Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.2, Apr. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.2.245

국내 중소 제조 기업 실정에 적합한 Modbus 프로토콜 취약점 대응 대책 연구

유 정 훈,[1†] 배 춘 석,[1] 고 승 철[2‡]
[1,2]수원대학교 (대학원생, 교수)

An Empirical Study on the Vulnerability of the Modbus Protocol Suitable for the SMEs Manufacturing Enterprises in Korea

Jung-hoon Yoo,[1†] Chun-sock Bae,[1] Sung-cheol Goh[2‡]
[1,2]The University of Suwon (Graduate student, Professor)

요 약

중소벤처기업부에서 발표한 스마트 제조혁신을 정부의 핵심 국정과제로 설정하고 2022년까지 스마트 공장 3만개를 보급을 추진하고 있으나, Modbus 프로토콜의 보안 이슈 사항은 여전히 남아있다. 이에 국내·외 Modbus 노출 현황과 주요 보안 정보 사이트를 통한 취약점 현황을 조사한다. 본 논문에서는 또한 조사된 Modbus 취약점을 악용한 산업제어시스템의 공격이 가능함을 확인할 목적으로 PERA 모델을 참고하여 Cell/Area Zone에서 Modbus/TCP의 실험환경을 구성하고 제어시스템의 위험성을 확인하였다. 이러한 위협요소를 해소할 목적으로 계층별 위험요소 및 대응 대책을 제시하고 전문가 집단을 통해 실용성을 확인하였다. 이를 통해 국내 중소기업에서 전산 담당자가 보안 체크리스트를 이용하여 사전예방을 위한 보안 대책 방안으로 활용할 수 있을 것으로 기대한다.

ABSTRACT

Although smart manufacturing innovation announced by the Ministry of SMEs and Startups is set as the government's core national task and is pushing to distribute 30,000 smart factories by 2022, security issues of Modbus protocol still remain. Accordingly, the current status of exposure to Modbus at home and abroad and the status of vulnerabilities through major security information sites are investigated. In this paper, the experimental environment of Modbus/TCP was constructed in Cell/Area Zone and the risk of the control system was confirmed by referring to the PERA model for the purpose of confirming that the attack of the industrial control system that exploited the investigated Modbus vulnerability is possible. For the purpose of solving these threats, risk factors and countermeasures for each class were presented, and practicality was confirmed through a group of experts. Through this, it is expected that in domestic SMEs, the computer manager can use the security checklist as a security countermeasure for proactive prevention.

Keywords: ICS Protocol, Modbus protocol, CIP, Industrial Control System, ICS Security Checklist

I. 서 론

Modbus는 제조 공장의 기계들을 자동화하고 제어하는 목적으로 사용되는 PLC(Programmable Logic Controller)들과의 상호 간의 통신 목적으로 개발된 시리얼 통신 프로토콜로서, Modbus는 산업제어 응용 분야와 석유 및 가스 분야에 주로 가장 많이 사용하고 있다.

Received(12. 15. 2020), Modified(02. 18. 2021), Accepted(02. 18. 2021)

† 주저자, james.yoo@suwon.ac.kr
‡ 교신저자, goh5703@suwon.ac.kr(Corresponding author)

프로토콜의 단순성과 효율성으로 산업 제조 환경에서 가장 널리 사용되고 있는 프로토콜로써, 일반적으로 산업제어시스템 분야에서 사실상(De facto) 표준 프로토콜로 간주 된다[1]. 하지만 전자 장치 간의 제어시스템들이 인터넷으로 전환됨에 따라 산업제어시스템에 적용된 Modbus/TCP를 사용되면서 다양한 보안 위협들이 존재하고 있다.

더불어 국내 산업단지에서도 공장 자동화 목적으로 구축된 산업제어시스템에서 널리 이용되고 있으며, 최근 중소벤처기업부에서 발표된 스마트 제조혁신을 정부의 핵심 국정과제로 설정하고 2022년까지 스마트 공장 3만개를 보급을 추진하나 전자기기들을 연결하는 주요특화된 산업제어시스템에서 사용하는 Modbus 프로토콜을 여전히 사용 되고 있다[2].

상황이 이러함에도 불구하고 중소기업에서는 예산과 인력이 부족할 뿐만 아니라 경영진의 정보보안 인식 재고가 부족하고 가동 중인 시스템들도 노후화되어 있어 패치나 업그레이드가 어려운 실정이다.

특히, 국내 중소기업에서도 산업제어시스템 내에 있는 Modbus/TCP 프로토콜이 활용되고 있어 보안취약점을 간과할 수 없다. Modbus 취약점으로는 무단 명령 실행 공격(Unauthorized Command Execution Attacks), Modbus DOS 공격(Modbus Denial-of-Service Attacks), MITM 공격(Man-in-the-Middle Attacks), 재사용 공격(Replay Attacks)이 대표적인 공격이다[3].

이에 해킹에 의한 보안 사고가 발생될 가능성이 확인할 목적으로 국내·외 Modbus 취약점 현황을 네 가지 종류의 취약점 검색엔진을 활용하여 조사하였다.먼저 실시간 Shodan ICS Radar 사이트를 통한 Modbus 채용 현황[4]을 확인하고 미국의 취약점 데이터베이스 NVD(National Vulnerability Database) 검색엔진을 통한 Modbus 취약점 현황[5] 및 비영리 단체인 Mitre의 CVE (Common Vulnerabilities and Exposures)를 활용하여 공격 유형별 Modbus 취약점 현황[6]을 조사하였다.

더불어, IBM X-Force Exchange를 활용하여 제조사별 CVE 취약점 현황[7]을 조사하였다.

본 논문에서는 앞서 조사된 Modbus 취약점의 위험성을 입증하기 위해서 Shodan을 이용하여 산업제어시설 내의 특화된 Modbus/TCP 프로토콜을 탑재한 장비의 취약한 요소를 확인하였다. 또한 산업제어시스템의 제어 로직 공격이 가능함을 확인할 목적으로 Purdue Enterprise Reference Architecture (PERA)[8]를 참고하여 Cell/Area (OT) Zone에서 Modbus/TCP Master와 Slave 실험환경을 구성하고 내부의 PLC 시스템을 4가지의 공격 (Move and Fill, Never Stop, Stop All, Stop and Fill)으로 실제 위험성이 있음을 재차 확인하였다.

본 논문에서 이러한 위협요소를 해소할 목적으로 산업제어 법규와 기존에 나와 있는 보안 체크리스트를 참고하여 계층별 위험 요소 및 대책을 제시한 후 국내 중소기업에서 전산 담당자가 기본적인 점검을 손 쉽게 적용 가능 하도록 보안 체크리스트를 개발하고 전문가 집단을 통한 설문조사를 통하여 보안 체크리스트의 타당성을 입증하였다. 이를 통해 중소기업에서 전산 담당자가 최소한의 사전예방을 위한 취약점 보안 대응 대책 방안으로 활용 할 수 있을 것으로 기대한다.

II. 선행연구 분석

본 논문에서는 Modbus 취약점과 관련되어 2008년 이후부터 발표된 주요 결과를 분석한다.

P. Huitsing 등(2008)은 Modbus Serial과 Modbus/TCP 프로토콜의 보안 위협과 특성을 식별하고 공격 영향도를 도출하고 다양한 공격을 통해 피해가 발생할 수 있음을 제안하였으나[9], Modbus의 프로토콜의 위협과 특성 및 공격 영향도 측면에서만 한정하였다.

송재구 등(2009)은 스카다(SCADA: Supervisory Control and Data Acquisition)시스템에서 사용된 Modbus 프로토콜의 RS-232와 RS-485를 통해 MITM 위협요소를 사용하여 해킹 테스트 프로그램 개발을 논하였고[10], Modbus Serial 방식에만 연구범위를 한정하였다.

이종주 등(2010)은 “SCADA 시스템의 보안성 평가를 위한 테스트베드 구성”에서 SCADA 시스템의 계층구조와 통신 사양 및 통신규약(Modbus RTU: Modbus Remote Terminal Unit)을 통한 보안성 평가 측면에서 물리적 접속방법이나 해킹 방법 및 절차를 제안하였으나[11], Modbus RTU 방식에만 연구범위를 한정하였다.

유형욱 등(2013)은 “제어시스템 보안을 위한 whitelist 기반 이상 징후 탐지 기법”에서 제어시스템에서 발생할 수 있는 이상 징후 유형들을 분류하고, 네트워크 레벨에서의 화이트리스트를 통해 이상

징후를 탐지할 수 있는 모델을 논하였고[12], 이 연구 결과는 기술적 보안에만 한정되어 전문 인력이 부족한 국내 중소기업에 적용하기가 곤란하다.

김현석 등(2018)은 "산업제어시스템보안을 위한 패킷분석 기반 비정상행위 탐지시스템 구현"에서 사이버 공격에 있어 보안솔루션 적용이 매우 중요하다고 하였고, 침입 탐지시스템을 활용하여 세 가지 규칙(통신주기, 페이로드 크기, 페이로드의 데이터 값)을 반영하여 입증은 하였으나[13], 이 연구는 기술적 보안에 한정되어 있어 중소기업 담당자가 현실적으로 활용하기에는 어렵다.

이처럼 선행 연구들을 살펴본 결과 프로토콜에 대한 물리적, 관리적, 기술적 연구는 있지만, 현실적으로 중소기업을 위한 적용할 수 있는 사전예방대책이 매우 시급하다.

III. 배경 지식

3.1 Modbus/TCP 개요 및 동작 방식

Modbus/TCP는 OSI 모델의 7계층에 위치한 애플리케이션 계층 메시지 프로토콜로서, 서로 다른 유형의 버스 또는 네트워크에 연결된 장치 간 클라이언트/서버 통신을 제공한다. 현재까지 Modbus 프로토콜은 단순하고 수행할 수 있는 기능과 활용성이 다양하여 현재까지도 많이 활용되고 있다. 1996년에 발표된 Modbus/TCP 프로토콜을 살펴보면 IANA(Internet Assigned Number Authority)에 등록되어 있고 포트 번호는 502로 기본 할당되어 있다. 기본적인 Modbus 통신방식은 다음과 같다.

Fig. 1.과 같이 Modbus 통신방식은 Master-Slave 구조이며, Master(Modbus Client)가 통신을 개시하여 Slave(Modbus Server)에게 명령을 보내면 Slave는 이에 반영하여 주어진 명령을 수행하고 이에 맞는 응답을 Master에게 회신하는 폴링 방식이다[14].

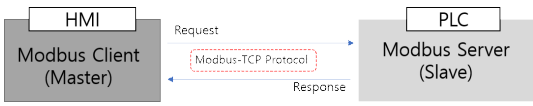

Fig. 1. Modbus Client/Server Communication

3.2 Modbus/TCP 프로토콜의 문제점

산업제어시스템에 활용되고 있는 Modbus/TCP 프로토콜의 문제점은 다음과 같다.

Table 1.과 같이 Modbus/TCP 프로토콜의 보안 문제점은 기밀성 결함, 무결성 결함, 인증 결함, 단순 프레이밍, 세션 구조 결함과 같이 5가지의 문제점이 존재하고 사이버 공격에 취약하다. 이러한 프로토콜은 제어 네트워크 내에서만 허용되어야 하나 실제로는 외부 검색엔진에 정보가 노출되어 사이버 공격의 위험성이 존재한다.

Table 1. Modbus/TCP Protocol Vulnerability

Security Issues	Detailed Description
Lack of Confidentiality	All Modbus messages are transmitted in clear text across the transmission media.
Lack of Integrity	There are no integrity checks built into the Modbus application protocol. As a result, it depends on lower layer protocols to preserve integrity.
Lack of Authentication	There is no authentication at any level of the Modbus protocol. One possible exception is some undocumented programming commands.
Simplistic Framing	Modbus/TCP frames are sent over established TCP connections. While such connections are usually reliable, they have a significant drawback. TCP connection is more reliable than UDP but the guarantee is not complete.
Lack of Session Structure	Like many request/response protocols (ex. Simple Network Management Protocol (SNMP), HTTP, etc.), Modbus/TCP consists of a short transaction in which the master initiates a request that requires a single operation to the slave.

IV. 국내·외 Modbus 공격사례 및 취약점 현황

4.1 국내·외 Modbus 취약점 공격 사례

2011년 데일리시큐 기사에 따르면, 국제 해킹보

안 컨퍼런스 POC 2011에서 이스라엘 해커 Yaniv Miron는 "SCADA Dismal, or, Bang SCADA"라는 주제로 발표를 진행하였다[15]. Modbus는 중요한 인프라 분야에 널리 사용되는 통신 표준으로 통신 프로토콜의 위험성을 입증한 바 있다.

2015년 보안뉴스 기사에 따르면, 한수원의 원전 자료 유출 사태로 인해 'SCADA 시스템'을 노린 사이버 공격이라는 점에서 문제가 심각하고 인터넷의 발달로 사내 회사 망과 연결되는 경우와 외부 협력업체와의 협업으로 인한 문제, 다양한 저장매체 이용 등으로 인해 보안취약점이 점점 증가된 것을 언급하였다. 또한, 한국 내 SCADA 시스템의 보안수준을 알아보기 위해 국제계측제어학회(ISA)의 ISCI(ISA Security Compliance Institute)가 제공하는 ISASecure 인증 프로그램의 통신 강건성 테스트(CRT: Communication Robustness Test)에 사용되는 'Defensics(디펜직스)'라는 퍼징(Fuzzing) 도구로 국내에서 점유율이 높은 PLC 제조사의 한 제품을 테스트한 결과 제로데이 취약점이 다수 포함되었다[16].

2020년 보안뉴스 기사에 따르면, ICS(Industrial Control System, 산업제어시스템) 분야의 경우 무조건 '폐쇄망'이라고 믿고 있어 사이버보안의 중요성을 간과하고 있으며, 외부에서 들어온 장비가 바이러스에 감염될 것임을 인지하는 기업은 많지 않다[17]. 또한, 제어시스템 장치 내에 있는 Modbus가 외부 검색엔진을 통해 외부에 연결되었는지를 내부 담당자들이 모르는 부분이 많다는 것을 언급하였다.

2020년 IT World 기사[18]에 따르면, 트렌드마이크로(Trend Micro)가 최근 블랙햇 USA 가상 보안 콘퍼런스에서 Industry 4.0 환경에서 프로토콜 게이트웨이 장치가 새로운 취약성을 보여주는 중요한 공격요소임을 확인시켜 주었다. 더불어, Modbus는 OT(Operational Technology) 네트워크에서 가장 광범위하게 사용되는 프로토콜 가운데 하나이기 때문이다.

4.2 국내·외 Modbus 프로토콜 취약점 현황

국가 취약점 데이터베이스(NVD)를 활용하여 Modbus를 조사하였고 취약점은 83개 확인하였다.

Fig. 3.와 같이 Modbus의 경우 년도 별로 2007, 2011, 2018년에도 취약점이 발견된 것을 재확인확인 하였다. Modbus 노출 인지도를 살펴보기 위해 또한, 실시간 Shodan ICS Radar(2020. 02. 21 기준)사이트를 활용하여 Modbus 프로토콜의 취약점 개수는 다음과 같다.

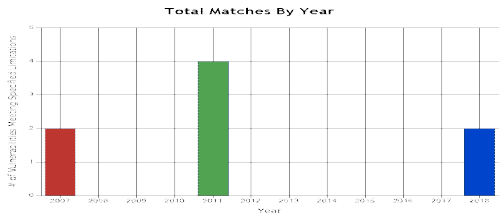

Fig. 2. Total Matches By Year by Modbus Protocol

Table 2.는 실시간 Shodan ICS Radar 사이트를 통해 Modbus 프로토콜을 사용하는 502 포트의 노출 개수는 13,949개임을 확인하였다.

더불어, Shodan사이트(2020. 02. 21 기준)을 통해 국내·외 Modbus 노출 개수를 기준으로 국내·외 Modbus 취약점 Top 3을 확인하였다.

Table 3.의 경우 미국은 3,661개, 프랑스는 1,652개, 한국은 1,547개로써 Modbus 프로토콜의 노출 개수가 많다는 것을 확인하였다. 이에 따라, 한국의 Modbus 프로토콜이 노출됨에 따라 사이버 공격에 위험성이 있음을 확인하였다. 국내 기준으로 지역별 Modbus 프로토콜의 노출 현황을 살펴보았다.

Table 4.의 경우 서울이 52개, 속초와 광주

Table 2. Number of Vulnerable Modbus Protocols via Real-time Shodan ICS Radar

Protocol	Total Count	Default Port
Modbus	13,949	502

Table 3. Top 3 Exposure status of Modbus Protocol based on Domestic and overseas Industrial Control System

U.S	France	Korea
3,661	1,652	1,547

Table 4. Number of systems using Modbus protocol by region

Region	Total Count
Seoul	52
Sokcho	22
Gwangju	22
Jeonju	18
Iksan	16

가 22개로 가장 많았고, 그다음으로 전주와 익산이었다.

종합적으로 살펴보면, Table 2.~Table 4.를 확인한 결과, 전 세계의 Modbus 프로토콜 노출 현황을 확인하였고, 한국에도 Modbus 프로토콜이 많아 3위임을 확인하였고, 국내의 경우 서울, 속초, 광주에 Modbus 프로토콜을 활용한 502 포트가 노출된 것을 확인하였다.

4.3 Mitre를 활용한 공격유형별 Modbus 취약점 현황

Mitre CVE 사이트(https://cve.mitre.org)를 통해 Modbus 프로토콜 취약점 현황을 조사하였다.

Table 5.는 CVE를 통한 Modbus 취약점은 다음과 같다. 샘플링을 통해 공격 유형을 확인한 결과 7개의 공격 유형이었고 총 71개 이다, 무차별 공격은 34개로 가장 많았으며, 그다음은 버퍼 오버 플로워가 12개, 예외 처리는 9개, 스푸핑&재사용 공격은 4개, 접근제어와 정보 노출의 경우 각각 3개이다.

Table 5. Number of Modbus Vulnerabilities by Attack type through Mitre CVE

Source	Attack Type	Total Count
CVE (71)	denial of service	34
	buffer overflow	12
	Uncaught Exception	9
	downloaded, modified, and uploaded	6
	spoofing or replay attacks	4
	Access Control	3
	Information Exposure	3

4.4 X-Force를 활용한 공격유형별 Modbus 취약점 현황

IBM X-Force Exchange 사이트를 통해 Modbus 프로토콜을 조회한 결과는 다음과 같다.

Table 6. Manufacturer's CVE Vulnerability

Source	CVE-ID	Attack Type
Schneider Electric (25)	CVE-2019-6808 CVE-2018-7847 CVE-2013-0664	Schneider Electric Modicon Controllers code execution
Schneider Electric (25)	CVE-2018-7853 CVE-2018-7855 CVE-2018-7854 CVE-2019-6819 CVE-2018-7849 CVE-2018-7857 CVE-2019-6807 CVE-2018-7856 CVE-2018-7851 CVE-2018-7852 CVE-2018-7843	Schneider Electric Modicon Controllers denial of service
	CVE-2019-6816	Schneider Electric Modicon Quantum denial of service
	CVE-2019-6806 CVE-2018-7848 CVE-2018-7844 CVE-2018-7845	Schneider Electric Modicon Controllers information disclosure
	CVE-2018-7824	Schneider Electric Modbus Serial Driver privilege escalation
	CVE-2017-6032	Schneider Electric Modicon Modbus Protocol brute force
	CVE-2017-6034	Schneider Electric Modicon Modbus Protocol security bypass
	CVE-2011-4861	Schneider Electric Quantum Ethernet Module Modbus_125_handler security bypass
	CVE-2017-7575	Schneider Electric Modicon TM221CE16R information disclosure
	CVE-2013-0662	Multiple Schneider Electric products Modbus Serial Driver buffer overflow

Source	CVE-ID	Attack Type
Siemens (1)	CVE-2019-6578	Siemens SINAMICS PERFECT HARMONY GH180 Drives NXG I and NXG II denial of service
Kunbus (5)	CVE-2019-6531 CVE-2019-6549	Kunbus PR100088 Modbus gateway information disclosure
	CVE-2019-6527 CVE-2019-6533	Kunbus PR100088 Modbus gateway security bypass
	CVE-2019-6529	Kunbus PR100088 Modbus gateway denial of service
Auto-Maskin (1)	CVE-2018-5400	Auto-Maskin RP remote panels and DCU controls units security bypass
Belden (1)	CVE-2017-11401	Belden Hirschmann Tofino Xenon Security Appliance security bypass
GE (1)	CVE-2017-7905	GE Multilin SR Protective Relays information disclosure
Traingle Research (2)	CVE-2013-5741 CVE-2013-2784	Traingle Research Nano-10 PLC Modbus data denial of service
Automated Solutions (2)	CVE-2010-4709	Automated Solutions Modbus/TCP Master OPC Server Modbus buffer overflow
	CVE-2007-4827	Automated Solutions Modbus/TCP Slave ActiveX control buffer overflow

Table 6.은 제조사별 CVE 현황을 확인하였다. 확인한 결과 Schneider Electric 제조사가 25개로 가장 많은 취약점이 있고, 그다음으로 Kunbus 제조사가 5개의 Modbus 취약점을 보유하고 있고, Traingle Research, Automated Solutions는 제조사별로 2개의 Modbus 취약점이 있다. 마지막으로, GE, Belden, Auto-Maskin의 경우 제조사별로 1개씩의 Modbus 취약점을 가지고 있다. 종합적으로 요약하자면, 공통적으로 발생한 취약점은 4개의 형태로써 Denial of service, buffer overflow, information disclosure, Security bypass의 공격을 많다는 것을 확인하였다.

V. 모의실험 환경을 통한 취약점 분석

본 논문에서는 공격자로 가정하여 쇼단을 활용하여 Modbus 프로토콜을 탑재하고 있는 장비를 정찰 후에 장비의 초기 패스워드의 노출 위험성을 검증하였다.

5.1 산업제어시설의 취약점 확인 절차

Fig. 3.과 같이 공격자 관점에서 쇼단을 활용하여 Modbus 프로토콜 관련 내용을 검색 후 장비 이름 또는 제품명을 통하여 매뉴얼을 확인한다. 확인된 매뉴얼을 통해 제품 매뉴얼 내에 초기 패스워드가 있는지 검증하였다.

Table 7.과 같이 Shodan을 활용하여 검색된 Modbus /TCP 프로토콜을 탑재한 Anybus 장비의 경우 기본 패스워드를 확인하였고, 공격자 관점에서 활용될 수 있음으로 취약한 요소이다.

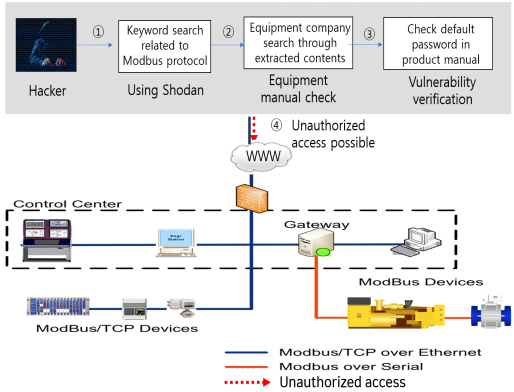

Fig. 3. Vulnerability Check Procedure of Industrial Control Equipment

Table 7. Default Password for Industrial Control Equipment applying Modbus/TCP

Company	Product	Port detection	Default Password
HMS	Anybus	502	admin

5.2 Modbus 테스트 환경 구성

Modbus 취약성을 진단하기 위해 PERA 아키텍처 환경을 고려 하여 전체적인 환경을 구성한 후 OT Zone 측면에서만 실험환경을 구성하였다.

Fig. 4.와 같이 PERA 아키텍처의 환경을 간략히 도식화하였으며 OT와 IT간 구분하며, 3개 영역과 6개 레벨로 구분하고 있다. 3개의 영역은 Enterprise Security Zone, Industrial Demilitarized Zone(IDMZ), Manufacturing Security Zone으로 크게 나누고, 6개의 레벨은 Level 4, 5의 엔터프라이즈 영역은 IT 영역이고, Level 0~3부분은 OT 영역이고, Level 0~2부분은 Cell/Area Zone 영역이다.

Fig. 5.와 같이 공격 방법은 ICS Cyber Kill Chain 모델의 공격 절차 방법론을 참고하여 Cell/Area(OT) Zone의 Level 0~2 사이 영역을 4단계로 분류한 후 Reconnaissance, Select the Target, Vulnerability Scan, Exploit 형태로 공격을 진행하였다.

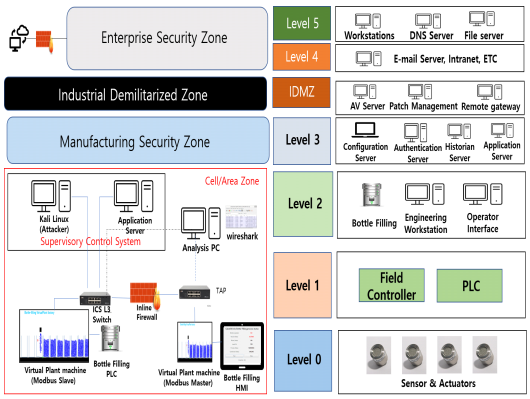

Fig. 4. Modbus Test Environment Configuration

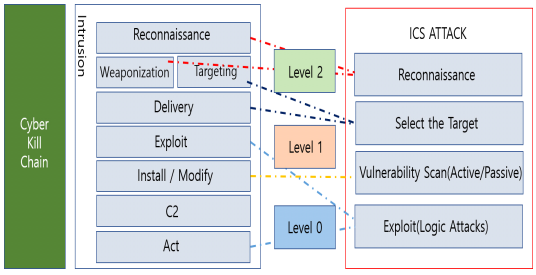

Fig. 5. ICS Attack Procedure

5.3 수행 절차

5.3.1 시뮬레이션 환경

Fig. 6.은 Virtual Plant 환경에서 Position Detect를 기준으로 빈 병에 음료를 넣는 공정인데 순차적으로 0.5초 간격으로 음료를 넣고 0.7초쯤에 다음 병에 음료를 담는 시뮬레이션 환경이다.

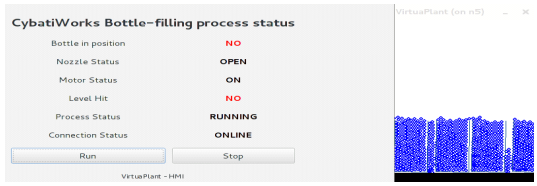

Fig. 6. Virtual Bottle Filling Process Simulation

5.3.2 진단 대상 선정

Table 8.은 Virtual Plant 환경에서 Modbus/TCP 프로토콜을 대상으로 취약점 대상으로 진행하였다.

Table 8. Selection of Diagnosis Target

Target	Content
Virtual Plant	Vulnerability identification of Modbus/TCP protocol using Virtual Plant

5.3.3 점검 도구

앞서 설명하였던 Fig. 4.와 같이 Virtual Plant ICS 환경을 가상으로 구성하여 Modbus/TCP 취약점을 진단하였다.

Table 9.은 Virtual Plant 환경에서 Modbus/TCP를 진행할 수 있는 도구를 선정하였다.

Table 9. Inspection Environment and Inspection Tools

Diagnostic tool	Content
Modbus Master	Modbus Sever
Modbus Slave	Modbus Client
Kali	Vunerability Tool through Attack Command
Wireshark	Open Source Tool for Traffic Analysis

5.3.4 진단 테스트 절차

Table 10.은 테스트 진단 절차로써 정찰, 대상선정, 스캐닝, 익스플로잇 형태로 순차적으로 진행하였다.

Table 10. Test Diagnostic Procedure

Step	Content
Reconnaissance	System Environment Analysis
Target	Modbus/TCP
Scanning	Scanning through Passive/Active
Exploit	Process Logic Attack

5.3.5 점검 결과

제어시스템의 시스템 점검 결과는 다음과 같다.

Fig. 7.과같이 시스템의 점검 결과는 80, 102 포트와 Modbus 프로토콜인 502 포트가 개방 되어 있는 것을 확인하였다.

Fig. 8.은 Wireshark를 통해 구동한 결과 Fig. 6.과 같이 “tcp.port == 502” 필터링을 하여 검색한 결과 여러 트래픽 중 Modbus를 추출하였다.

Fig. 9.는 Modbus의 정보를 상세 파악한 결과 Slave 장치의 Function Code 3번인 Read Holding Registers로서 장치의 메시지를 0~16까지의 주소에 접근한다는 것을 확인하였고 상세 데이터 값도 암호화가 되어 있지 않아 평문 노출되었다.

진행 중인 공정에서 취약점을 확인 후 패킷을 조작하여 4가지의 형태로 Move and Fill, Never Stop, Stop All, Stop and Fill을 진행하였다.

Fig. 10.~Fig. 14.를 살펴보면 HMI에서 정상적으로 프로그램은 구동되나 Logic Attack을 진행하는 순간 공정제어 담당자가 HMI에서는 Stop을 누르더라도 계속 진행하게 되는 것을 확인하였다. 분석결과, 인라인 방화벽에 Any, Any로 정책이 허용된 것을 확인하였다. 더불어 Modbus 프로토콜 보안에 있어 각 영역별 위협과 대응대책이 필요하다.

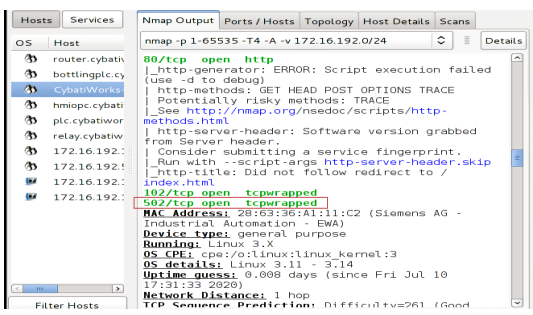

Fig. 7. System Info and Port Check

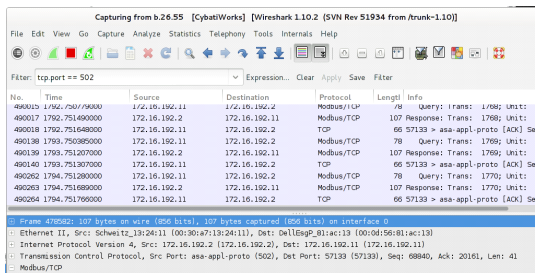

Fig. 8. Modbus/TCP Process

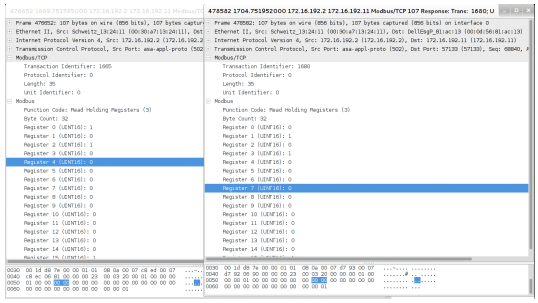

Fig. 9. Detailed of Modbus Information

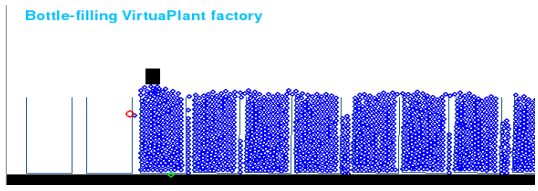

Fig. 10. Move and Fill

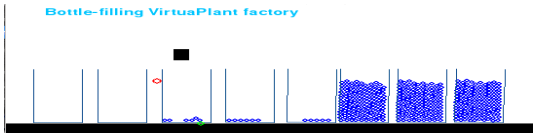

Fig. 11. Never Stop

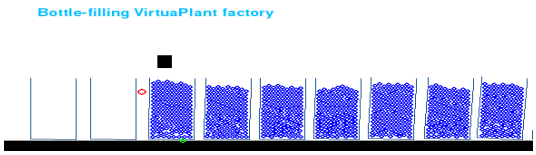

Fig. 12. Stop All

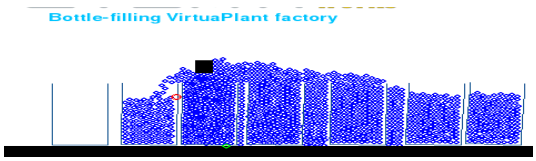

Fig. 13. Stop and Fill

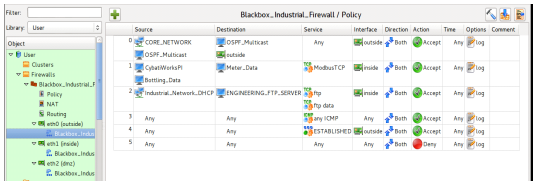

Fig. 14. Firewall Configuration

VI. 각 영역별 위협과 대응대책 방안

6.1 Enterprise Zone의 위협과 대응대책

Enterprise Zone 단에서는 IT 영역인 L4~L5에서의 위협과 대응책은 다음과 같다.

Table 11.은 Enterprise Zone의 위협과 대응책을 살펴본 결과 인터넷이 연결되는 곳이니 스피어 피싱이나 랜섬웨어의 공격을 사전에 방지할 필요가 있다. 이에 따라, 전산 담당자는 단말기 등의 바이러스 검사와 자산 관리 대상을 주기적으로 확인하여 자산의 최신성을 유지한다. 외부 검색엔진을 통해 내부 자산 정보가 검색되는지 확인한다.

6.2 Industrial DMZ Zone의 위협과 대응대책

IDMZ Zone 단에서는 IT/OT 영역인 L3.5에서의 위협과 대응책은 다음과 같다.

Table 11. Threats and Countermeasures in the Enterprise Zone

Risk Factor	Countermeasure
Spear phishing via Email	-Prohibit clicking on untrusted sites -Scan and repair PC virus with the latest updated vaccine -"Spam treatment" function setting for the sender address and domain -Prohibit disclosure of internal asset information and identity online
Ransomware against users and endpoints	-Prohibit disclosure of employee information on external Internet -Beware of visiting websites with weak security -Periodic inspection of asset management ledger

Table 12.은 IDMZ 존의 위협과 대응책을 살펴본 결과 외부에서 VPN(Virtual Private Network) 없이 직접 노출되어 원격 액세스 연결을 통해 OT 영역 내의 시스템에 악성코드가 삽입되거나 DDos 공격을 사전에 방어할 필요가 있다. 전산 담당자는 외부와의 연계가 있는 유지보수 시스템이 있는 경우 지정된 아이피와 명확히 지정하고 외부 검색엔진을 통해 공장 내의 시스템 정보나 포트 정보가 있는지 재차 확인이 필요하며, 방화벽 룰 점검 및 변경 관리 이력이 필요하며, 긴급할 때 사후조치를 위해 비상 연락망 체계 수립이 필요하다.

Table 12. Threats and Countermeasures in the IDMZ Zone

Risk Factor	Countermeasure
Systems exposed directly without VPN technology can be easily exploited	-Plant Firewall Check -ACL, IPS/IDS Check -Check whether the DMZ zone of the separated network is configured
Malware entering an organization's	-Remote desk remote check through external engine

Risk Factor	Countermeasure
OT network through remote access connections.	-When maintaining equipment in the OT area, it is necessary to clearly designate the sender and receiver in the firewall setting Enable IPS Need to prepare emergency contact network
DDos attack on remote access gateway	-Disable ICMP Echo -Check firewall rule settings Check -Emergency contact network required

6.3 Manufacturing Zone의 위협과 대응대책

Manufacturing Zone 단에서는 OT 영역인 L3에서의 위협과 대응책은 다음과 같다.

Table 13.는 Manufacuring Zone의 위협과 대응책을 살펴본 결과 엔드포인트의 랜섬웨어의 위협과 이 메일 통한 스피어 피싱(Spear Phishing) 및 비인가 USB로 인해 심각한 피해가 있으므로, 사전에 대응대책이 필요하다. 이에 전산 담당자는 외부 검색엔진을 통해 자산의 정보가 노출되었는지 재차 확인하고, 이메일의 경우에는 신뢰되지 않는 메일은 열지 말고, USB의 경우에는 반입절차를 확인하고 내부에서는 정보 자산 쪽에 USB Port Lock 설치를 권장한다.

Table 13. Threats and Countermeasure in the Manufacturing Zone

Risk Factor	Countermeasure
Ransomware on Endpoints	-Prohibit disclosure of employee information on external Internet -Beware of visiting websites with weak security -Periodic inspection of asset management ledger
Phishing via Email	-Prohibit clicking on untrusted sites -Scan and repair PC virus with the latest updated vaccine -Prohibit disclosure of internal asset information and identity online
Bot infections of the operator workstation	-In the firewall settings, specify the IP sent from the worker workstation to the PLC
Unsecured USB Ports	-Security USB Port Lock installation recommended -Equipment and mobile media carry-in/out-of-country list check

6.4 Cell/Area Zone의 위협과 대응대책

OT 영역 내의 Cell/Area Zone 단에서는 Level 0~2 에서의 위협과 대응책은 다음과 같다.

Table 14.은 Cell/Area Zone의 위협과 대응책을 살펴본 결과 산업스파이를 통해 산업공정에 대해 생산설비의 직접적인 시설 파괴 장애 등(사보타주)이 발생될 수 있으므로 사전 예방대책이 필요하다. 이중 가장 이슈가 되고 요소는 기운용되고 있는 제어 설비의 경우 산업 특화용으로 개발된 프로토콜로 개발되어 인증, 권한, 암호화의 설계 부족으로 악의적인 공격을 진행할 수 있어 해당 시스템의 관리가 필요하다. 이에 지정된 업무 담당자만 제어할 수 있게 진행하고 특화된 Modbus 프로토콜인 502 포트가 노출되었는지 주기적인 확인이 필요하다. 외산 벤더의 경우 이슈가 발생할 경우 Modbus 보안프로토콜을 패치 하거나 미흡한 설정을 벤더 사에 요청하여 개선 조치한다. 다만, 가용중인 시스템이 대다수이고 설정값을 변경시마다 비용이 크게 들어가서 조치가 쉽지 않다.

이에 전산 담당자는 502 포트를 외부에서 내부로 노출되어 있는지를 점검하고, 예방 차원에서 OT 영역 내에서 방화벽 설정을 송신자와 수신자를 명확히 지정하고 악의적인 트래픽을 차단하기 위해 네트워크 트래픽 이상 탐지 도구이나 통합 보안 관리 도구를 통한 이상 징후 트래픽 분석 시스템이 필요하다.

중장기적으로는 예산 확보를 통해 솔루션 도입을 하거나 오픈소스를 활용하여 이상 징후 솔루션 구축을 통해 비정상 트래픽 예방 검토가 필요하다.

본 장에서는 국제 자동화 협회의 ISA99 위원회에서 개발된 ISA/IEC 62443 표준[19]과 ISO/IEC 27002

Table 14. Threats and Countermeasures in the Cell/Area Zone

Risk Factor	Countermeasure
Industrial spy	-Confirm that only designated personnel are authorized to OT area
Sabotage	-In the firewall settings, specify the IP sent from the worker workstation to the PLC. -Protect vulnerable systems with virtual patches instead of patching physical systems with gateways running IPS
Unwanted modifications to the industrial process	-Make sure that only the SCADA protocol is shown in Level 1. -Identify the EOS system and recommend a patch.
Self-defect of industrial control protocol - lack of authentication - lack of authority - lack of encryption	-Traffic analysis through SEIM monitoring -IDS Monitering
Complicated procedures for system patching or technical support in use as products from foreign vendors	-Traffic analysis through SEIM monitoring -IDS Monitering -Periodically check whether port 502 is exposed to external search engines -In the firewall settings, specify the IP sent from the worker workstation to the PLC

국제표준[20]을 검토하여 발간된 '스마트 공장 최소보안 가이드(2016)'[21]와 '스마트 공장 사이버보안 가이드(2019)'[22]를 바탕으로 5장에서 언급한 영역별 위협요소와 대응대책을 토대로 중소기업의 전산 담당자가 할 수 있는 범위 내에서 물리적, 관리적, 기술적 보안을 포괄적으로 손쉽게 점검할 수 있는 보안 체크리스트를 제시하고 전문가 집단을 통해 보안 체크리스트의 적정성을 검증하고자 한다.

Table 15.와 같이 스마트 공장의 보안 체크리스트는 만들어져 있으나, 스마트 공장의 일반적인 기본 요건이나 기본준수사항만 있다. 중소기업 담당자 관점에서는 특화된 산업제어 프로토콜인 Modbus와 같은 점검을 하는데 있어 지식이 다소 부족한 상태이다. 또한, 예방관점에서 공장시스템 침해사고 관리 부분에서는 비상 연락망을 추가로 보안 체크리스트에 포함하여 제안하였다. 또한, 공장시스템 개발 보안 부분에서도 점검자의 관점에서 해당 항목을 제외하였고 개인정보의 항목은 Modbus 프로토콜의 점검 관점이므로 개인정보 부분은 제외하였다. 이에 따라 경영보안과 기술보안을 참고하고 앞서 본 6장에서 언급한 영역별로 위협과 대응대책을 제시한 근거를 바탕으로 보안 체크리스트를 제시한다.

Table 15. Smart Factory Security Checklist Control Items that can be Performed by the Computer Managers

Classification	Control Area	Control Item	Computing person in charge
Business security (9)	Organization & Regulation	5	-Inventory identification (Physical,1)
	Facility, facility, equipment and media security	4	-Access control Half access to equipment and media (Physical,2)
Technology security (16)	Factory system access authority management	7	-Password management (Managerial,1) -Firewall rule inspection and change management (Managerial,2)
	Factory system operation security	6	-Remote access control (Technical, 1) -Public server security (Technical, 1) -Malware control (Technical, 1) -Log management and

Classification	Control Area	Control Item	Computing person in charge
			monitoring (Technical, 3)
	Factory system development security	1	N/A
	Factory system infringement accident management	1	-Additional suggestions: Emergency contact network establishment (Managerial,1)
	Privacy	1	N/A

Table 16.는 정보보안의 3요소 (CIA: Confidentiality(기밀성), Integrity(무결성), Availability(가용성)) 기준으로 중소기업의 전산 담당자가 최소한의 점검을 할 수 있는 내용으로 도출하였다. 점검기준은 9개를 선정하였고, 보안 체크리스트는 20개로 선정하였다. 선정된 보안 체크리스트 기준으로 설문 조사 도구(구글 폼)를 사용하여 동종 분야별 정보보안 전문가들을 통해서 설문 조사를 진행하였고, 설문 조사 기간은 2021.02.04.~02.15일(12일)까지 진행하였다. 총 35명이 설문 조사에 참여하였다. 전문가들의 응답 결과를 분석한 결과 중소기업 담당자들이 최소한의 보안 체크리스트가 필요하다는 것을 설문 조사를 통해 입증하였고, 설문 조사에 참여한 직무 관련 업무 분야는 다음과 같다.

Table 16. Industrial Security Checklist for Small and Medium Business Computer Managers

Classification	Control Item	Checklist
Physical Security	Direct and indirect facility destruction (sabotage)	-Has the authorized person properly controlled access to the protected area?
	Equipment and media access management	-Do internal/external persons manage carry-in/in/out control for equipment and moving storage media? -Is the USB Port Lock installed on the internal or external system?
Managerial Security	Inventory identification	-Is the identification and classification of assets in the company periodically checked?
	Firewall Policy	-Do you check the firewall rules of the information protection system or control system? -Are changes to the firewall policy being managed?
	Password Management	-Are you establishing and implementing secure user password management procedures for information systems and information protection systems? -Is the password of the control system exposed to the outside?
	Infringement accident	-Are you establishing and implementing an emergency contact network system to prevent factory infringement accidents?

Classification	Control Item	Checklist
Technical Security	Basic Check	-Did you conduct a vaccine test on the internally operating system? -Do you check security patches to respond to vulnerabilities to known malware or viruses in the system? Have you checked whether the ping of the core control system is blocked?
	Remote access control	-When operating the system remotely through internal/external networks, have you checked whether access is allowed only to specific terminals? -Did you check whether the information of the control system (plain text exposure) is exposed to the outside through the vulnerability tool? -Has the external search engine checked whether the keyword related to Modbus and port 502 were exposed?
	Log management and monitoring	-Do you establish and check log management procedures for the control system? -Did you review the sender and receiver of the designated system in the OT area? -Are you monitoring various system activities (information access, authentication, data transmission traffic)?

Fig. 15.와 같이 정보보호에 해당하는 6개 업무 분야를 기준으로 설문 조사를 진행하였고, 가장 참여가 많았던 업무 분야는 정보보호 컨설팅(40%)과 정보보호 운영(34.3%)전문가들이 많았으며, 그다음으로 정보보호 관리자와 정보보호 구축 전문가들이 22.9%를 차지하였다. 마지막으로, 정보보호 인증 전문가와 정보보호 보안감사자(8.6%)들이 설문 조사에 참여하였다. 설문 조사에 참여한 정보보안 분야의 경력 연수는 다음과 같다.

Fig. 16.은 설문 검증에 참여한 정보보호 전문가들의 근무경력을 분석한 결과 정보보호 분야에서 10년 이상(74.3%) 근무한 경력자들이 참여한 것이 해당 설문조사의 신뢰도 측면에서도 충분하다고 판단하였다. 그다음으로 5년 이상~10년 이하의 전문가가 14.3%를 응답하였고, 3년 이상~5년 이하의 경우에는 11.4%가 응답하였고, 1년 이상~3년 이하의 경우에는 설문 조사에 참여가 없었다. 더불어 보안 체크리스트를 종합적으로 분석한 결과는

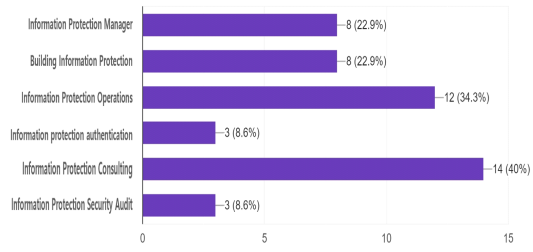

Fig. 15. Job-related work areas

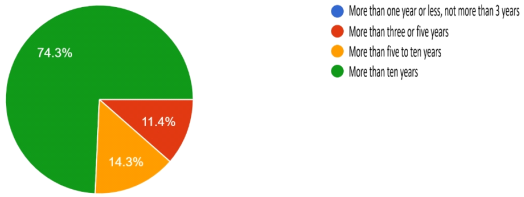

Fig. 16. The Number of years in Information Security Work

다음과 같다.

Table 17.을 확인 결과 각 영역별 보안 체크리스트가 적합하다는 것을 확인하였다. 세부적으로 살펴보면, 점검기준의 보안 체크리스트 상세 항목 결과는 다음과 같다.

Table 17. Validity of the Security Checklist

Classification	Control Item	Suitable	Not Suitable
Physical Security	Direct and indirect facility destruction (sabotage)Direct and indirect facility destruction (sabotage)	100%	0%
	Equipment and media access management	100%	0%
	Inventory identification	100%	0%
Managerial Security	Firewall Policy	100%	0%
	Password Management	100%	0%
	Infringement accident	100%	0%
Technical Security	Basic Check	100%	0%
	Remote access control	100%	0%
	Log management and monitoring	100%	0%

Table 18.을 살펴보면 9개 점검 영역별로 20개의 보안 체크리스트를 확인 결과, 전체적으로 보안 체크리스트의 타당성이 합당하다는 것이 입증하였다. 종합적으로 중소기업을 위한 보안 체크리스트의 타당성을 확인하기 위해 담당자들이 업무관점의 실용성 검증은 다음과 같다.

Table 18. Security Checklist Result of Certification Criteria

Control Item	Checklist	Suitable	Not Suitable
Direct and indirect facility destruction (sabotage)	-Has the authorized person properly controlled access to the protected area?	100%	0%
Equipment and media access management	-Do internal/external persons manage carry-in/in/out control for equipment and moving storage media?	100%	0%
	-Is the USB Port Lock installed on the internal or external system?	91%	9%
Inventory identification	-Is the identification and classification of assets in the company periodically checked?	100%	0%
Firewall Policy	-Do you check the firewall rules of the information	100%	0%

Control Item	Checklist	Suitable	Not Suitable
	protection system or control system?		
	-Are changes to the firewall policy being managed?	94%	6%
Password Management	-Are you establishing and implementing secure user password management procedures for information systems and information protection systems?	97%	3%
	-Is the password of the control system exposed to the outside?	74%	26%
Infringement accident	-Are you establishing and implementing an emergency contact network system to prevent factory infringement accidents?	97%	3%
Basic Check	Did you conduct a vaccine test on the internally operating system?	94%	6%
	-Do you check security patches to respond to vulnerabilities to known malware or viruses in the system?	100%	0%
	-Have you checked whether the ping of the core control system is blocked?	91%	9%
Remote access control	-When operating the system remotely through internal/external networks, have you checked whether access is allowed only to specific terminals?	97%	3%
	-Did you check whether the information of the control system (plain text exposure) is exposed to the outside through the vulnerability tool?	94%	6%
	-Has the external search engine checked whether the keyword related to	85%	15%

Control Item	Checklist	Suitable	Not Suitable
	Modbus and port 502 were exposed?		
Log management and monitoring	-Do you establish and check log management procedures for the control system?	97%	3%
	-Did you review the sender and receiver of the designated system in the OT area?	88%	12%
	-Are you monitoring various system activities (information access, authentication, data transmission traffic)?	91%	9%

Table 19.와 같이 보안 체크리스트 도출을 통해 담당자들이 업무관점에서 도움 된다는 응답이 97% 임을 확인하였고, 이에 보안 체크리스트의 실용성이 적합함을 입증하였다. 더불어, 보안 체크리스트를 통해 기업의 보안성 향상 측면에서의 조사 결과는 다음과 같다.

Table 19. Practicality of the Security Checklist

Control Item	Suitable	Not Suitable
Checking the practicality of improving corporate security through a security checklist through verification	97%	3%

Table 20. Verification of Corporate Security Improvement through Security Checklist

Control Item	Suitable	Not Suitable
Whether the security of the enterprise is improved through the security checklist through verification	100%	0%

Table 20.을 살펴보면, 정보보호전문가 35명의 만장일치로 보안 체크리스트를 통해 기업의 보안성 향상의 적합하다는 것을 확인하였다. 이를 통해, 중소기업에서 활용할 수 있는 보안 체크리스트가 실용성과 활용성에 전반적으로 도움 된다는 것을 확인하였다. 도출된 체크리스트를 통해 전문가가 아닌 국내 중소기업의 전산 담당자가 손쉽게 사용할 수 최소한의 보안 체크리스트를 활용할 것이다.

VII. 결 론

본 연구는 기존 연구들과 다르게 재검증과 실제 일어날 수 있는 위험성을 도출하였고, 전문가 집단 검증을 통해 보안 체크리스트의 실용성과 적정성을 검증하였다. 이에 국내 중소기업의 전산 담당자가 기본적인 내용을 쉽게 적용할 수 있는 보안 체크리스트가 개발하였다. 추후 연구로는 다양한 산업 분야의 특화된 프로토콜의 연구를 통하여 여러 분야의 종사자들이 도움이 될 수 있는 대책 방안을 지속적으로 연구하고자 한다.

References

[1] wikipedia, “modbus” https://en.wikipedia.org/wiki/Modbus,Dec. 2020.
[2] Ministry of SMEs and Startups, https://www.mss.go.kr/site/smba/ex/bbs/View.do?cbIdx=86&bcIdx=1009410&parentSeq=1009410, Dec. 2018.
[3] I. N. Fovino, A. Carcano, M. Masera and A. Trombetta, “Design and im-

plementation of a secure modbus protocol," Critical Infrastructure Protection III, Springer Berlin Heidelberg, vol. 311, pp. 83 - 96, 2009.
[4] Shodan ICS Radar, https://ics-radar.shodan.io, Feb., 2020
[5] National Vulnerability Database, "modbus" https://nvd.nist.gov/vuln/search, Feb. 2020.
[6] Mitre CVE, "modbus" http://https://cve.mitre.org/data/downloads/index.html, Feb. 2020.
[7] IBM X-force Exchange, "modbus" https://exchange.xforce.ibmcloud.com, Feb., 2020.
[8] Purdue Enterprise Reference Architecture, https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture, Feb. 2020.
[9] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, "Attack taxonomies for the Modbus protocols," International Journal of Critical Infrastructure Protection, vol. 1, pp. 37-44, Dec. 2008.
[10] Jae-gu Song, Sungmo Jung, Seoksoo Kim, Taihoon Kim, Dong-Ju Kang, Seok Ju Kim, "Design of Hacking Test System for Modbus based SCADA", Korean institute of information Technology, vol. 7, no. 5, pp. 183~190, Oct. 2009.
[11] Jong-Joo Lee · Seog-Joo Kim · Dong-Joo Kang, "A SCADA Testbed Implementation Architecture for Security Assessment", Journal of the Korean Institute of IIIuminating and Electrical Installation Engineers, vol. 24(4), pp. 50-56, Jan. 2010.
[12] Yoo, Hyunguk, Yun, Jeong-Han, Shon, Taeshik, "Whitelist-Based Anomaly Detection for Industrial Control System Security", The Journal of Korea Information and Communications Society, vol. 38B(8), pp. 641-653, Aug. 2013.
[13] Hyun-Seok Kim · Dong-Gue Park "Implementation of abnormal behavior detection system based packet analysis for industrial control system security", Journal of the Korea Academia-Industrial, vol.19(4). pp. 47-56, Apr. 2018.
[14] Modbus Organization, "MODBUS Application Protocol Specification V1.1b3", pp.2, Apr. 2012.
[15] Dailysecu, "Deadly loopholes in the SCADA system revealed... Easily hacked" https://www.dailysecu.com/news/articleView.html?idxno=992, Nov. 2011.
[16] Boannews, "The control facility network is no longer a "safe zone" https://www.boannews.com/media/view.asp?idx=45439, Mar. 2015.
[17] Boannews, "[OT Security Report-3] Concentrated Dissection of Cyber Security Solutions in Smart Factory" https://www.boannews.com/media/view.asp?idx=93087&kind=3, Dec. 2020.
[18] ITWORLD, "ICS weaknesses revealed by protocol gateway flaws... Trend Micro Presentation at Black Hat Conference" https://www.itworld.co.kr/t/63417/%EC%82%AC%EB%AC%BC%EC%9D%B8%ED%84%B0%EB%84%B7/160645, Aug. 2020.
[19] ISA, "Quick Start Guide: An Overview of the ISA/IEC 62443 Standards", https://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards, Jun. 2020.
[20] ISO/IEC 27002, "Information Technology-Security Techniques-Code of practice for information security controls", Second edition, Oct, 2013.
[21] Smart Manufacturing Standardization Forum, "Smart Factory Minimum Security Guide",http://smartforum.or.kr/policy/policy_read.html?seq=46&page=1, Sep, 2016.
[22] KISA, "Smart Factory Cyber Security Guide", Dec, 2019.

〈저자소개〉

유 정 훈 (Jung-hoon Yoo) 정회원
2015년 8월: 건국대학교 정보보안학과 석사
2017년 8월~현재: 수원대학교 컴퓨터학과 박사수료
2020년 2월~현재: 클라우드그램(주) PS팀 재직, CISSP
〈관심분야〉 개인정보보호 및 정보보호관리체계, IoT, 산업보안, 클라우드컴퓨팅

배 춘 석 (Chun-sock Bae) 정회원
1993년 2월: 전남대학교 경영학과 학사
2017년 2월: 건국대학교 정보보안학과 석사
2021년 2월: 수원대학교 컴퓨터학과 박사
1993년 4월~현재: ㈜LG CNS 클라우드아키텍처팀 재직, 정보관리기술사(2008)
〈관심분야〉 정보보호, 데이터센터 구축 및 운영, 클라우드컴퓨팅

고 승 철 (Sung-cheol Goh) 종신회원
1981년 2월: 연세대학교 수학과 학사
1983년 2월: 연세대학교 수학과 석사
1992년 8월: 포항공과대학교 수학과 박사
2011년 9월~현재: 수원대학교 정보보호학과 교수
〈관심분야〉 정보보호, 국방사이버보안, 암호학, 클라우드컴퓨팅