Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1099

산업용 제어기기의 통신 견고성 시험 방안 연구

박 경 미,[1†] 신 동 훈,[2] 김 우 년,[1] 김 신 규[1‡]
[1]ETRI 부설연구소, [2]대구경북과학기술원

A study on Communication Robustness Testing for Industrial Control Devices

Kyungmi Park,[1†] Donghoon Shin,[2] WooNyon Kim,[1] SinKyu Kim[1‡]
[1]The Affiliated Institute of ETRI, [2]DGIST

요 약

다양한 산업 분야 및 주요 기반시설에서 사용되는 산업 제어시스템의 보안 위협에 대응하기 위해 산업용 제어기기에 대한 보안 평가 제도가 도입되어 운영되고 있다. 산업용 제어기기의 보안 평가 시험은 산업 제어시스템을 구성하는 각 구성요소별 보안요구사항을 시험하는 것으로서 기기 자체의 보안 기능에 대한 시험과 통신 견고성에 대한 시험을 포함한다. 본 논문에서는 국내·외 산업용 제어기기의 인증 시험인 EDSA, Achilles, 산업 제어시스템 보안요구사항(TTA 표준) 및 각각의 통신 견고성 시험의 특징을 분석하였다. 통신 견고성 시험은 퍼징 및 과부하 패킷을 전송하는 동안 기기의 정상동작 여부를 확인하는 것으로 기존의 시험환경 및 기준은 대부분 임베디드 장치의 특징에 초점이 맞춰져 있어 다양한 산업용 제어기기에 적용하기에는 한계점이 존재한다. 이에 본 논문에서는 산업 제어시스템에서 사용되는 제어 H/W, 제어 S/W, 현장장치, 네트워크 장비의 특성을 반영한 통신 견고성 시험환경 구축방안 및 시험 시 고려해야할 사항을 제시하였다. 향후에는 제안한 기기별 통신 견고성 시험 기준을 실제 제품에 적용할 때 발생하는 이슈사항을 확인하고 이에 대한 해결책을 제시하고자 한다.

ABSTRACT

Industrial control systems(ICS) are widely used in various industrial area and critical infrastructure. To mitigate security threats on ICS, the security assurance test for industrial control devices has been introduced and operating. The test includes testing of the security function of the device itself and testing of communication robustness. In this paper, we describe the security requirements of EDSA, Achilles, and Korea's TTA standard(security requirements for ICS). And also, we analyzed the characteristics of communication robustness test(CRT) of each certification. CRT verifies the device's operation of essential function while transmitting fuzzing and stress packets. Existing test methods are mostly focused on the embedded devices and are difficult to apply to various devices. We propose a method to test communication robustness which reflect the characteristics of control H/W, control S/W, field devices and network devices in ICS. In the future, we will apply the proposed communication robustness test to actual products and present solutions for arising issues.

Keywords: ICS, Communication robustness testing, Industrial control devices, EDSA, Achilles, Network robustness test, Fuzzing test, Stress test

Received(05. 24. 2019), Modified(1st: 08. 26. 2019, 2nd: 09. 16. 2019), Accepted(09. 17. 2019)

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

I. 서 론

산업 제어시스템은 분산되어 있는 다양한 자산을 측정, 감시, 제어를 수행하는 시스템으로 목적에 따라 SCADA(Supervisory Control And Data Acquisition), DCS(Distributed Control Systems), PLC(Programmable Logic Controller) 등으로 구성되며 에너지, 화학, 교통, 제조 등의 다양한 산업 분야 및 주요 기반시설에서 사용된다. 산업 제어시스템의 사이버 공격으로 주요 기반시설이 마비되면 국민의 생명, 환경, 재산, 국가 경제에 중대한 영향을 미칠 수 있으므로 산업 제어시스템의 보안은 가용성이 가장 중요한 요소로 고려되는 특성이 있다[1].

기존의 산업 제어시스템은 외부망과 분리된 폐쇄적인 환경에서 운용하여 사이버 공격과 위협으로부터 비교적 자유로웠으나 정보기술의 발전에 따라 상호호환성 및 효율성을 위해 Ethernet, TCP/IP 등이 적용되어 보안위협 및 취약점 발견 사례가 증가하고 있다. 최근에는 산업용 제어기기 관련 취약점이 지속적으로 발견되고 있으며 제어시스템을 대상으로 하는 사이버 공격 또한 증가하고 있는 추세이다. 특히, Stuxnet, Blackenergy, CrashOverride 등 기반시설 내 산업 제어시스템을 목표로 하는 악성코드를 활용한 공격은 막대한 사회·경제적 손실을 유발하였다. 또한, 4차 산업혁명과 더불어 등장한 스마트 팩토리, 스마트 시티는 다양한 산업 제어시스템의 요소들을 유·무선 네트워크로 연결하여 관리함으로써 제어시스템과 취약한 네트워크와의 연결 가능성이 기하급수적으로 증가하며 보안위협이 증가하고 있다[2].

이와 같은 산업 제어시스템의 보안위협에 대응하기 위해 산업 제어시스템 및 산업용 제어기기의 보안 평가를 위한 시험 및 인증 제도가 도입되었다. 산업 제어시스템의 보안 시험은 일반적으로 조직의 보안정책 및 시스템 전체의 보안요구사항에 대한 시험 항목을 포함한다. 산업용 제어기기의 보안 시험은 기기 자체의 보안기능에 대한 시험과 통신 견고성에 대한 시험으로 구성된다. 통신 견고성 시험은 다양한 산업용 제어기기의 프로토콜 구현상의 취약점과 비정상적인 트래픽에 대한 대응책을 검증하는 것을 그 목적으로 한다. 하지만, 기존의 통신 견고성 시험 기준은 대부분 임베디드 장치에 초점이 맞춰져 있어 다양한 산업용 제어기기에 적용하기 어렵다. 본 논문에서는 국내·외 산업용 제어기기의 통신 견고성 시험의 특징을 분석하고 산업용 제어기기의 특성을 고려한 기기별 통신 견고성 시험 방법 및 기준을 제시하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 기존 산업용 제어기기의 보안 인증 시험에 대해 설명하고 Ⅲ장에서는 통신 견고성 시험 방법에 대해 설명한다. Ⅳ장에서는 산업용 제어기기별 특성을 고려한 통신 견고성 시험 방안을 제안한다. 마지막으로 Ⅴ장에서는 결론을 맺는다.

II. 산업용 제어기기의 보안 인증 시험

산업용 제어기기는 산업 제어시스템을 구성하는 요소로서 현장에 설치되어 측정 및 동작을 수행하는 센서·액추에이터 등의 현장장치와 로직을 탑재하고 명령을 전달하는 PLC, RTU(Remote Terminal Unit), IED(Intelligent Electronic Devices), DCS 등의 임베디드 장치, 이를 모니터링 및 관리하기 위한 소프트웨어인 EWS(Engineering Workstation), HMI(Human Machine Interface) 등을 포함한다.

산업 제어시스템의 보안을 확보하기 위해서는 이를 구성하는 각각의 산업용 제어기기가 필요한 보안기능을 제공해야 한다. 산업용 제어기기의 보안 인증은 각 기기에 필요한 보안기능을 제시하고 이를 만족하는지를 평가하는 것이다. 산업용 제어기기의 보안 인증에서는 기기 자체가 필요한 보안 기능을 가지고 있는지 확인하는 시험과 사이버 공격에 대한 통신 견고성 시험을 수행한다.

통신 견고성 시험은 산업용 제어기기의 네트워크 프로토콜 구현이 비정상적인 패킷이나 악의적인 공격에 대응하여 얼마나 안정적으로 동작하는지를 시험한다. ISASecure의 EDSA(Embedded Device Security Assurance), GE의 Achilles 인증, 국내 산업 제어시스템 보안요구사항(TTA 표준)은 이러한 통신 견고성 시험 항목을 포함하고 있다.

2.1 ISASecure EDSA

ISASecure 인증은 산업 제어시스템과 산업용 제어기기의 보안성을 평가하기 위해 ISCI(ISA Security Compliance Institute)에서 관리하는 인증 프로그램이다. ISASecure는 임베디드 장치를 위한 EDSA, 제어시스템을 위한 SSA(System Security Assurance), 개발 라이프 사이클을 위한 SDLA(Security Development Lifecycle Assurance) 인증으로 구성된다[3].

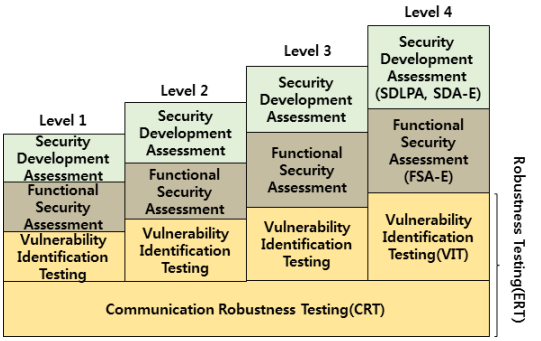


Fig. 1. Evaluation Elements for ISASecure EDSA Certification[4]

산업용 제어기기에 대한 EDSA 인증은 임베디드 장치의 보안에 중점을 두고 시험을 수행한다. EDSA 인증은 Fig. 1.과 같이 SDA(Security Development Assessment), FSA(Functional Security Assessment), ERT(Embedded device Robustness Testing)로 구성된다[4].

SDA는 개발 프로세스를 평가하는 항목이며 제조사의 개발 프로세스를 인증하는 SDLPA(Security Development Lifecycle Process Assessment)와 임베디드 장치에 적용된 개발 프로세스를 인증하는 SDA-E로 구성된다. FSA는 IEC 62443-4-2[5]와 관련된 임베디드 장치의 보안 기능을 평가한다. ERT는 알려진 취약점을 확인하는 VIT(Vulnerability Identification Testing)와 프로토콜에 대한 통신 견고성을 시험하는 CRT(Communication Robustness Testing)로 구성된다. EDSA 인증은 레벨 1~4까지 존재하며 FSA, VIT의 경우 레벨의 상승에 따라 기준이 엄격해진다. CRT 기준은 인증 레벨에 관계없이 동일하다.

2019년 3월말 기준으로 EDSA 인증제품의 수는 총 34개이며 레벨 1 인증제품은 28개, 레벨 2 인증제품은 6개이고 레벨 3 이상의 인증제품은 없다[6]. Table 1.에서 확인할 수 있듯이 EDSA 인증 제품은 DCS 컨트롤러가 가장 높은 비율을 차지한다. 제조사별 인증제품의 수는 Table 2.와 같으며 Honeywell과 Schneider Electric의 제품이 각각 전체의 44.1%, 20.6%를 차지하였다. EDSA 인증은 2011년부터 도입되었으며 2016년부터는 EDSA 2.0.0 인증이 시작되어 이후 인증 제품의 78.2%를 차지하고 있다. EDSA 2.0.0 레벨 2 인증 제품은 모두 Honeywell의 제품으로 PLC, RTU, UOC(Unit Operations Controller) 등 총 5개의 제품에 대해 인증을 받았다.

Table 1. Number of EDSA certified products by device type (Mar. 2019)

Certification / Device type	EDSA 2.0.0 Level 1	EDSA 2.0.0 Level 2	EDSA 2010.1 Level 1	EDSA 2010.1 Level 2	Total
Controller			1		1
DCS Controller	3		8		11
Field Control Processor			1		1
Field Device Controller	2				2
Fieldbus Controller			1		1
PLC		1			1
Remote Terminal Unit		1			1
Safety Control System			2		2
Safety Manager	1	1	1	1	4
Safety Related Programmable Electronic System	6		1		7
Unit Operations Controller		2			2
Wireless Device Manager	1				1
Total	13	5	15	1	34

Table 2. Number of EDSA certified products by vendor (Mar. 2019)

Certification / Vendor	EDSA 2.0.0 Level 1	EDSA 2.0.0 Level 2	EDSA 2010.1 Level 1	EDSA 2010.1 Level 2	Total
ABB			1		1
Azbil Corporation			1		1
Beijing Consen Technologies	1				1
HIMA Paul Hildebrandt GmbH	1				1
Hitachi, Ltd.			1		1
Honeywell Process Solutions	5	5	5		15
RTP Corporation				1	1
Schneider Electric	5		2		7
Toshiba infrastructure systems & solutions			1		1
Tri-Sen Systems Corporation	1				1
Yokogawa Electric Corporation			4		4
Total	13	5	15	1	34

2.2 Achilles 인증

Achilles 인증은 GE에 인수된 Wurldtech에서 개발한 산업 제어시스템의 기기에 대한 평가 기준 및 인증이다[7]. Achilles 인증은 ACC(Achilles Communications Certification), APC(Achilles Practices Certification)의 두 종류가 있다.

ACC는 통신 견고성에 대한 인증으로 임베디드 장치(PLC, DCS, RTU 등), 네트워크 장비(라우터, 스위치 등), 호스트 장비(EWS, 히스토리안 서버, 도메인 컨트롤러 등), 제어 애플리케이션(HMI, 제어 소프트웨어 등)을 대상으로 한다. ACC는 보안강도에 따라 레벨 1(L1)과 레벨 2(L2) 인증을 제공하며 레벨 2 인증은 레벨 1 인증보다 더 많은 테스트케이스와 모니터링 기준을 적용한다[8][9].

APC는 WIB 2.0에 기반하여 제조사가 제품을 개발하는데 사용된 프로세스 및 절차에 사이버 보안 모범 사례를 따르는지 인증한다. 시험 대상은 제품 자체가 아닌 사이버 보안 절차, 실무 지침, 개발, 시험, 유지관리 등 시스템 생명주기 전반에 해당한다[8][9].

Wurldtech의 기존 Achilles 인증 외에도 GE에서 ASC(Achilles System Certification) 인증을 제공하고 있다. ASC는 산업 제어시스템 공급업체가 IEC 62443-3-3 표준을 준수하였다는 것을 인증하는 프로그램으로 IEC 62443-3-3 표준과 동일하게 네 가지 보안 레벨(SL-1~SL-4)의 인증을 제공한다[10].

2019년 3월말 기준으로 ACC 인증 제품은 28개 제조사의 358개 제품이며[11] APC 인증 솔루션은 10개 제조사의 17개가 있다[12].

Table 3.과 같이 ACC 인증 제품은 L1 209개, L2 149개이며 임베디드 장치가 대다수를 차지하고 있다. L2 레벨 인증을 받은 제어 애플리케이션은 VxWorks 7 RTOS, Nucleaus RTOS, Mentor Embedded Linux의 3개이다. Table 4.는 제조사별 ACC 인증 제품의 수를 정리한 표이다. L1 인증의 경우 Sensus, GE, Invensys, Schneider 순으로 인증제품을 보유하고 있으며 이들 제조사의 제품이 전체의 74.6%를 차지한다. L2 인증은 Siemens가 전체의 67.8%를 보유하고 있으며 임베디드 장치, 네트워크 장비 및 제품군(Product Families)에 대해 인증을 획득하였다.

APC 인증 솔루션은 Bronze 14개, Silver 인증 2개가 있고 이외에 GE Digital의 Cimplicity v9.5는 IEC 62443-2-4 Product certification 레벨 인증을 획득하였다.

Table 3. Number of ACC certified products (Mar. 2019)

Level	Device type	Certified product	Total
L1	Control Applications	5	209
	Embedded Devices	125	
	Network Devices	58	
	Product Families	21	
L2	Control Applications	3	149
	Embedded Devices	116	
	Network Devices	12	
	Product Families	18	
Total		358	

Table 4. Number of ACC certified products by Vendor (Mar. 2019)

Vendor	L1	L2	Total
Emerson Process Management	18	3	21
GE	37	2	39
Invensys	34		34
Schneider Electric	33	26	59
Sensus	52		52
Siemens	1	101	102
Yokogawa	11	2	13
Etc.	23	15	38
Total	209	149	358

2.3 산업 제어시스템 보안요구사항(TTA 표준)

TTA 표준인 산업 제어시스템 보안요구사항은 국내 산업 제어시스템의 운영 계층, 제어 계층, 현장장치 계층의 3계층에 대해 각 계층별 보안요구사항을 정의하고 있다. 산업 제어시스템 보안요구사항은 개념 및 참조모델(TTAK.KO-12.0307-part1), 현장장치 계층(TTAK.KO-12.0307-part2), 제어 계층(TTAK.KO-12.0307-part3), 운영 계층(TTAK.KO-12.0307 - part4)의 4부로 구성되어 있다.

운영 계층은 제어 계층으로부터 전달받은 데이터를 통해 현장장치 상태를 모니터링 하거나 제어명령을 전송하는 역할을 하며 HMI, EWS 등을 포함한다. 제어 계층은 현장장치에서 계측, 수집한 데이터를 모

Table 5. Security functions for Field Device, Control, and Operation layer

Areas	Functions	Field Device Layer	Control Layer	Operation Layer
Network Robustness	Fuzzing Test	O	O	O
	Stress Test	O	O	X
Service Continuity	Resource Availability	O	O	O
	Physical Interface Protection	O	O	X
	Event Response	O	O	O
Security Functions	Security Audit	O	O	O
	Identification and Authentication	O	O	O
	Access Control	O	O	O
	Transmission Data Protection	O	O	O
	Stored Data Protection	O	O	O
	Security Function Management	O	O	O
	State Management	O	O	O

니터링 계층으로 전달하거나 모니터링 계층의 제어명령을 받아 현장장치를 제어하고 PLC, DCS, RTU 등의 제어 H/W를 포함한다. 현장장치 계층에는 센서, 액추에이터 등이 포함되며 데이터 수집 또는 제어 동작을 수행한다[13].

산업 제어시스템 보안요구사항 표준에서는 각 계층별로 네트워크 견고성, 서비스 지속성, 보안 기능의 3개 분야별로 필요한 기능 시험을 분류하고 이에 따른 세부 보안요구사항을 정의하였다[14][15][16]. Table 5.는 각 계층별로 필요한 기능을 정리한 것이다. 운영 계층의 경우 운영체제 위에서 동작하는 특성에 따라 스트레스 시험과 물리적 인터페이스 보호 기능은 제외되었다.

III. 산업용 제어기기의 통신 견고성 시험 항목

Ⅱ장에서 설명한 바와 같이 통신 견고성 시험은 EDSA, Achilles, 산업 제어시스템 보안요구사항(TTA 표준) 등의 산업용 제어기기 인증 시험에 포함되는 항목이다. 통신 견고성 시험은 제어기기 내 통신 프로토콜 구현의 오류 검증 및 비정상적인 트래픽에 대한 대응 기능 확인을 그 목적으로 한다. 본 장에서는 앞에서 설명한 각 인증별 통신 견고성 시험 항목과 그 방법에 대해 설명한다.

3.1 EDSA CRT

EDSA 인증의 요구사항은 Fig. 2.와 같이 구성된다. 보안 개발 프로세스 검증은 SDLA-100, 300, 312(SDLPA) 및 EDSA-312(SDA-E)에 정의되어 있다. 임베디드 장치의 보안 기능 검증(FSA-E)은 CSA-311, 견고성 시험에 대한 요구사항(ERT)은 EDSA-310에 각각 정의되어 있다. ERT는 VIT와 CRT로 구성되며 각각 SSA-420, EDSA-401~406에 정의되어 있다[17].

CRT는 네트워크 프로토콜 구현 오류와 알려진 서비스 거부 취약점을 식별하는 것을 목적으로 하여 임베디드 장치의 프로토콜에 대한 견고성을 시험한다. CRT 검증을 위해 시험자는 높은 트래픽이나 오류 패킷을 발생시켜 전송하는 상황에서 필수 기능이 동작하는지 확인한다.

3.1.1 시험 항목

CRT는 임베디드 장치 내 프로토콜 구현이 정상 및 오류 패킷들에 대응하여 제어 기능을 정상적으로 제공할 수 있는지를 시험한다[18].

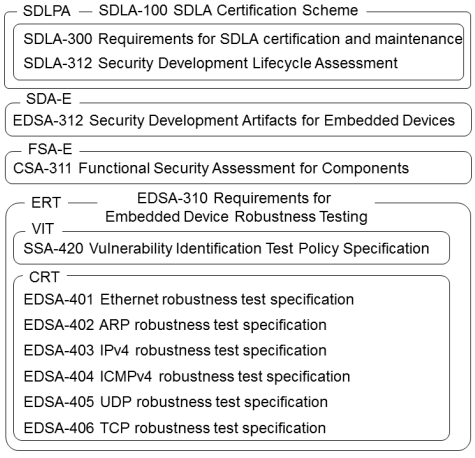


Fig. 2. Requirements for EDSA certification

Table 6. Test cases of ICMPv4 network protocol[19]

ICMPv4.T00	Baseline operation
ICMPv4.T01	Undefined ICMPv4 PDU types
ICMPv4.T02	Malformed ICMPv4 PDUs of defined PDU types
ICMPv4.T03	ICMPv4 PDUs of contextually inappropriate PDU type
ICMPv4.T04	ICMPv4 PDUs of appropriate PDU type but with invalid field content
ICMPv4.T05	Rejection of NPDUs with multicast or broadcast source IP addresses
ICMPv4.T06	Rejection of IP multicasts and broadcasts
ICMPv4.T07	Contextually inappropriate error PDUs
ICMPv4.T08	Maintenance of service under high load, including network saturation: Raw ICMPv4 NPDU flood

CRT는 인터페이스 시험(Interface Surface Tests), 견고성 시험(Basic Robustness), 로드 스트레스 시험(Load Stress Robustness)으로 구성된다. 인터페이스 시험은 프로토콜에 관계없이 공통 항목으로 정의되어 있으며 프로토콜별 표준 시험 스펙에는 견고성 시험, 로드 스트레스 시험이 정의되어 있다.

인터페이스 시험은 시험 대상에서 제공하는 서비스와 포트 식별을 통해 시험 대상 프로토콜 및 시험 대상의 필수 기능 동작 여부를 시험한다.

견고성 시험은 시험 대상의 특정 프로토콜에 대한 견고성을 시험하는 항목이다. 이 시험은 시험 프로토콜이 일반적인 상황에서 정상 동작하는지 확인하는 기본 동작 시험과 오류 메시지를 전송하는 시험으로 구성된다. 오류 메시지는 정의되지 않은 구조를 가지는 메시지, 잘못된 값을 포함하는 메시지, 문맥상으로 부적합한 메시지 등을 포함한다.

로드 스트레스 시험은 시험 대상에게 최대 대역폭 근처의 높은 트래픽으로 정상 패킷을 전달하는 경우 시험 대상이 필수 기능을 수행하는지 확인한다.

EDSA에는 Ethernet, ARP, IPv4, ICMPv4, UDP, TCP 프로토콜에 대한 시험 스펙이 표준에 정의되어 있다. Table 6.은 ICMPv4 프로토콜의 테스트 케이스로 견고성 시험, 로드 스트레스 시험 항목을 포함한다.

3.1.2 시험 방법

EDSA에서는 산업용 임베디드 장치의 필수 기능을 제어 기능, 프로세스 뷰, 알람, 명령, 히스토리 기능 등으로 정의한다[18]. 시험 신청자는 시험 대상이 제공하는 필수 기능, 필수 기능의 모니터링 기준, 서비스 제한 대역폭, 제어 신호의 최대 허용 지터, 시험 대상의 네트워크 인터페이스 및 구현 프로토콜 리스트 등을 식별하여 제공해야 한다. CRT 시험을 진행하는 동안에는 신청자가 식별한 임베디드 장치의 필수 기능이 네트워크 상태나 공격에 영향 없이 유지되는지를 확인한다.

필수 기능 중 하나인 제어 기능의 정상 동작 판단을 위해서 Fig. 3.과 같은 아날로그 출력과 디지털 출력을 제공하는 로직을 임베디드 장치에 탑재한다. 시험 진행 중에는 출력 신호에 지터가 발생하는지 확인한다[18].

- 아날로그 출력: 최소에서 최대까지 10단계로 나누어 증가하고 20 단계로 감소(1초씩 변화)
- 디지털 출력: 3초 주기 듀티 사이클(1초 동안은 1이 출력되고 2초 동안 0이 출력)

CRT는 다양한 프로토콜 구현 오류나 네트워크 트래픽 상황에서 시험 대상의 제어 기능을 비롯한 뷰, 알람, 명령, 히스토리 등의 필수 기능이 정상적으로 동작하는지 시험한다. 시험 대상의 방어 메커니즘에 의해 플러딩 발생 상황에서 필수 기능을 제공하지 않는 경우에는 플러딩이 멈춘 다음 필수 기능이 정상으

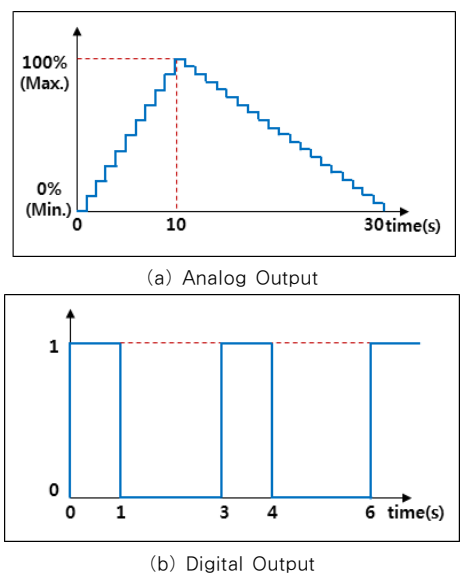


Fig. 3. Analog output and Digital output for DUT(Device under test)

Table 7. Recognized CRT Test Tools[20]

Supplier	Tool Name & Version	Date
Synopsys	Defensics Ethernet Test Suite 4.0.0, ARP Test Suite 6.0.0, IPv4 Test Suite 5.1.0, ICMPv4 Test Suite 5.1.0, TCP Server Test Suite 8.1.0, Codenomicon ISASecure Load Stress Testing Solution 2.1.0	2017.08.31
Hitachi Systems	Raven ES 2.0.0.0	2017.10.04
Beyond security	beSTORM EDSA 6.1.1 build 6584	2017.03.21
Wurldtech	Achilles Test Platform r2 3.16.1 Build 3.16.20 151217193830	2018.02.07
Wurldtech	Achilles Test Platform r3 3.16.1 Build 3.16.20 151217193830	2018.02.07
CNCERT/CC & Beijing Xinlian Kehui Technology Co. LTD	Acheron 2.2	2017.02.22
Beijing Winicssec Technologies Co. Ltd.	VHunter IVM (Industrial Control Vulnerability Mining System) V3.0	2019.01.25

로 돌아오는지 확인하여 정상동작 여부를 판단한다.

3.1.3 시험 도구

EDSA는 CRT 시험 도구에 대한 인증을 진행하고 있으며 시험기관은 인증 도구를 사용하여 인증 시험을 진행한다. 현재까지 인증된 CRT 시험 도구는 Table 7.과 같이 6개 제조사의 7개 제품이 있으며 Synopsys의 Defensics, Wurldtech의 Achilles Test Platform, Beyond security의 beSTORM 등이 포함된다[20].

3.2 Achilles 통신 인증 시험(ACC)

ACC는 통신 견고성 시험을 목적으로 프로토콜 구현, 알려진 취약점 등의 시험을 수행하며 임베디드 장치, 네트워크 장비, 호스트 장비, 제어 애플리케이션 등을 그 대상으로 한다. ACC는 Ethernet, IP, ARP, ICMP, TCP, UDP의 통신 프로토콜 이외에 Modbus/TCP 등의 산업용 제어 프로토콜도 대상에 포함한다[8][11].

Table 8. Types of test cases in Achilles[22]

Types	Description
Scan	examine whether the DUT can withstand port scanning
Storm	examine how the DUT handles packets at different packet rates
Fuzzer	generate valid and invalid packets with randomized header values
Grammar	generate invalid packets to test a specific protocol implementation
Known vulnerability	examine known vulnerabilities

3.2.1 시험 항목

ACC 시험 항목은 Table 8.과 같이 시험 대상이 포트 스캐닝을 견딜 수 있는지 시험하는 Scan, 다양한 패킷 대역폭을 견딜 수 있는지 시험하는 Storm, 프로토콜의 구현과 스택 기능 검증을 위한 Fuzzer와 Grammar 등의 시험으로 구성된다[22].

ACC 인증은 레벨에 따라 L1, L2로 나뉘며 L2 인증이 L1보다 많은 테스트 케이스에 대해 엄격한 기준을 적용하여 시험한다. 시험 프로토콜은 레벨에 관계없이 Ethernet, ARP, IP, ICMP, TCP, UDP이며 이외에 특정 제어 프로토콜에 대해 추가 인증을 요청할 수 있다. ACC 인증 제품 중 추가 프로토콜에 대해 인증을 받은 제품은 총 44개로 Modbus/TCP(18개), FlexNet RF(12개) 등의 제어 프로토콜에 대해 인증을 획득하였다.

ACC 인증의 시험 항목 수는 Table 9.와 같다. L1 시험 항목은 총 31개(L1: 8개, L1/L2 공통: 23개)이며, L2 시험 항목은 총 55개(L2: 32개, L1/L2 공통: 23개)로 구성된다. L2 인증은 L1보다 다양한 Grammar 항목을 포함하며 TCP 항목의 경우, TCP URG, TCP FIN 등의 Storm 항목에 대해 추가 시험을 수행한다. Etc. 항목은 문맥상 잘못된 TCP selective acknowledgment, receive window 등의 시험을 포함한다.

3.2.2 시험 방법

ACC 인증 시험 수행을 위해서는 Fig. 4.와 같이

Table 9. Test cases in ACC test suite

(a) Test cases in L1 only

	Scan	Fuzzer	Grammar	Storm	Etc.	Total
ARP			1			1
Ethernet			1			1
ICMP			1			1
IP			3			3
TCP			1			1
UDP			1			1
Total			8			8

(b) Test cases in L2 only

	Scan	Fuzzer	Grammar	Storm	Etc.	Total
ARP			1			1
Ethernet			4		1	5
ICMP		1	2			3
IP			4	1		5
TCP			4	6	6	16
UDP			2			2
Total		1	17	7	7	32

(c) Test cases in L1/L2

	Scan	Fuzzer	Grammar	Storm	Etc.	Total
ARP				3		3
Ethernet		1		3		4
ICMP				1	1	2
IP		1		4		5
TCP	1	1		2		4
UDP	1	1		3		5
Total	2	4		16	1	23

시험 도구를 시험 대상과 관리 S/W에 연결한다. 시험 도구는 패킷을 전송하는 동시에 시험 대상의 상태를 모니터링 하는 기능을 제공한다[23].

제어 기능의 정상 동작 확인을 위해 시험 대상의 디지털 출력은 0.5초 동안 1이 출력되고 0.5초 동안 0이 출력되는 1초 주기의 듀티 사이클로 구성한다.

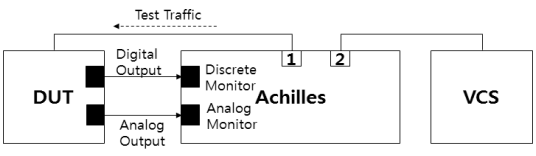


Fig. 4. ACC Level 2 Test Setup for Embedded Devices[23]

Table 10. Achilles Monitors[22]

Observation	Monitor
Control	- Analog monitor(analog output) - Discrete monitor(periodic digital output)
Communications	- ARP monitor(ARP response) - ICMP monitor(ICMP response) - Link state monitor(Ethernet link between the DUT and the Achilles) - Heartbeat monitor(recurring heartbeat message from the DUT)
Performance	- OPC monitor(observe VCS system performance) - Linux system monitor(DUT system performance)
Service	- TCP ports monitor(open port during testing) - UDP ports monitor(open port during testing)
View	- OPC monitor (DUT is communicating with the VCS)
* VCS: engineering station running HMI or device control S/W * DUT: Device Under Test	

아날로그 출력은 EDSA CRT와 동일하게 30초 주기의 신호로 구성한다. 이후 인증 시험에 필요한 상태 모니터와 시험 항목을 설정하여 시험을 수행한다.

3.2.3 시험 도구

GE의 Achilles Test Platform은 ACC L1, L2 레벨의 인증을 위한 시험 도구로서 패킷 전송 및 모니터링 기능을 제공한다. Achilles 시험 도구는 제어, 통신, 성능, 서비스, 뷰 기능의 상태 확인을 위해 Table 10.과 같이 다양한 모니터를 제공한다. Achilles Test Platform은 EDSA CRT 인증 도구로써 L2 레벨 시험 항목은 EDSA CRT 시험에도 사용된다[22].

3.3 산업 제어시스템 보안요구사항 네트워크 견고성 시험(NRT: Network robustness test)

산업 제어시스템 보안요구사항 표준은 제어시스템의 제어 계층, 운영 계층, 현장장치 계층별 네트워크 견고성 보안요구사항을 규정하고 있다[14][15][16]. 네트워크 견고성 보안요구사항은 시험 대상의 네트워

Table 11. Network Robustness test cases in Security Requirements for Control Layer

Fuzzing Test	
CH_FT.1	Handling of field order violations
CH_FT.2	Handling of truncated packet
CH_FT.3	Handling of field minimum length violations
CH_FT.4	Handling of field maximum length violations
CH_FT.5	Handling of specified field length violations
CH_FT.6	Handling of minimum repeat count violations
CH_FT.7	Handling of maximum repeat count violations
CH_FT.8	Handling of specified repeat count violations
CH_FT.9	Handling of fixed field value violations
CH_FT.10	Handling of field values for valid range violations
CH_FT.11	Handling of protocol context violations
Stress Test	
CH_ST.1	Handling of effective packet flooding
CH_ST.2	Handling of excessive connection attempts

크 기능에 대한 가용성에 관련된 보안요구사항으로 비정상적인 통신데이터 및 과도한 양의 통신데이터에 대한 대응 기능을 규정하고 있다.

3.3.1 시험 항목

산업 제어시스템 보안요구사항 네트워크 견고성 시험은 Table 11.과 같이 퍼징 시험 11개 항목과 스트레스 시험 2개 항목으로 구성되며 운영계층의 경우 스트레스 시험을 제외하고 수행한다.

퍼징 시험은 필드를 조작한 오류 패킷을 생성하여 전송하는 항목과 프로토콜 문맥상 부적절한 값으로 구성된 패킷을 전송하는 항목으로 이루어진다.

스트레스 시험은 시험 대상의 서비스 제한 최대 대역폭에 상응하는 패킷 플러딩이 발생하는 경우와 동시 접속 시도가 허용치를 초과하여 발생하는 경우 시험 대상이 정상 동작하는지 여부를 시험하는 항목으로 구성된다.

3.3.2 시험 방법

산업 제어시스템 보안요구사항 네트워크 견고성 시험은 시험 대상에 구현된 프로토콜 중에서 이더넷 환경에서 동작하는 프로토콜을 대상으로 하며 Fig. 5.와 같이 시험 도구 및 필수 기능 모니터링 장치를 시험 대상에 연결하여 진행한다[15].

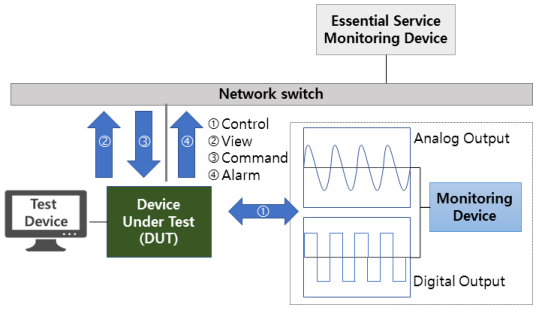


Fig. 5. Experimental environment for Network Robustness test[15]

네트워크 견고성 시험에서는 시험 대상에 패킷을 전송하는 동시에 정상적인 필수 기능을 유지하는지 확인한다. 제어 계층의 필수 기능은 제어 기능, 명령 기능, 뷰 기능, 알람 기능으로 정의한다. 제어 기능은 EDSA CRT와 동일하게 주기적인 디지털 출력과 아날로그 출력 로직을 구현한 다음 시험 도중 지터 발생 여부를 확인한다. 명령 기능은 시험 대상에게 일정시간마다 명령을 전송하도록 환경을 구성한 후 명령에 따른 제어 신호의 변경 여부를 통해 확인한다. 뷰 기능은 상태 정보 모니터에 불연속 구간이 발생하지 않는지를 확인한다. 알람 기능은 주기적으로 HIGH, LOW 알람이 발생하도록 설정한 다음 알람 이벤트 로그를 통해 누락이 없는지 확인한다.

3.3.3 시험 도구

산업 제어시스템 보안요구사항을 위한 네트워크 견고성 시험 도구는 현재 존재하지 않는다. 시험을 위해서는 EDSA, Achilles의 통신 견고성 시험 도구나 제어기기를 위해 오픈소스로 개발된 Peach, Sulley 등의 퍼징 시험 도구들을 활용할 수 있다[24]. 이때, 각각의 시험 도구에서 생성되는 퍼징 및 스트레스 패킷이 보안요구사항의 각 항목에 부합하는지에 대해서 확인이 필요하며 시험 대상의 필수 기능 모니터링 방법 또한 연구가 필요하다.

3.4 통신 견고성 시험 분석

CRT, ACC, NRT는 시험 대상과 시험 프로토콜

의 범위에 있어 일부 차이가 있지만 오류 패킷과 대용량 트래픽을 전송하는 동시에 필수 기능 유지 여부를 확인하는 것으로 진행하는 시험 방법은 유사하다. 특히, 제어 기능의 정상 동작 확인 방법은 시험 대상의 출력 신호를 주기적 신호로 설정한 다음 지터를 측정하는 방식으로 모두 동일하다.

기존의 시험 기준은 임베디드 장치의 특징에 초점이 맞춰져 있고 이외의 다른 산업용 제어기기의 시험 환경이나 기준에 대해서는 구체적인 설명이 부족하여 다양한 산업용 제어기기에 적용하기에는 한계가 존재한다. 이에 본 논문에서는 다양한 제어기기의 특성을 분석하고 이를 고려한 통신 견고성 시험 방안을 제시하고자 한다.

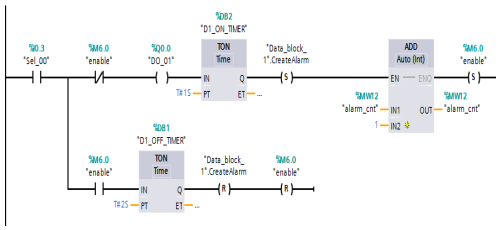
IV. 제안한 통신 견고성 시험 방안

산업 제어시스템은 제어기능을 수행하는 임베디드 장치인 제어 H/W와 이를 모니터링하고 관리하기 위한 제어 S/W, 현장에 설치되어 측정 및 명령을 수행하는 현장장치, 기기 간의 통신을 제어하기 위한 네트워크 장비 및 방화벽 등으로 구성된다. 본 장에서는 이러한 산업용 제어기기별 특징을 고려한 통신 견고성 시험환경 구축방안 및 시험 시 고려해야 할 사항을 제시하고자 한다.

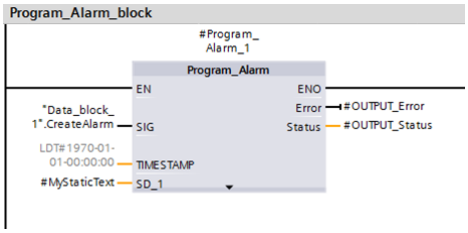
4.1 제어 H/W

제어 H/W는 로직의 수행 및 현장장치의 신호를 취합하고 명령을 전달하는 역할을 하는 장치로서 PLC, DCS, RTU, IED 등을 포함한다. 제어 H/W는 일반적으로 로직 탑재가 가능하고 디지털 및 아날로그 입출력 기능을 제공한다는 특징이 있다. 제어 H/W는 임베디드 장치의 특징을 가지고 있으므로 기존의 통신 견고성 시험 기준에 활용되는 제어, 알람, 뷰, 명령의 필수 기능에 대해 EDSA CRT 기준을 적용하여 시험 진행이 가능하다. 제어 H/W의 통신 견고성 시험 및 필수 기능 동작 확인을 위해 다음과 같이 설정한다.

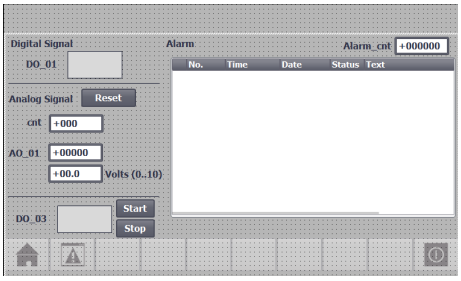
- 제어 기능 설정 : Fig. 3.과 같은 디지털 및 아날로그 신호 출력을 위한 로직을 구성한다. Fig. 6.(a)는 3초 주기의 디지털 출력 신호를 위한 래더 로직의 예이다.
- 알람 기능 설정 : 시험 대상의 알람 기능을 이용하여 주기적인 알람을 발생시킨다. 이 때, 제어 H/W의 알람 기능을 활용하거나 Fig. 6.(b)와 같이 래더 로직을 활용하여 구현한다. 알람의 발생시간과 내용은 로그에 저장하여 정상 동작 분석에 활용한다.
- 뷰 기능 설정 : Fig. 6.(c)와 같이 제어 H/W의 디지털 출력, 아날로그 출력 값을 읽어 와서 화면에 출력하는 HMI를 구성한다.



(a) Ladder logic for 3s duty cycle



(b) Ladder logic for alarm setting



(c) HMI screen

```
Dim LastTime, StopTime, i

StopTime=Now+1/24/3600

Do
    If Now>LastTime+0.1/24/3600 Then
        i=i+1
        LastTime=Now
    End If
Loop Until Now>=StopTime

End Sub
```

(d) Command script for output toggle

Fig. 6. Setting for Control H/W

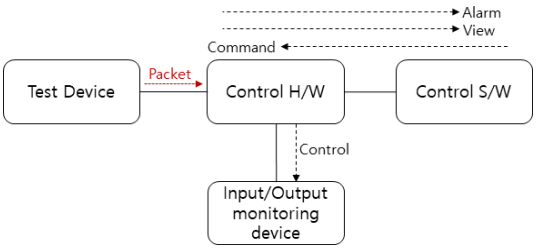


Fig. 7. Test environment for Communication robustness: Control H/W

- 명령 기능 설정 : Fig. 6.(d)와 같은 명령어 스크립트를 HMI에서 실행하여 제어 H/W의 디지털 출력을 주기적으로 변경하는 명령을 전송한다.

제어 H/W의 필수 기능을 설정한 다음, 통신 견고성 시험 환경을 Fig. 7.과 같이 구성한다. 제어 H/W의 출력 신호의 모니터링 도구로는 Labjack, NI의 LabView, 오실로스코프 등을 활용할 수 있다. 시험 도구가 오류 패킷 또는 대용량 트래픽을 전송하는 동안 입출력 모니터링 도구를 활용하여 아날로그 및 디지털 출력을 모니터링하고 제어 기능을 확인한다. 또한 사전에 구성한 HMI를 활용하여 명령 기능과 뷰 기능을 확인하고 알람의 히스토리 분석을 통해 알람 기능의 정상 동작을 확인한다.

4.2 제어 S/W

제어 S/W는 일반적으로 워크스테이션 및 운영체제 상에서 동작하는 소프트웨어로서 EWS, HMI 등을 포함한다. EWS는 제어 H/W 설정 및 로직의 개발·관리에 사용하며 HMI는 입출력 신호와 상태를 모니터링하고 명령을 입력하는 사용자 인터페이스를 제공한다.

제어 S/W는 제어 H/W에게 명령을 전달하는 명령 기능과 제어 H/W의 출력 상태를 모니터링 하는 뷰 기능을 필수적으로 제공해야 한다. 필수 기능의 확인을 위해 제어 S/W를 다음과 같이 설정한다.

- 명령 기능 설정 : 제어 S/W에서 주기적으로 명령을 전달하여 제어 H/W의 디지털 출력을 변경하도록 한다.
- 뷰 기능 설정 : 제어 S/W에서 입출력신호 및 히스토리를 모니터링 한다.

제어 S/W의 통신 견고성 시험 환경은 Fig. 8.과 같이 구성하고 필수 기능의 정상 동작을 확인한다. 시험 도구가 제어 S/W에 패킷을 전송하는 동안 제어 S/W의 명령이 제어 H/W에 전송되어 출력신호가 지속적으로 변하는지 확인한다. 동시에 입출력 신호가 끊어지지 않고 모니터링 되는지 확인한다.

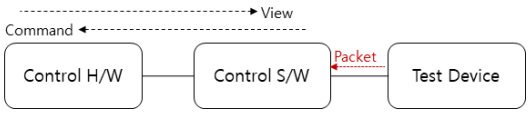


Fig. 8. Test environment for Communication robustness: Control S/W

제어 S/W는 운영체제 상에서 응용프로그램의 형태로 실행되는 경우가 많기 때문에 운영체제에서 통신을 처리하고 필요한 데이터만 제어 S/W로 전달할 가능성이 높다. 따라서 퍼징 패킷을 전송하는 시험에서는 운영체제에서 처리되는 계층 이외의 제어 S/W로 전달되는 데이터만을 시험 대상으로 해야 한다. 또한 대부분의 운영체제에서 대용량 트래픽에 대한 처리를 수행하기 때문에 해당 항목은 제어 S/W의 견고성 시험범위에서는 제외한다. 예외적으로 제어 S/W가 운영체제가 아닌 자체 구현한 드라이버를 사용하여 통신 데이터를 처리하는 경우에는 해당 프로토콜에 대해 통신 견고성 시험을 진행해야 한다.

HMI는 산업 제어시스템의 운영 중 상시 사용되는 소프트웨어이기 때문에 위협에 노출될 가능성이 높고 문제가 발생하는 경우 제어시스템의 가용성에 미치는 영향이 크다. 또한 고객의 요구사항에 따라 변경 가능성이 높은 소프트웨어라는 특징이 있다. 따라서 구현이 완료된 버전을 정확히 시험 대상으로 선정해야 하며 변경이 발생하는 경우 재시험이 필요하다. EWS는 상용 S/W로서 구현이나 기능상의 변경이 발생할 가능성이 낮아 인증 버전을 선정하기가 상대적으로 쉽다. 이와 같이 제어 S/W의 경우 시험 대상의 버전 선정이 중요한 이슈가 된다. 또한 소프트웨어의 변경이 발생하는 경우를 대비하여 변경된 구현 사항에 따른 재시험 항목의 선정 방안이 추가로 필요하다.

4.3 현장장치

현장장치는 현장에 설치되어 온도, 압력, 진동 등의 현장 상황을 측정 및 감지하여 전달하는 센서와 시스템을 제어하거나 동작을 수행하는 액추에이터를 포함한다. 기존의 현장장치는 Profibus, Modbus

등의 버스를 활용한 통신을 주로 수행하였으나 최근에는 Profinet, Modbus/TCP, EtherNet/IP 등의 이더넷 기반 프로토콜을 통해 통신하는 기기가 증가하고 있다. 통신 견고성 시험은 이와 같이 이더넷 환경에서 동작하는 현장장치를 대상으로 수행한다. EtherNet/IP 통신을 지원하는 Exlar의 TrexII 액추에이터, Profinet 통신을 지원하는 Siemens의 VS120 센서 등이 이에 포함된다.

현장장치는 장비의 기능과 특성에 따라 제공하는 필수 기능이 다양하다. 센서의 경우 주기적으로 값을 모니터링 하여 다른 제어기기에 전달하는 역할을 하기 때문에 측정값 전송이 필수 기능이 된다. 액추에이터는 시스템의 제어 동작을 수행하는 기기로서 어떤 환경에서도 제어 동작을 정상적으로 수행해야 한다. 이와 같이 산업 제어시스템의 현장장치는 그 특징에 따라 필수 기능의 선정 및 통신 견고성 시험 기준의 변경이 필요하다. 현장장치의 필수 기능 확인을 위해 다음과 같이 설정한다.

- 센서 기능 설정 : 센서에서 주기적으로 측정값(온도, 진동 등)을 제어 H/W에 전달하고 전달된 값을 지속적으로 모니터링 및 저장하는 환경을 구성한다.
- 액추에이터 기능 설정 : 액추에이터가 주기적으로 동작하도록 제어 H/W 출력을 설정한 다음, 액추에이터의 동작 히스토리를 로그에 저장하도록 한다.

현장장치의 통신 견고성 시험 환경은 Fig. 9.와 같이 구성하고 센서와 액추에이터의 각 필수 기능이 정상 동작하는지 확인한다. 센서의 경우, 통신 견고성 시험 패킷을 전송하는 동안 센서의 측정값이 제어 H/W에 정상적으로 전달되는지 확인한다. 액추에이터를 시험하는 경우, 통신 견고성 시험 중에도 액추에이터가 사전에 설정한대로 동작하는지 확인한다.

현장장치는 일반적으로 제어 H/W나 제어 S/W에

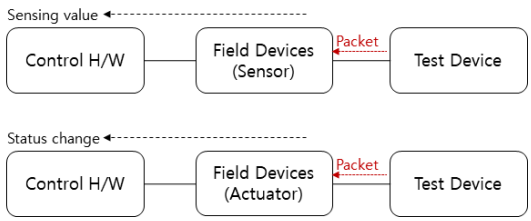


Fig. 9. Test environment for Communication robustness: Field Devices

비해 프로세서나 메모리의 사양이 떨어지는 경우가 대부분이다. 따라서 연산 능력이나 제공하는 보안기능에 제약이 존재하며 프로토콜 구현의 범위나 안전성 또한 한계가 있을 것으로 예상된다. 이러한 현장장치에 대한 통신 견고성 시험은 해당 기기의 취약점이나 가능한 위협을 확인하기 위한 중요한 수단이 될 수 있다. 최근에는 스마트 팩토리의 도입에 따라 무선통신 및 무선 제어 프로토콜(WirelessHART, ISA 100.11a 등)을 활용한 제품이 등장하고 있어 향후 이에 대한 통신 견고성 시험 방안이 추가로 필요할 것으로 보인다.

4.4 네트워크 장비 및 방화벽

네트워크 장비는 산업용 제어기기 간의 통신을 용이하게 하거나 통제하기 위해 사용되는 장비로서 스위치, 라우터 등을 포함한다. 방화벽은 망분리 및 이상 패킷의 탐지 또는 통제를 목적으로 활용된다. 산업 제어시스템 내 네트워크 장비 및 방화벽의 기능은 기기간의 통신 제어 및 관리 측면에서 일반적인 IT 환경과 큰 차이가 없지만 필요에 따라 산업용 프로토콜 통신을 지원하는 경우가 있다. IEC 61850 프로토콜을 지원하는 것으로 알려진 Ruggedcom 스위치와 Modbus, DNP 등의 제어 프로토콜에 대한 패킷 분석 기능을 제공하는 GE의 Opshield가 이에 해당한다.

네트워크 장비 및 방화벽은 어떤 상황에서도 산업용 제어기기 간의 정상적인 통신 상태를 제공하는 것을 목표로 한다. 따라서 기기간의 통신에 문제가 발생하지 않는 경우 필수 기능을 제공하는 것으로 판단할 수 있다.

네트워크 장비 및 방화벽의 통신 견고성 시험을 위해서는 Fig. 10.과 같이 제어 H/W, 제어 S/W, 시험 도구를 네트워크 장비 또는 방화벽을 통해 연결한 다음 제어 H/W와 제어 S/W 간의 명령 기능과 뷰 기능을 설정한다. 필수 기능의 확인을 위해서 시험 대상 장비를 기능에 따라 다음과 같이 설정한다.

- 네트워크 장비 기능 설정 : 제어 H/W와 제어 S/W를 네트워크 장비에 연결하여 둘 간의 통신이 네트워크 장비를 통해 이루어지도록 한다.
- 방화벽 장비 기능 설정 : 제어 H/W와 제어 S/W를 방화벽 장비에 연결하고 방화벽 장비에서 둘 간의 통신만 허가하도록 설정한다.

시험 도구가 시험 패킷을 네트워크 장비나 방화벽에

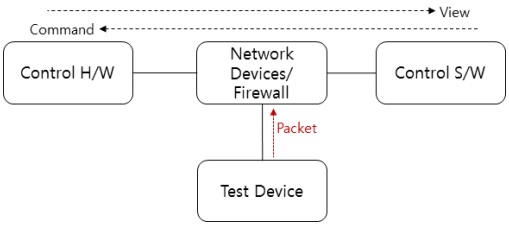


Fig. 10. Test environment for Communication robustness: Network Devices

전송하는 동안 제어 H/W와 제어 S/W 간의 명령 기능과 뷰 기능의 정상 동작을 확인함으로써 시험 대상의 필수 기능 제공 여부를 판단한다. 기기 간 통신 기능 확인을 위해서는 제어관련기기가 아닌 PC 두 대를 네트워크 장비로 연결하여 둘 간의 통신이 정상인지 여부를 확인해도 무방하지만 산업 제어시스템의 환경에 맞추어 시험을 진행하기 위해서 제어 H/W와 제어 S/W를 활용한 시험 환경을 구성한다.

네트워크 장비나 방화벽의 기능은 스스로 다른 장비와 직접 통신을 수행하는 것이 아니라 연결된 기기 간의 통신을 제어하는 것이다. 네트워크 장비에 구현된 프로토콜은 장비의 설정을 위한 목적이 대부분이며 일부 제어 프로토콜 기능 또한 자신에게 전달되는 메시지가 아닌 다른 기기 간 메시지의 통신 우선순위 조절을 주목적으로 한다. 따라서 네트워크 장비를 타깃으로 전송하는 패킷은 정상 패킷의 경우에도 버려지거나 응답이 오지 않을 가능성이 있다. 또한, 네트워크 장비는 문제가 발생할 경우 장비의 리셋을 통해 다른 기기간의 통신을 자동으로 복구하는 Watchdog 기능을 제공하는 경우도 있다. 이와 같은 네트워크 장비의 특성을 고려하여 시험 항목 선정과 정상 동작 판단 기준을 다음과 같이 추가하여 적용한다.

- 시험 항목 선정 : 동일한 기능의 정상 패킷을 다양하게 변경하면서 전송하여 응답이 모두 오지 않으면 해당 기능의 패킷은 버려지거나 응답하지 않는다고 판단하고 관련된 퍼징 시험은 항목에서 제외한다.
- 정상 동작 여부 판단 : Watchdog 기능을 포함하는 네트워크 장비의 경우, 통신 견고성 시험으로 인한 오류 발생 시 자동으로 리셋 하여 기기 간 정상 통신이 재개되는 데 일정시간 이하가 소요되면 통과로 간주한다.

4.5 시험 결과

이 장에서는 제안한 산업용 제어기기의 통신 견고성 시험 방안을 활용하여 시험 환경을 구축하고 시험을 수행한 결과를 설명한다. Fig. 11.은 제어 H/W를 대상으로 한 통신 견고성 시험 환경이다.

앞에서 설명한 바와 같이 통신 견고성 시험은 퍼징 패킷 또는 스트레스 시험을 위한 고부하 패킷을 전송하는 동안 시험 대상의 통신 상태 및 필수 기능을 모니터링 한다. 시험 수행을 위해 EDSA 인증 시험 도구인 Defensics를 사용하여 퍼징 및 스트레스 패킷을 전송하고 모니터링 하였다. 이 때, 제어 신호의 모니터링은 입출력장치에 Labjack을 연결하여 수행하였다. 시험을 진행하는 동안 시험 도구와 시험 대상 간의 통신 상태와 함께 필수 기능 정상동작 여부를 모니터링 하였다. 퍼징 시험의 통신 상태는 Defensics에서 시험 대상에 퍼징 패킷을 전송한 다음 정상 패킷을 전송하여 이에 대한 응답을 통해 성공 여부를 판단한다. 스트레스 시험의 통신 상태는 과부하 패킷이 시험 대상에 전송되는 동안 Labjack의 제어 신호에 지터가 발생하는지 확인하여 성공 여부를 판단한다. 또한 Fig. 12.와 같이 시험 대상의 필수 기능을 확인할 수 있는 HMI를 제작하여 결과 분석에 활용하였다.

시험 대상은 Table 12.와 같이 제어 H/W, 제어 S/W, 네트워크 장치, 방화벽 각각에서 주요 제조사 제품을 선택하여 제안한 방안의 시험을 수행하였다.

Table 13.은 PLC인 A 장비의 시험 결과이다. 해당 제품은 TCP 이하의 프로토콜로 통신을 수행하는 것으로 확인되어 Ethernet, IPv4, TCP 프로토콜을 대상으로 하여 시험을 수행하였다. 표에서 확인할 수 있듯이 퍼징 및 스트레스 시험을 하는 동안 시

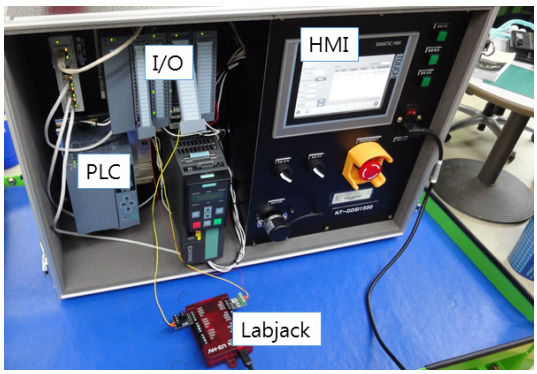


Fig. 11. Test environment for Communication robustness

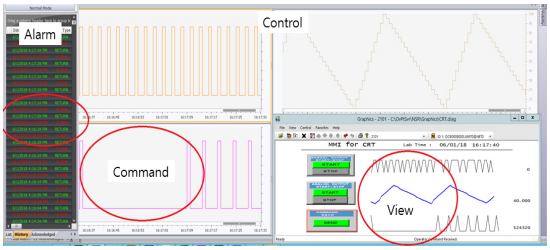


Fig. 12. Status Monitoring HMI for Control H/W

험 도구와 시험 대상 간의 통신 상태의 오류는 발생하지 않았으며 필수 기능도 모두 정상 동작하는 것으로 확인되었다.

Table 14.는 DCS인 B 장비의 시험 결과이다. 시험 결과, ARP 및 TCP 프로토콜에 대해서는 일부 퍼징 패킷 전송 시 시스템 리셋이 필요한 필수 기능 오류가 발생하는 것을 확인하였다. Fig. 12.는 ARP 시험 도중 명령 기능에 오류가 발생한 상황이다. 이때, 모니터링 화면에는 약 30초 동안의 명령에 대한 알람이 확인되지 않았으며 명령 및 뷰 화면에 출력 신호가 나타나지 않는 것을 확인하였다. 이와 같이 통신 견고성 시험을 수행하는 동안 필수 기능에 오류가 발생하는지 지속적인 확인을 통해 시험 결과를 판단하였다.

Table 12. Device Under Test

	Category	Product
A	Control H/W	PLC(Vendor A)
B	Control H/W	DCS(Vendor B)
C	Control S/W	HMI(Vendor C)
D	Network devices	Industrial Switches(Vendor D)
E	Firewall	Industrial Firewall(Vendor E)

Table 13. Test Results for Device A(PLC)

(a) Communication status

Protocol	Test cases	Fuzzing	Stress
Ethernet	98,602	Pass	Pass
IPv4	206,755	Pass	Pass
TCP	460,807	Pass	Pass

(b) Essential functions

Essential functions	Monitoring status
Control	Normal
View	Normal
Alarm	Normal
Command	Normal

Table 14. Test Results for Device B(DCS)

(a) Communication status

Protocol	Test cases	Fuzzing	Stress
Ethernet	98,602	Pass	Pass
ARP	358,389	Fail	Pass
IPv4	206,775	Pass	Fail
TCP	233,227	Fail	Fail
UDP	74,316	Pass	Fail

(b) Essential functions

Essential functions	Monitoring status
Control	Error
View	Error
Alarm	Error
Command	Error

Table 15.는 장비 C(HMI)에서 시험한 결과이다. 시험 결과, TCP 퍼징 시험을 하는 동안 시험 도구와 시험 대상 간의 통신 세션에 이상이 발생하였으나 그 경우에도 HMI의 모니터링 화면과 명령 기능은 정상 동작하였다. 해당 HMI 제품은 Windows CE 운영체제에서 동작하고 있으며 운영체제에서 대용량 트래픽에 대한 처리를 수행하기 때문에 스트레스 시험은 수행하지 않았다.

Table 16.은 D 장비에서 시험한 결과이다. 해당 제품은 EtherNet/IP로 통신을 수행하는 산업용 네트워크 스위치로 EtherNet/IP 및 TCP 이하의 프로토콜을 대상으로 시험을 수행하였다. EtherNet/IP는 이더넷 통신을 기반으로 하는 산업용 프로토콜로서 Rockwell의 PLC, EWS 등의 산업용 제어기기 간의 통신에 주로 사용된다. TCP/IP 기반의 통신에 CIP(Common Industrial Protocol)를 응용 계층으로 사용한다.

시험 결과, UDP 퍼징 시험 도중 시험 도구와의 세션에 문제가 발생하였으나 이와 연결된 기기

Table 15. Test Results for Device C(HMI)

(a) Communication status

Protocol	Test cases	Fuzzing	Stress
Ethernet	98,602	Pass	-
IPv4	206,775	Pass	-
TCP	298,937	Fail	-

(b) Essential functions

Essential functions	Monitoring status
View	Normal
Command	Normal

Table 16. Test Results for Device D(Industrial switch)

(a) Communication status

Protocol	Test cases	Fuzzing	Stress
Ethernet	98,602	Pass	Pass
ARP	358,389	Pass	Pass
IPv4	206,775	Pass	Pass
TCP	463,109	Pass	Pass
UDP	74,316	Fail	Pass
EtherNet/IP (connected)	106,142	Pass	-

(b) Essential functions

Essential functions		Monitoring status
Flow control (PLC-HMI)	View	Normal
	Command	Normal

(PLC-HMI) 간 통신에는 문제가 없었으며 스위치의 필수 서비스를 정상적으로 모니터링 할 수 있었다. 시험 도구로 사용한 Defensics는 산업용 프로토콜에 대한 스트레스 시험 기능을 제공하지 않아 EtherNet/IP의 스트레스 시험은 진행하지 못했다.

Table 17.은 산업용 방화벽 E에서 Ethernet, IPv4, TCP 프로토콜을 대상으로 하여 시험을 수행

Table 17. Test Results for Device E(Firewall)

(a) Communication status

Protocol	Test cases	Fuzzing	Stress
Ethernet	3,932	N/A	N/A
IPv4	3,033	Pass	Pass
TCP	8,494	N/A	N/A

(b) Essential functions

Essential functions		Monitoring status
Flow control (PLC-HMI)	View	Normal
	Command	Normal

한 결과이다. 시험 대상 장비의 경우 MAC 주소에 대한 규칙 설정이 불가능하여 Ethernet 퍼징 패킷을 모두 통과시켜(bypass) 시험을 진행할 수 없었다. 또한 TCP 시험 시 정상 동작을 확인하기 위한 응답 패킷만 통과시킬 방법이 없어 신뢰할 수 있는 시험 진행이 가능하지 않았다. IPv4 프로토콜에 대한 시험에서는 통신 세션 및 필수 기능이 모두 정상 동작 하는 것을 확인하였다.

4.6 통신 견고성 시험 방안 비교

Table 18.은 장비별 통신 견고성 시험 방안을 비

Table 18. Comparison on test methods among communication robustness testing

Device category	Test method	EDSA	ACC	NRT	Proposed
Control H/W	whether or not to test	O	O	O	O
	Essential function	Control View Alarm Command History reporting	Control	Control View Alarm Command	Control View Alarm Command
Control S/W	whether or not to test	X	O	O	O
	Essential function	undefined	unknown	View Command	View Command
Field devices	whether or not to test	X	X	O	O
	Essential function	undefined	undefined	Function for each device (not specific)	Sensor: Sensing value Actuator: Status change
Network devices/ Firewall	whether or not to test	X	O	X	O
	Essential function	undefined	unknown	undefined	Flow control (Command and View between devices)

교한 표이다. 표에서 확인할 수 있듯이 기존의 통신 견고성 시험은 제어 H/W에 대해서는 모두 유사한 시험 방안을 정의하고 있지만 제어 S/W, 현장장치, 네트워크 장비 및 방화벽에 대해서는 시험 대상으로 정의하지 않거나 시험 방안이 알려지지 않은 경우가 다수 존재한다.

제안한 시험 방안은 제어시스템을 구성하는 제어 H/W, 제어 S/W, 현장장치, 네트워크 장비 및 방화벽의 요소들 각각에 대해 시험 방안과 시험 시 판단 기준이 되는 필수 기능을 정의하였다. 제안한 시험 방안은 장비별 특성을 고려하여 작성되어 다양한 산업용 제어기기의 통신 견고성 시험에 활용이 가능하다. 특히 기존의 시험 방안에서 구체적인 방법이 확인되지 않는 현장장치와 네트워크 장비 및 방화벽의 통신 견고성 시험 시 활용성이 높을 것으로 예상된다.

V. 결 론

산업 제어시스템은 다양한 산업 분야 및 주요 기반 시설에서 사용되고 있으며 최근 취약점 및 이에 대한 사이버 공격이 증가하고 있다. 이러한 보안 위협에 대응하기 위해 산업용 제어기기에 대한 보안 평가 제도가 도입되어 운영 중이다. 본 논문에서는 국내·외 산업용 제어기기의 보안 평가 항목 중 통신 견고성 시험 제도에 대해 설명하고 그 특징을 분석하였다. 또한, 제어기기의 기능 및 특성에 기반한 기기별 통신 견고성 시험 기준 및 시험 방안을 제시하였다.

통신 견고성 시험은 제어기기의 공격에 악용될 수 있는 프로토콜 구현상의 취약점과 비정상적인 트래픽에 대한 대응책을 검증하는 것을 그 목적으로 한다. ISASecure의 EDSA, GE의 Achilles, 국내 TTA 표준인 산업 제어시스템 보안요구사항이 통신 견고성 시험 항목 및 기준을 정의하고 있다. 기존의 시험환경 및 기준은 대부분 임베디드 장치의 특징에 초점이 맞춰져 있고 이외의 다른 산업용 제어기기에 적용하기에는 한계점이 존재한다. 이에 본 논문에서는 산업 제어시스템에서 사용되는 제어 H/W, 제어 S/W, 현장장치, 네트워크 장비 및 방화벽의 특성을 반영한 통신 견고성 시험환경 구축방안 및 시험 시 고려해야 할 사항을 제시하였다. 제어 S/W의 경우 소프트웨어 변경이 발생하면 변경된 구현 사항에 따른 재시험 항목의 선정 방안이 필요하다. 현장장치의 경우 통신 견고성 시험 중 정상 동작 확인을 위해 다른 제어기기와의 연계가 필수적이며 제공하는 기능에 따라 필수 기능의 선정 및 통신 견고성 시험 기준의 변경이 필요하다. 네트워크 장비와 방화벽의 통신 견고성 시험을 위해서는 제어 H/W, 제어 S/W, 시험 도구와 시험 대상을 연결한 다음 견고성 시험을 진행하는 동안 서로간의 통신이 정상적으로 유지되는지 확인하는 것이 필요하다.

이와 같이 산업용 제어기기는 기능적 특성에 따라 시험 대상, 시험 프로토콜의 범위, 시험 항목 및 판단 기준이 달라질 수 있으므로 각 장비의 기능을 확인하고 그 기능에 따라 적용 가능한 시험 방법과 기준을 수립한 이후 시험 진행이 필요하다. 향후에는 본 논문에서 다루지 않은 IDS, IPS 등의 다양한 산업용 보안 장비에 대한 분석 및 시험 방안에 대한 연구가 추가적으로 진행되어야 한다. 또한 산업용 제어기기의 원격 증명 및 OTA 상황에서의 통신 견고성 시험 방안에 대해서도 연구가 필요하다.

References

[1] K. Stouffer, J. Falco, and K. Scarfone, “Guide to industrial control systems (ICS) security”, NIST SP 800-82 Revision 2, May 2015.

[2] SungJin Kim and Taeshik Shon, “Randomness Based Fuzzing Test Case Evaluation for Vulnerability Analysis of Industrial Control System”, Journal of The Korea Institute of Information Security & Cryptology, 28(1), pp. 179-186, Feb. 2018.

[3] ISASecure Certifications, https://isasecure.org/en-US/Certification.

[4] ASCI, “Embedded Device Security Assurance (EDSA) - version 3.0.0”, Oct. 2018.

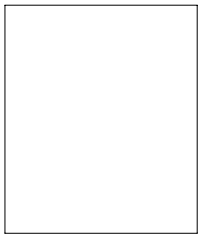
[5] “Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components”, IEC 62443-4-2 Ed.1, Jan. 2019.

[6] ISASecure Certified Devices, https://isasecure.org/en-US/End-Users/ISASecure-Certified-Devices.

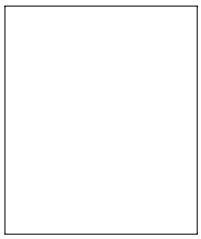
[7] Son Kyung Ho, “Industrial control system security evaluation and certification trend analysis,” REVIEW OF KIISC, 2

4(5), pp. 15-25, Oct. 2014.
〔8〕 Wei Zhao, Feng Xie, Yong Peng, Yang Gao, Xuefeng Han, Haihui Gao, and Dejin Wang, "Security Testing Methods and Techniques of Industrial Control Devices," Proceedings of the 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 433-436, Oct. 2013.
〔9〕 Xie F., Peng Y., Zhao W., Gao Y. and Han X., "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, Nov. 2014.
〔10〕 Achilles-System-Certification-FAQ, https://www.ge.com/digital/sites/default/files/download_assets/Achilles-System-Certification-FAQ.pdf.
〔11〕 Achilles Communications Certified Products, https://www.ge.com/digital/applications/achilles-communications-certified-products.
〔12〕 Achilles Practices Certified Solutions, https://www.ge.com/digital/applications/achilles-practices-certified-solutions.
〔13〕 Security Requirements for Industrial Control System - Part 1: Concepts and Reference Model, TTAK.KO-12.0307-Part1, June 2017.
〔14〕 Security Requirements for Industrial Control System - Part 2: Field Device Layer, TTAK.KO-12.0307-Part2, June 2017.
〔15〕 Security Requirements for Industrial Control System - Part 3: Control Layer, TTAK.KO-12.0307-Part3, June 2017.
〔16〕 Security Requirements for Industrial Control System - Part 4: Operation Layer, TTAK.KO-12.0307-Part4, June 2017.
〔17〕 ASCI, "Embedded Device Security Assurance - ISASecure certification requirements (EDSA-300) - version 3.6", Oct. 2018.
〔18〕 ASCI, "Embedded Device Security Assurance - Requirements for embedded device robustness testing (EDSA-310) - version 2.2", Feb. 2015.
〔19〕 ASCI, "Embedded Device Security Assurance - Testing the robustness of implementations of IETF ICMPv4 network protocols (EDSA-404) - version 1.3", Sep. 2010.
〔20〕 ISASecure - CRT Test Tools, https://isasecure.org/en-US/Test-Tools/Recognized-CRT-Test-Tools.
〔21〕 Achilles Test Platform Datasheet, https://www.ge.com/digital/sites/default/files/download_assets/achilles-test-platform-from-ge-digital-datasheet.pdf.
〔22〕 Wurldtech, "Achilles Test Platform User Guide - v 3.17", Dec. 2015.
〔23〕 Achilles Level 2 Certification Requirements for Embedded Devices, https://www.se.com/es/es/download/document/CERTLEV2/.
〔24〕 Steffen Pfrang and David Meier, Michael Friedrich and J¨urgen Beyerer, "Advancing Protocol Fuzzing for Industrial Automation and Control Systems", International Conference on Information Systems Security and Privacy, pp.570-580, Jan. 2018.

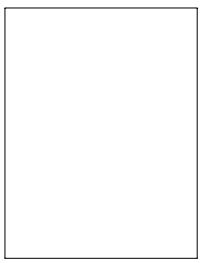
〈저자소개〉



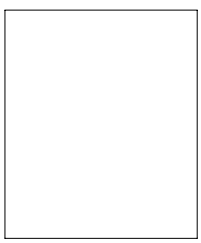
박 경 미 (Kyungmi Park) 정회원
2003년 2월: 한국과학기술원 전산학과 졸업
2011년 2월: 한국과학기술원 전산학과 박사
2011년 3월~2016년 8월: 삼성전자 VD사업부 책임연구원
2016년 9월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 기반시설보안, ICS 보안, 프로토콜 퍼징, 산업용 무선통신, 머신러닝



신 동 훈 (Donghoon Shin) 종신회원
2007년 9월: 한동대학교 전산학/전자공학 학사
2009년 9월: 한국과학기술원 전산학과 석사
2016년 2월: 한국과학기술원 전산학과 박사
2016년 3월~2019년 2월: ETRI 부설연구소 선임연구원
2019년 2월~현재: 대구경북과학기술원 조교수
〈관심분야〉 기반시설보안, ICS 보안, 무선통신, 계산이론



김 우 넌 (WooNyon Kim) 정회원
1996년 2월: 안동대학교 컴퓨터공학과 졸업
1998년 2월: 경북대학교 컴퓨터과학과 석사
2000년 2월: 경북대학교 컴퓨터과학과 박사수료
2000년 3월~2003년 12월:㈜니츠 선임연구원
2003년 12월~현재:ETRI 부설연구소 책임연구원
〈관심분야〉 기반시설보안, ICS/CPS/IIoT 보안, ICS 보안성/안전성 평가



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 선임연구원/팀장
〈관심분야〉 기반시설보안, 스마트그리드 보안, 취약점 분석, CPS 보안