTA_MCS.1	Basic limitation on multiple concurrent sessions
	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.3	TSF-initiated termination
	FTA_TAH.1	TOE access history
	FTA_TSE.1	TOE session establishment
FTP	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

5.2 국내 표준문서와 제안사항 비교·분석

제안한 보안요구사항의 검증을 위해 국내에서 공개된 산업용 현장장치 보안성 평가 표준을 선정하여 비교·분석을 수행하였다.

Table 6. The relationship between security requirements and attack threats

Type	Threat	TTAK.KO-12.0307-part2	KS X IEC 62443-4-2	Suggestion
Physical	P1	O	O	O
	P2	O	O	O
	P3	O	O	O
	P4	O	O	O
	P5	O	O	O
	P6	O	O	O
	P7	O	O	O
	P8	O	O	O
	P9	X	X	X
	P10	X	X	X
Software	S1	△	X	X
	S2	△	X	X
	S3	△	X	X
	S4	△	X	X
	S5	O	O	O
	S6	O	O	O
	S7	X	X	X
	S8	X	X	X
	S9	X	X	X
	S10	O	O	O
	S11	O	O	O
Communication	C1	O	O	O
	C2	O	O	O
	C3	O	O	O
	C4	O	O	O
	C5	O	O	O
	C6	O	O	O
	C7	O	O	O
	C8	X	X	X
	C9	O	O	O
	C10	O	O	O
	C11	O	O	O
	C12	O	O	O
	C13	O	O	O
	C14	O	O	O
	C15	O	O	O
	C16	X	X	O
	C17	O	O	O
	C18	O	O	O
	C19	O	O	O
	C20	X	X	O

Table 6.은 기존의 국내 표준문서 및 본 논문에서 제안한 보안요구사항과 산업용 무선통신기기 보안위협 대응 관계를 비교·분석한 결과이다.

분석 결과, 물리 공격에 대해서는 기존의 표준 및 제안한 요구사항 모두에서 동일한 위협 대응 결과를 보이는 것으로 확인되었다. 보안요구사항에서 권고한 최소 요구사항을 만족한다면 공격자가 물리적으로 접근하여 노드를 탈취(P1, P2, P3)하거나, 위장 노드(P4, P5) 설치, 부채널 공격(P6, P7, P8)을 수행하는 등의 위협을 다수 완화할 수 있다. 그러나 노드를 파괴(P9)하거나 중단(P10)하는 등의 서비스 중단은 보안요구사항으로는 대응하기 어렵다. 예를 들면 '사우디아라비아 석유시설 드론 정밀 타격'[26]등의 공격이 있으며, 향후 관련 연구를 통해 대응 방안을 마련해야 할 것이다.

소프트웨어 공격에 대해서는 기존의 표준 및 제안한 요구사항 모두에서 유사한 위협 대응 결과를 보이는 것으로 확인되었다. 악의 펌웨어 설치(S5), 신뢰할 수 없는 데이터 수신(S6), 약한 인증(S10), 약한 암호화 방식(S11)에 대해서는 보안요구사항 항목으로 대응이 가능하다. 그 외의 공격은 장치 내 잘못된 설계, 구현으로 인한 잠재적 위협으로, 시큐어 코딩[27]을 통해 위험을 최소화해야 한다.

통신 공격은 기존 표준 및 제안한 요구사항을 만족하면 공통적으로 15개의 공격 위협을 완화할 수 있으나, 재밍 공격(C8)은 대응할 수 없다. 산업용 무선프로토콜은 재밍 공격 방지를 위해 채널, 주파수 호핑 기법을 적용하고 있으나, 전 주파수 대역에 대한 연속적인 재밍에 대해서는 대응할 수 없어 차폐 가능한 환경에서 사용하지 않는 경우 대응에 한계가 존재한다.

제안한 보안요구사항은 기존의 국내 보안성 평가 표준에서 대응할 수 없었던 호밍 공격(C16), 트래픽 분석(C20)에 대한 위협완화 요구사항과, 국내 보안성 평가 표준에서 고려하지 못한 부분인 조인키 등의 비밀정보 관리를 위한 요구사항이 포함되어 있다.

호밍 공격, 트래픽 분석 완화를 위한 요구사항으로 FPT_ITC.1, FTP_ITC.1, FTP_TRP.1 컴포넌트를 추가하였다. FPT_ITC.1 컴포넌트는 현장장치와

Table 7. Comparison and analysis of security requirements standards and suggestions

	TTAK.KO-12.0307-part2		KS X IEC 62443-4-2		Suggestion	
Target	Field device with calculation and communication functions		All components of ICS		Industrial wireless gateways and wireless field devices	
Classification	• Fuzzing test • Stress test • Resource availability • Physical interface protection • Event response • Security audit • Identification and authentication • Access control • Transmission data protection • Stored data protection • Security function management • State management		• Identification and authentication control • Use control • System integrity • Data confidentiality • Restricted data flow • Timely response to events • Resource availability		• Security audit • Communication • Cryptographic support • User data protection • Access control policy • Identification and authentication • Security management • Management of functions if TSF • Protection of the TSF • Resource utilization • TOE access • Trusted path/channel	
Number of requirements	52		58		64	
Mitigate threats within the Attack tree	**Physical**	8	**Physical**	8	**Physical**	8
	Software	8	**Software**	4	**Software**	4
	Communication	17	**Communication**	17	**Communication**	19

관련된 IT 제품 간의 전송 데이터를 인가되지 않은 노출로부터 보호하도록 비밀성을 보장할 것을 요구한다. 전송 데이터는 공격에 이용될 수 있는 모든 것을 포함하며, 비밀성 제공을 위해 암호화 알고리즘, 채널·주파수 호핑 등의 적용 유무를 확인할 수 있다. FTP_ITC.1, FTP_TRP.1 컴포넌트는 사용자-현장장치 혹은 현장장치 간의 신뢰된 통신 채널/경로를 통해 안전한 식별 및 인증, 세션 연결을 지원하도록 요구한다. 이는 보증된 채널, 경로를 통해 신뢰되지 않은 장치 혹은 응용프로그램에 의한 변경이나 노출로부터 전송 데이터를 보호할 수 있다.

비밀정보 관리를 위한 요구사항으로 FIA_SOS.1, FIA_SOS.2 컴포넌트를 추가하였다. WirelessHART, ISA100.11a 네트워크에서 조인키가 디폴트로 설정되어 있거나 유추하기 쉽게 구성된 경우 공격자가 조인키를 쉽게 획득할 수 있고 이를 통해 현장장치 계층의 보안이 취약해지므로 조인키의 안전한 생성·관리가 필요하다. FIA_SOS.1, FIA_SOS.2 컴포넌트는 비밀정보의 생성·검증을 위한 보안요구사항이며 비밀정보를 특정 표준에 맞추어 생성한 후, 이를 검증하도록 요구하고 있다.

Table 7.은 기존의 산업용 현장장치 보안요구사항 표준과 제안한 보안요구사항의 특징을 비교·분석한 결과이다.

'TTAK.KO-12.0307-part2' 표준은 산업제어시스템 환경의 현장장치 계층을 대상으로 보안요구사항을 정의하였다. 현장장치 계층의 적용 대상에는 연산, 통신 기능이 적용된 센서, 액추에이터, 게이트웨이 등이 포함된다. 본 표준은 산업제어시스템의 안전한 운영·관리를 위해 네트워크 견고성, 서비스 지속성, 보안 기능 등 3개 분야별로 필요한 기능 시험을 분류하고, 이에 따른 세부 보안요구사항 52 항목을 정의하였으며, 수명주기(Life cycle)의 구축 단계에서 적용 대상의 보안성, 가용성을 평가한다.

'KS X IEC 62443-4-2' 표준은 ICS, SCADA를 포함한 모든 산업제어시스템을 대상으로 가용성, 무결성을 만족하기 위한 기술적인 보안요구사항을 정의하였다. 본 표준은 IEC 62443-1-1 문서에서 요구하는 7가지 기본 요구사항인 액세스 제어, 사용 제어, 데이터 무결성, 데이터 기밀성, 데이터 흐름 제한, 시기적절한 이벤트, 자원 가용성 등에 기반한 세부 보안요구사항 58 항목을 정의하였다.

본 논문에서 제시하는 보안요구사항은 WirelessHART, ISA100.11a 등의 무선 센서 네트워크를 지원하는 산업용 무선통신기기에 특화된 보안요구사항 64 항목을 도출하였다. 알려진 및 잠재적인 보안위협을 최소화하기 위해 적용 대상에 발생 가능한 공격 기법을 분석하였고, 이를 고려하여 공통평가기준에 맞춘 보안요구사항을 도출하였다. 정확성, 신뢰성 및 보안성 등을 갖춘 국제적으로 활용 가능한 평가 기준을 제시하였으며 국내 표준문서와 달리 산업제어시스템의 무선 통신 보안에 특화하여 향후 산업용 무선통신기기 도입 시 보안위협을 최소화할 수 있을 것이다.

VI. 결 론

본 논문에서는 현재까지 알려진 무선 센서 네트워크 환경에서 발생 가능한 보안위협 41개를 식별·분석하여 WirelessHART, ISA100.11a를 지원하는 산업제어기기에 특화된 공격 트리를 작성하였다. 또한 공격기법을 고려한 대응방안을 도출한 다음, 공통평가기준을 반영한 보안요구사항을 제시하였다.

무선 네트워크 기술이 발전함에 따라 무선 기능을 도입한 현장장치가 활발하게 개발·적용 중이며, 점차 그 적용분야가 다양해지고 있다. 따라서 국가기반시설을 포함한 모든 산업 시설에서 산업용 무선통신기기 활용 시, 본 논문에서 제시한 보안요구사항을 활용한다면 보안위협을 다수 완화할 수 있을 것으로 기대한다.

향후에는 현장관계자들의 인터뷰 및 참여를 통해 더욱 체계화된 보안위협모델이 도출되어야 한다. 그 과정에서 생성된 보안 체크리스트를 이용해 실제 산업제어시스템에 보안성 평가를 수행할 수 있어야 하며, 적용 결과를 분석하여 완성도 높은 보안성 평가 기준을 개발하는 것이 필요하다.

References

[1] Kyungmi Park, Donghoon Shin, Woonyon Kim and Sinkyu Kim, "A study on Communication Robustness Testing for Industrial Control Devices," *Journal of the Korea Institute of information Security & Cryptology*, 29(5), pp. 1099-1116, Oct. 2019

[2] "Industrial communication networks -

Network and system security - Part 1-1: Terminology, concepts and models", *IEC 62443-1-1:2009*, Jul. 2009

[3] Sunghyuck Hong, "Research on Wireless Sensor Networks Security Attack and Countermeasures: Survey", *Journal of Convergence for Information Technology*, 4(4), pp. 1-6, Dec. 2014

[4] "Industrial Wireless Sensor Network(IWSN) Market Analysis and Segment Forecasts To 2025", *Grand View Research, Inc.*, 2017

[5] Cristina Alcaraz and Javier Lopez, "A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems", *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, vol. 40, pp. 419-428, Jul. 2010

[6] T.Tsao, R. Alexander, M. Dohler, V. Daza and A. Lozano, "A Security Framework for Routing over Low Power and Lossy Networks", *Internet Engineering Task Force(IETF)*, Feb. 2009

[7] Erwin Paternotte and Mattijs van Ommeren, "It WISN't me, attacking industrial wireless mesh networks", *HITBSecConference*, 2018

[8] Lyes Bayou, David Espes, Nora Cuppens-Boulahia and Frederic Cuppens, "Security Analysis of WirelessHART Communication Scheme", *Conference of International Symposium on Foundations and Practice of Security*, Dec. 2017

[9] Feng Xie, Yong Peng, Wei Zhao, Yang Gao and Xuefeng Han, "Evaluating Industrial Control Devices Security: Standards, Technologies and Challenges", *IFIP International Conference on Computer Information Systems and Industrial Management, LNCS*, vol. 8838, pp. 624-635, 2015

[10] TUV SUD, https://www.tuev-sued-de/topics/information-technology-it/industrial-it-security

[11] exida for IEC 62443 Cyber Certification, http://www.exida.com/ Certification/IEC62443-Cyber-Cert, 2019

[12] ANSSI, Certification CSPN, https://www.ssi.gouv.fr/administration/produits-certifies/cspn

[13] "Security Requirements for Industrial Control System - Part 2: Field Device Layer", *Telecommunications Technology Association(TTA)*, Jun. 2017

[14] "Security for industrial automation and control system -Part 4-2: Technical security requirements for IACS components", *Korean Standards and Certification*, Jan. 2019

[15] "Security Requirements for Industrial Control System - Part. 1: Concepts and Reference Model", *Telecommunications Technology Association(TTA)*, Jun. 2017

[16] Mark Nixon, "A Comparison of WirelessHART and ISA100.11a", *Emerson*, Sep. 2012

[17] Stig Petersen and Simon Carlsen, "WirelessHART Versus ISA100.11a: The Format War Hits the Factory Floor", *IEEE Industrial Electronics Magazine*, vol. 5, pp. 23-34, Dec. 2011

[18] Andrzej Bialas, "Vulnerability Assessment of Sensor Systems", *Sensors*, 19(11), Jun. 2019

[19] Lyes Bayou, "Assessment and enforcement of wireless sensor network-based SCADA systems security", *Hyper Articles on Line(HAL)*, Jun. 2018

[20] "Intrinsically Secure WirelessHART Field Device Networks and the Industrial Internet of Things(IIoT)", *Fieldcomm Group*, Jun. 2017

[21] "S3-17: SUTD Security Showdown Event Report", *iTrust: Centre for Research in Cyber Security*, Nov. 2017
[22] "Wireless communication network and communication profiles - WirelessHART", *IEC 62591 Edition 2.0*, Mar. 2016
[23] "NISTIR-7176, System Protection Profile-Industrial Control Systems Version 1.0", *National Institute of Standards and Technology(NIST)*, Feb. 2004
[24] "Field Device Protection Profile for SCADA systems in Medium Robustness Environments Version 0.71", *National Institute of Standards and Technology(NIST)*, May. 2006
[25] "Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5", *The Common Criteria Recognition Agreement (CCRA)*, Apr. 2017
[26] BBC News, https://www.bbc.com/korean/international-49705340
[27] Dahye Jung, Jinyoung Choi and Songhee Lee, "Nuclear-related Software Analysis based on Secure Coding", *Journal of the Korea Institute of Information Security & Cryptology*, 23(2), pp. 243-250, Apr. 2013
[28] Woonyon Kim, Eungki Park and Sinkyu Kim, "A Study on a Cybersecurity Evaluation Method for Industrial Control Systems in the 4th Industrial Revolution Era", *The Journal of Korean Institute of Communications & Information Sciences*, 44(5), pp. 943-956, May. 2019

〈저자소개〉

이 지 섭 (Jiseop Lee) 정회원
2016년 2월: 조선대학교 컴퓨터공학부 학사
2019년 2월: 고려대학교 정보보호대학원 석사
2019년 7월~현재: ETRI 부설연구소 연구원
〈관심분야〉 기반시설보안, ICS 보안, 보안성분석평가, 취약점 분석

박 경 미 (Kyungmi Park) 정회원
2003년 2월: 한국과학기술원 전산학과 졸업
2011년 2월: 한국과학기술원 전산학과 박사
2011년 3월~2016년 8월: 삼성전자 VD사업부 책임연구원
2016년 9월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 기반시설보안, ICS 보안, 프로토콜 퍼징, 산업용 무선통신, 머신러닝

김 신 규 (Sinkyu Kim) 정회원
2000년 2월: 연세대학교 기계전자공학부 졸업
2002년 2월: 연세대학교 컴퓨터과학과 석사
2014년 2월: 연세대학교 컴퓨터과학과 박사
2003년 12월~현재: ETRI 부설연구소 책임연구원/팀장
〈관심분야〉 기반시설보안, 스마트그리드 보안, 취약점 분석, CPS 보안