The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 3, pp.153-161, Jun. 30, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.3.153
JIIBC 2020-3-22

산업용 네트워크 장비와 보안 장비의 특징 분석

Characteristic Analysis of Industrial Network and Security Equipment

신동진[*], 황승연[**], 오재곤[***], 김정준[****], 이용수[*****], 박경원[******]

Dong-Jin Shin[*], Seung-Yeon Hwang[**], Oh Jae-Kon[***], Jeong-Joon Kim[****], Yong-Soo Lee[*****], Kyung-won Park[******]

요 약 최근 4차 산업혁명의 발전으로 인해 AI, IoT, Cloud, Big Data 등 다양한 기술을 유기적으로 연결한 스마트공장이 증가하고 있다. 이를 바탕으로 내부 공정이 자동 제어되는 산업환경에서 PLC와 같은 기기 제어에 필요한 결정성과 악의적인 공격에 의해 스마트공장의 내부 공정이 멈추게 되었을 때 발생하는 손실에 대한 고가용성이 확보되어야 한다. 다양한 산업 분야에서 사용되는 산업용 네트워크 장비와 보안 장비에 대한 조사 및 분석은 국가 기반시설에서 산업용 제어시스템의 효율성과 활용성을 높여줄 수 있고, 나아가 관련 인프라 구축에 중요한 피드백을 제공할 수 있다. 따라서 본 논문에서는 산업용 네트워크 장비와 보안 장비를 다양한 측면에서 비교 분석하였으며, 본 논문의 결과를 기반으로 산업용 네트워크 장비와 산업용 보안 장비의 관련 기술 개발 로드맵으로 활용될 수 있을 것이라 예상된다.

Abstract Due to the recent development of the 4th industrial revolution, Smart Factories that organically link various technologies such as AI, IoT, Cloud, and Big Data are increasing. Based on this, in the industrial environment where the internal process is controlled automatically, high availability should be secured against the loss caused when the internal process of the Smart Factory is stopped due to the determinism and malicious attack necessary to control the device such as PLC. The research and analysis of industrial network equipment and security equipment used in various industries can improve the efficiency and usability of industrial control systems in national infrastructure and can provide important feedback to build related infrastructure. Therefore, we compared industrial network equipment and security equipment in this paper in a variety of ways and expect to be used as a roadmap for developing technologies for industrial network equipment and industrial security equipment based on the results of this paper.

Key Words : Smart Factories, Industrial Network Equipment, Industrial Security Equipment,

[*]준회원, 안양대학교 ICT 융합공학부 대학원생
[**]준회원, 안양대학교 ICT 융합공학부 대학원생
[***]정회원, ㈜진우산전 이사
[****]정회원, 안양대학교 ICT 융합공학부 조교수
[*****]정회원, 여주대학교 소프트웨어융합과 교수
[******]정회원, 한국산업기술대학교 컴퓨터공학부 조교수
접수일자 2020년 3월 12일, 수정완료 2020년 5월 1일
게재확정일자 2020년 6월 5일

Received: 12 March, 2020 / Revised: 1 May, 2020 / Accepted: 5 June, 2020
[*****]Corresponding Author: chrisndanny@kpu.ac.kr
Dept. of Computer Engineering, Korea Polytechnic University, Korea.

Ⅰ. 서 론

최근 제조업 혁신에 따른 스마트공장이 이슈화되면서 산업용 네트워크 기술의 관심이 높아지고 있다[1]. 산업용 네트워크 장비와 보안 장비는 스마트공장 등 제조업의 산업 현장에서 생성되는 많은 데이터를 안전하고 정확하게 전달하여야 하며, 데이터 손실 및 외부 침입 방지에 필요하다[2]. 하지만 스마트공장의 규모와 환경이 각각 다르며, 일반 IT 환경의 네트워크 장비와 보안 장비는 산업제어시스템의 특성을 고려하지 않기 때문에 효율적인 산업제어시스템의 운영 및 관리를 위해서 산업용 네트워크 장비와 보안 장비의 현황을 조사하고, IT 환경의 유사 장비와 특징 및 기술 비교·분석이 필요하다. 또한, 국내외 IT 환경의 네트워크 장비와 보안 장비 기술 분석 연구개발 사례는 있으나 산업용 네트워크 장비와 보안 장비 기술 분석 연구개발 사례는 미비한 상황이다.

따라서 산업용 네트워크 장비와 보안 장비 기술을 IT 환경의 유사 장비와 비교 분석하여 국가 인프라 시설 및 산업 시설 보안을 위한 장비 선정 및 네트워크 아키텍처 구성의 가이드라인을 제시하고자 한다.

본 논문의 2장에서는 다양한 네트워크 장비 중 스위치와 보안 장비에서 사용되는 장비를 설명하고, 3장에서는 IT와 산업용에서 사용되는 스위치에 대하여 비교 및 분석한다. 4장에서는 IT와 산업용에서 사용되는 방화벽에 대하여 비교 및 분석하고, 마지막 5장에서 결론을 설명한다.

Ⅱ. 관련 연구

IT 네트워크의 주요 장비 중 스위치는 OSI 계층 중 2 Layer에 위치하며, 전달되는 패킷의 대상 주소를 기반으로 하여 모든 포트로 전송하지 않고, 각 패킷을 원본 포트에서 특정 대상 포트로만 전송하기 때문에 다른 포트와 충돌을 피하여 전체적인 네트워크 처리량을 향상한다[3]. 관련 기술이나 제품을 개발하는 회사로는 Cisco, Huawei, HPE(Hewlett Packard Enterprise), juniper가 대표적이다[4].

산업용 네트워크 장비는 IT 스위치 장비를 산업환경에 적합하게 개량한 장비로 기존 이더넷 환경에서 취약점인 시간 결정성, 실시간성, 토폴러지 문제를 개선하고, 기존에 쓰이던 산업용 네트워크 기술을 접목한 장비이다[5]. 관련 기술이나 제품을 개발하는 회사로는 Siemens, Rockwell, Schneider, Beckhoff, Cisco, Moxa가 대표적이다[6].

산업용 스위치는 관리형 스위치(Managed Switch와 비관리형 스위치(Unmanaged Switch) 두 가지로 구분되고, 관리형 스위치는 네트워크 장비의 정보 수집, 구성 및 모니터링에 사용되는 SNMP(Simple Network Management Protocol)을 지원할 수 있으며, 비관리형 스위치는 단순히 LED를 통해 네트워크 연결을 표시한다. 산업용 스위치 장비는 포트 미러링(Port Mirroring), 이중화(Redundancy), QoS(Quality of Service), IGMP(Internet Group Management Protocol) 등과 같은 다양한 기능을 갖추고 있고, 또한 높은 온도와 같은 요구사항을 만족하여야 한다[7].

산업용 보안 장비는 산업에서 사용되는 기밀 데이터를 보안 측면에서 방어하기 위해 필요한 장비이다. 주요 장비는 산업용 방화벽, 데이터 다이오드, ICS(Industrial Control System) Anomaly Detection이 대표적인 장비 유형이다. 산업용 방화벽은 접근제어를 이용한 외부 침입에 방어 및 내부 정보유출 방지를 위한 장비이고, 데이터 다이오드는 일 방향 전송 장비로 보안영역(제어망)에서 비 보안영역(업무망)으로만 데이터를 일 방향으로 전송하며, 안전한 망을 구성하여 사이버 침해행위를 방지하기 위한 장비이며, ICS Anomaly Detection는 정상적인 트래픽과 비정상적인 트래픽을 탐지하여 정상과 비정상 트래픽을 구분하기 위한 장비이다[8]. 관련 기술이나 제품을 개발하는 회사로는 Siemens, Tofino, Cisco, Palo Alto Networks, Check Point, Fortinet, Symantec, GE OpShield, 3eTI가 대표적이다[9].

Ⅲ. IT 및 산업용 스위치 비교

IT 네트워크 장비와 산업용 네트워크 장비에는 스위치, 라우터, 게이트웨이 등 다양한 장비가 존재하고, 이 중에서 스위치 장비를 선정하였으며, IT 스위치 장비의 모델은 Cisco 3850, 산업용 스위치 장비의 모델은 Cisco IE-4000, Moxa EDS-P510A, Siemens X-414로 선정하여 환경 측면, 관리 측면, 제어프로토콜 측면 3가지로 정리하여 기술 분석하였다[10-13].

1. 환경 측면

IT 스위치 장비와 산업용 스위치 장비는 환경적 측면에서 큰 차이를 가지고 있다. 산업용 스위치 장비는 다음 표 1과 같이 크기, 설치방법, 무팬, 온도, 충격과 진동에

표 1. IT 스위치와 산업용 스위치 환경 측면 비교표
Table 1. IT Switch and Industrial Switch Environment Comparison

모델명 / 비교항목		IT 스위치 장비	산업용 스위치 장비		
		Cisco 3850	Cisco IE-4000	MOXA EDS-P510A	SIEMENS X-414
Dimensions (H x W x D)		4.45 x 44.5 x 45.0cm	15.0 x 15.5 x 12.9cm	7.9 x 13.5 x 10.5cm	34.4 x 14.5 x 11.7cm
Installation		Rack-mount kits	DIN-Rail mount kit	DIN-rail mounting	35 mm DIN-rail
Fanless		X	O	O	O
Operating environment		-5 to +45C	-40 to +75C	-40 to +75C	-40C to + 70C
		Altitude 3,048m	Altitude 4,000m	Altitude 2,000m	Altitude 2,000m
Storage environment		-40 to +75C	-40 to +85C	-40 to +85C	-40 to +80C
		Altitude 4,000m	Altitude 4,000m	Altiude 2,000m	Altitude 2,000m
Shock	Operating	30G, 2ms	50G, 11ms	IEC 60068-2-27	-
	Non-Operating	55G, 2ms	65-80G, 9ms		
Vibration	Operating	0.41Grms from 3 to 500Hz	IEC 60068-2-6 IEC 60068-2-64 EN 61373	IEC 60068-2-6	10G 이상
	Non-Operating	1.12Grms from 3 to 500Hz	IEC 60068-2-6 IEC 60068-2-64 EN 61373		

대한 요구사항을 만족하기 때문에 산업환경의 까다로운 조건에서 사용될 수 있다.

IT 스위치 장비는 일반적으로 Rack 마운트에 맞춘 크기로 제작되며, 산업용 스위치 장비는 DIN-Rail을 사용할 수 있는 구조의 특징을 가지고 있다. 산업용 스위치 장비의 크기는 포트 수에 따라 차이가 있으며 IT 스위치 장비보다 작은 구조를 갖추고 있다.

IT 스위치 장비는 팬을 통한 공랭식 구조의 냉각 방법을 채택하고 있으나, 산업용 스위치 장비는 외부로 돌출된 방열판과 구리로 만들어진 히트 파이프를 통한 공랭식 구조를 채택하기 때문에 내부 공간의 효율성을 확보할 수 있다.

산업용 스위치 장비는 IT 스위치 장비보다 약 -40℃의 저온과 +75℃의 고온에서도 가동할 수 있으며, 고도 2000m 이상의 저압 환경에서 사용이 가능하다. 제철소, 정유공장, 냉동 창고 등의 온도에 영향을 많이 받는 환경과 비행기 실내 네트워크나 고원지대의 공장 등에서 산업용 스위치 장비가 활용될 수 있다.

MOXA와 SIEMENS에서 제공하는 문서에서 충격과 관련된 표준은 IEC 60008-2-27에 정의되어 있으며, 산업용 스위치 장비는 IT 스위치 장비에 비해 강한 충격에 견딜 수 있다.

진동과 관련된 표준은 IEC 60068-2-6, IEC 60068-2-64, EN 61373에 정의되어 있으며, 산업용 스위치 장비는 표준을 준수하여 제작되기 때문에 IT 스위치 장비보다 진동이 더 심한 철도, 발전소, 송전소, 중장비 제조 등에서 사용될 수 있다.

2. 관리 측면

관리적 측면에서 IT 스위치 장비와 산업용 스위치 장비는 큰 차이를 가지고 있다. 관리적 측면을 비교한 항목은 MTBF, Alarm, POE(Power of Ethernet), Port Mirroring 항목이며, 비교는 표 2와 같다.

표 2. IT 스위치와 산업용 스위치 관리 측면 비교표
Table 2. IT Switch and Industrial Switch Management Side Comparison

모델명 / 비교항목	IT	산업용		
	Cisco C3850	Cisco IE-4000	MOXA EDS-P510A	SIEMENS X-414
MTBF	315,840	558,310	710,166	210,240
Alarm	X	O	O	O
PoE	X	O	O	O
Port Mirroring	O	O	O	O

산업용 스위치 장비는 긴 MTBF 시간을 통해 장비를 오랫동안 가동할 수 있기 때문에 가용성이 좋다. 알람 기능은 네트워크 단선과 같은 장비의 이상 현상 발생 시 알람 신호를 발생하여 관리자에게 즉시 통보가 가능하기 때문에 장비의 이상 유무를 쉽게 판별할 수 있다. 또한, PoE 기능을 통한 이더넷 선을 통해 장비의 전원을 공급

받을 수 있으며, 포트미러링은 선택 포트의 모든 프레임을 원하는 다른 포트로도 모니터링 할 수 있는 리다이렉션 기능을 제공한다.

3. 제어프로토콜 측면

IT 스위치 장비는 산업용 제어프로토콜을 지원하지 않으며, 산업용 스위치 장비의 제어프로토콜은 결정성, 유연성, 확장성 세 가지 특징을 가지고 있다[14].

결정성은 산업환경에서 사용되는 기기 간에 데이터 패킷을 정해진 반응 시간 내에 전송 및 수신하는 것을 의미한다. 반응 시간은 제어프로토콜의 종류에 따라 달라지고, 평균적인 기기 제어에 필요한 반응 시간은 100ms 이하이다. 산업환경에서 기기 간에 데이터가 손실되거나 데이터 전송이 지연되면 제조 공정에서 심각한 결함이 발생하기 때문에 결정성은 산업용 스위치 장비에서 중요한 요소이다.

유연성은 산업용 스위치 장비에서 지원하는 이중화 프로토콜(Moxa의 Turbo Ring, Turbo Chain, Cisco의 REP)과 특정 제어프로토콜에서 지원하는 이중화 프로토콜(PROFINET의 MRP)을 이용하여 다양한 토폴로지를 구성하는 것을 의미한다. 즉, 산업환경의 제어 및 자동화 시스템에 문제가 생겼을 때 신속하게 복구할 수 있는 기능을 의미한다.

확장성은 산업환경의 제어 및 자동화 시스템에 사용되는 실시간 이더넷 환경에서 PLC부터 I/O 및 센서까지에 이르는 전반적인 다수의 기기에 대한 연결성을 의미한다. 기존 필드버스에서 제한되던 기기의 연결 개수를 실시간 이더넷이 적용된 산업용 스위치 장비의 제어프로토콜을 이용하면 필드버스에서 가능한 연결 개수보다 더 많이 연결할 수 있으며, 산업환경에서 더욱더 효율적으로 운영할 수 있다.

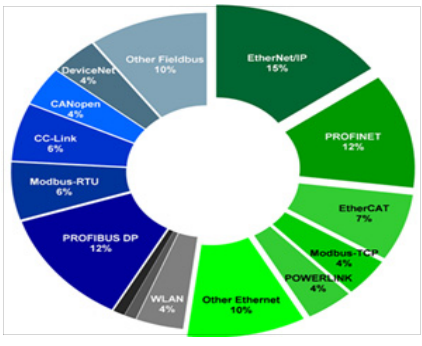


그림 1. 산업용 이더넷 제어프로토콜 점유율[15]
Fig. 1. Industrial Ethernet ControlProtocol Share

그림 1은 산업용 이더넷에서 사용되는 다양한 제어프로토콜의 종류와 점유율을 나타내고, EtherNet/IP는 전체 시장의 15%를 차지하면서 가장 큰 점유율을 차지하고 있으며, PROFINET, EtherCAT, Modbus-TCP, POWERLINK 등이 그 뒤를 따르고 있다[15]. 따라서 다양한 산업용 제어프로토콜이 현재 산업용 이더넷에서 사용되고 있는 것을 확인할 수 있다.

표 3. IT 스위치와 산업용 스위치 제어프로토콜 지원 비교표
Table 3. IT Switch and Industrial Switch Control Protocol Support Comparison

모델명 / 프로토콜	IT	산업용		
	Cisco C3850	Cisco IE-4000	MOXA EDS-P510A	SIEMENS X-414
Modbus-TCP	X	O	O	X
EtherNet/IP	X	O	O	X
PROFINET	X	△	X	0

IT 스위치 장비인 Cisco C3850은 제어프로토콜을 지원하지 않는다. 산업용 스위치 장비인 Cisco IE 4000은 Modbus-TCP, EtherNet/IP, PROFINET에서 IRT (Isochronous Real Time)를 제외한 NRT(Non Real Time), SRT(Soft Real Time)만 지원하고, Moxa P510A의 경우 Modbus-TCP, EtherNet/IP를 지원하며, Siemens X-414 제품의 경우 PROFINET에서 NRT, SRT, IRT를 지원한다. 본 논문에서 제어프로토콜 용도에 대한 비교 분석은 장비에서 지원하는 EtherNet/IP, Modbus-TCP, PROFINET만 분석하였다.

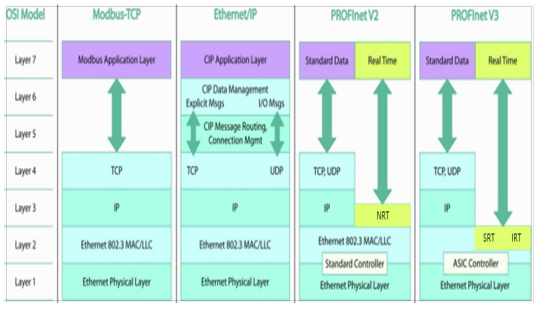


그림 2. Modbus-TCP, Ethernet/IP, PROFINET 구조 비교 [16]
Fig. 2. Modbus-TCP, Ethernet/IP, PROFINET Structure Comparison

그림 2는 제어프로토콜을 OSI 7 Layer의 계층적인 차이점을 나타내는 그림이다[16]. Modbus-TCP는 표준 인터넷 네트워크의 TCP/IP 계층을 활용해 쉽게 구현할

수 있는 것이 장점이지만, 실시간성 및 시간 결정성을 보장하지는 못하고, TCP/IP를 이용한 Modbus-TCP의 반응 시간은 최고 20ms이며, UDP/IP를 이용한 Modbus-RTPS는 Modbus-TCP와 비교하면 반응 시간을 더 줄일 수 있다.

EtherNet/IP는 표준 인터넷 네트워크의 TCP/IP 계층을 활용한 CIP(Common Industrial Protocol)를 사용하고, CIP는 산업 자동화에서 사용할 수 있는 메시지를 제공하며, 두 가지 클래스를 가지고 있다. TCP/IP는 동기식 메시지로 산업환경에서 사용하는 기기의 운영 설정값을 전송할 때 쓰이며, UDP/IP는 비동기식 메시지로 기기 간의 I/O 데이터를 빠르게 전송하기 위해 사용된다. 보통 10ms의 반응 시간을 가지고 있다.

PROFINET은 NRT, SRT, IRT 세 가지로 분류되며, 분류의 기준은 TCP/IP 계층의 이용 방법과 반응 시간에 따라 제어할 수 있는 분야가 달라진다. NRT는 표준 인터넷 네트워크의 TCP/IP 계층을 이용해 구현하기 때문에 반응 시간이 100ms로 일반적인 구성요소 기반 공정 자동화에 사용된다. SRT는 TCP/IP 계층을 이용하지 않고, 7계층과 직접 통신하는 직접 주소지정 및 우선순위 지정 메시지를 사용하여 반응 시간이 1ms로 기기 간의 I/O 데이터를 빠르게 전송하기 위해 사용된다. IRT는 TCP/IP 계층을 이용하지 않고, OSI 7계층 중 2계층인 MAC(Media Address Control)에 ASIC(Application Specific Integrated Circuit) 컨트롤러를 추가한 스위치가 필요하며, 반응 시간은 1ms 미만으로 자동화 모션 컨트롤에 사용된다.

Ⅳ. IT 및 산업용 방화벽 비교

IT 보안 장비와 산업용 보안 장비에는 방화벽, IDS/IPS, Data Diode 등 다양한 종류의 장비가 존재하고, 이 중에서 방화벽을 중점적으로 비교 및 분석하였으며, IT 보안 장비의 모델로 Cisco ASA 5508-X, 산업용 보안 장비의 모델로 3eTI CyberFence CIP를 선정하여 환경 측면, 보안 요구사항 측면 2가지로 정리하여 기술 분석하였다.

1. 환경 측면

IT 방화벽과 산업용 방화벽은 환경적 측면에서 큰 차이를 가지고 있다. 산업용 보안 장비는 다음 표 4와 같이 온도, 크기, 설치방법, 인터페이스가 요구사항을 만족하기 때문에 원자력, 스마트공장 등 다양한 산업환경 분야에서 사용될 수 있다[17, 18].

표 4. IT 방화벽과 산업용 방화벽 환경 측면 비교표
Table 4. IT Firewall and Industrial Firewall Environment Comparison

모델 / 비교항목	IT 방화벽	산업용 방화벽
	Cisco ASA 5508-X	3eTI CyberFence CIP
Operating Temperature	0 ~ 40℃	-40 ~ 70℃
Storage Temperature	-25 ~ 70℃	-40 ~ 85℃
Dimensions (H x W x D)	4.3 x 43.6 x 28.6cm	-
Installation	Rack mount	Din-Rail mount
Interface	• Gigabit Ethernet RJ45 : 8 • Console : Mini USB, RJ-45	• Encrypted black • Unencrypted red • Configurable Auxiliary • Local management

산업용 방화벽은 IT 방화벽 보다 약 -40℃의 저온과 +70℃의 고온에서 가동할 수 있고, 보관하기 위한 온도로 저온에서는 -40℃, 고온에서는 +85℃의 더 높은 온도에서 보관할 수 있기 때문에 다양한 산업 분야에서 사용될 수 있다.

IT 방화벽은 산업용 방화벽보다 크기가 좀 더 크고, 설치방법은 Rack 마운트 구조를 이용하며, 산업용 보안 장비는 Din-Rail 마운트 구조를 이용하기 때문에 IT 보안 장비보다 좀 더 작은 크기를 가지고 있다.

IT 방화벽인 Cisco ASA 5508-X는 기가 속도를 지원하는 이더넷 포트 8개와 시스템 설정을 위한 Mini USB, RJ-45 포트를 하나씩 가지고 있다. 3eTI CyberFence CIP는 기가 속도를 지원하는 이더넷 포트 4개를 가지고 있으며, Encrypted black port는 암호화를 통해 데이터를 전송하기 때문에 SCADA와 같은 보안이 중요한 장비와 연결한다. Unencrypted red port는 암호화하지 않고, 데이터를 전송하기 때문에 PLC와 같은 빠른 데이터 전송이 필요한 장비에 연결하며. Configurable Auxiliary Port와 Local management Port는 콘솔 포트로 이용되어 방화벽의 시스템을 설정할 수 있다.

2. 보안 요구사항 측면

IT 방화벽과 산업용 방화벽의 보안 요구사항은 공통평가 기준(Common Criteria)의 문서 중 보안 요구사항(Security Target)을 확인하였고, 주요 비교 사항은 SFR(Security Functional Requirements)이며. SFR은

보안 기능 요구사항이라 불리며, 제품에서 제공할 수 있는 개별 보안 기능을 설명한다[19, 20].

표 5는 IT 방화벽과 산업용 방화벽으로 선정한 Cisco ASA 5508-X, 3eTI CyberFence CIP 모델을 비교하였으며, 비교 사항이 같은 항목은 “해당 항목 동일”로 표현하였다.

표 5. IT 방화벽과 산업용 방화벽 보안 요구사항 측면 비교표
Table 5. IT Firewall and Industrial Firewall Security Requirements Comparison

비교항목 \ 모델	IT 방화벽	산업용 방화벽
	Cisco ASA 5508-X	3eTI CyberFence CIP
Security Audit	해당 항목 동일	
Cryptological Support	FCS_CKM.1(1)	-
	-	FCS_CKM.1
	FCS_CKM.1(2)	-
	-	FCS_CKM.2
	-	FCS_CKM.4
	FCS_CKM_EXT.4	-
	FCS_TLS_EXT.1	-
	FCS_SSH_EXT.1	-
Full Residual Information Protection	FDP_RIP.2	-
Identification and Authentication	-	FIA_X509_EXT.2
	-	FIA_X509_EXT.3
	FIA_AFL.1	-
	FIA_PSK_EXT.1	-
Security Management	-	FMT_MOF.1(1)
	-	FMT_MTD.1(1)
	FMT_MOF.1	-
	FMT_MTD.1	-
Protection of the TSF	FPT_FLS.1	-
	FPT_ITT.1	-
TOE Access	-	FTA_SSL.3
	FTA_SSL.3(1)	-
	FTA_SSL.3(2)	-
	FTA_TSE.1	-
	FTA_VCM_EXT.1	-
Trusted Path/Channels	해당 항목 동일	
Stateful Traffic Filtering	FFW_RUL_EXT.1	-
Deep Packet Inspection	X	O

Security Audit은 보안 장비 대응 행동에 대한 감사 대상 공격을 생성하고, 선택적으로 감사 기록의 생성 유무를 결정할 수 있으며, 악의적인 공격 여부 및 공격이 발생한 시간에 대한 정보를 포함하는 행동에 대한 기록을 생성한다.

Cryptological Support는 높은 수준의 보안성을 달성하기 위해 암호 기능에서 사용할 수 있는 항목을 설명하며, 인증, 부인 방지, 신뢰할 수 있는 경로, 신뢰할 수 있는 채널 및 데이터 분리의 내용이 포함되어있다. 또한, Cisco 장비에서 지원하는 FCS_CKM1(1, 2) 항목은 비대칭키 까지 암호화 생성을 할 수 있고, FCS_CKM_EXT.4 항목은 암호화키 파기가 아닌 제로화를 통해 삭제하는 내용을 설명한다. 또한, TLS와 SSH 프로토콜 지원 여부를 확인할 수 있다.

Full Residual Information Protection은 보안 장비에 전송되는 모든 정보 흐름이 이전 트래픽의 잔여 정보를 포함하지 않도록 보장하는 항목을 설명한다.

Identification and Authentication은 인증이 요구되는 사용자 신원을 확인하고, 검증하는 기능에 대한 요구사항을 설명한다. 또한, 3eTI 장비에서 FIA_X509_EXT.(2, 3) 항목은 X509 인증서의 인증과 요청을 의미하고, Cisco 장비에서 FIA_AFL.1, FIA_PSK_EXT.1 항목은 인증 실패 처리와 사전에 공유키를 생성할 수 있는 기능에 대하여 설명한다.

Security Management는 식별 및 인증, 보안 장비 감사 기능, 장비 암호화 기능, 접속 유지 시간, 구성 파일의 저장 및 검색, VPN 데이터 암호화 및 복호화를 포함하여 보안 장비에 의해 시행되는 정보 흐름 통제 정책 등을 설명한다. 또한, 두 장비 간의 항목 차이는 TSF 데이터를 업데이트할 때 일반적인 TSF 데이터인지 신뢰할 수 있는 TSF 데이터인지의 차이를 나타낸다.

Protection of the TSF는 식별, 인증, 인가된 관리자가 악의적인 클라이언트의 접근을 제한하는 접근 통제를 구현하여 신뢰 되지 않은 주체에 의한 간섭 및 침해로부터 보호하기 위한 항목을 설명한다. 또한, Cisco 장비에서 FPT_FLS, ITT 항목은 안전 실패와 내부전송 시 TSF 데이터의 기본적인 보호 방법을 나타낸다.

TOE(Target of Evaluation) Access는 관리자가 구성할 수 있는 경고 배너를 표시하며, 연결 비활성 시간이 되면 관리자 및 VPN 클라이언트 세션이 종료되고 다시 인증 하여야 하는 내용을 설명한다. 또한, Cisco 장비에서 FTA_SSL 항목은 SSL을 이용한 세션 종료에서 관리자와 VPN 클라이언트까지 종료할 수 있는 내용을 나타내고, FTA_TSE, VCM 항목은 세션 설정에 필요한 방법과 VPN 클라이언트 관리 방법을 나타낸다.

Trusted Path/Channels는 클라이언트가 보안 장비와 직접적인 통신을 통하여 기능을 수행할 필요가 있기 때문에 안전하고, 신뢰적인 통신 경로와 채널을 제공하는 설명을 하고 있고, 관리자 세션의 무결성 및 보호를 위해 TLS, HTTPS를 사용하는 내용을 설명한다.

Stateful Traffic Filtering은 정보의 무단 공개, 부적절한 서비스 액세스, 서비스 오용, 네트워크 데이터 전송 중단과 관련된 문제를 해결하기 위해 IP 주소 기반 필터링(IPv4, IPv6)을 포함한 상태 기반 트래픽 방화벽 기능에 대한 항목을 설명한다.

3eTI 장비에서 DPI 기능은 CC 인증 문서 중 Security Target에 언급은 되어 있으나, 어떤 항목에 대하여 보안 요구사항이 필요한지와 어떤 항목을 테스트하였는지는 확인할 수 없었다. 하지만, DPI는 악의적인 명령을 감지하여 PLC로 전송되지 않도록 하거나, 운영자에게 경고를 보낼 수 있고, OPC, DNP3, Modbus-TCP, BACNet, EtherNet/IP, CANopen/CAN 등 산업용 제어프로토콜의 패킷을 OSI 계층 중 7계층 단계까지 확인하기 때문에 강력한 보안 기능을 제공하며, 3eTI Cyberfence CIP에서 지원하고 있다.

V. 결 론

본 논문에서는 IT 네트워크 장비와 산업용 네트워크 장비 간에 차이를 비교하기 위해 환경, 관리, 제어프로토콜 3가지 측면으로 비교하였다. 환경 측면에서 산업용 스위치 장비는 산업환경에 맞추어 내온, 내구성 등이 강화되어있고, 관리 측면에서 산업용 스위치 장비는 IT 스위치 장비보다 가용성을 높이기 위한 MTBF, Alarm, PoE, Port Mirroring을 지원한다. 제어프로토콜 측면에서 산업용 스위치 장비는 산업용 장비가 가져야 할 결정성, 유연성, 확장성을 확보하기 위한 산업용 제어프로토콜들을 지원하고 있다. 따라서 산업용 스위치 장비는 제어프로토콜을 지원하고, 산업환경에서 사용하기에 적합한 요구사항을 가지고 있기 때문에 다양한 산업 분야의 네트워크 아키텍처를 구성할 수 있다.

IT 방화벽과 산업용 방화벽 간에 차이를 비교하기 위해 환경, 보안 요구사항의 2가지 측면으로 분석하였다. 환경 측면에서는 네트워크 장비 비교와 마찬가지로 산업환경에 맞추어 내온, 내구성 등이 강화되어있다. 보안 요구사항 측면에서 IT 방화벽과 산업용 방화벽의 차이점은 크지 않으나, 산업용 방화벽에서 DPI 기능은 산업용 제어프로토콜을 지원하기 때문에 산업용 시설 내외부의 비정상적인 패킷을 감지하는데 가장 핵심적인 역할을 하고 있다. 따라서 산업 시설을 노리는 대규모 사이버 테러에 대한 대비책으로 주요 국가 인프라 시설 및 산업 시설을 보호함으로 국가 안보 및 산업 시설 보호에 이바지할 것으로 기대된다.

References

[1] Dong-Boem Ko, Jeong-Min Park, "A Study on the Visualization of Facility Data Using Manufacturing Data Collection Standard", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 18, No. 3, pp. 159-166, Jun 2018.
DOI: https://doi.org/10.7236/JIIBC.2018.18.3.159

[2] Jin Hoh, Chul-Yong Jung, "Convergence-based Smart Factory Security Threats and Response Trends", The Journal of the Korea Convergence Society, Vol. 8, No. 11, pp. 29-35, Nov 2017.
DOI: https://doi.org/10.15207/JKCS.2017.8.11.029

[3] David L. Tennenhouse, Jonathan M. Smith, W. David Sincoskie, David J. Wetherall, Gary J. Minden, "A survey of active network research", IEEE Communications Magazine, Vol. 35, No. 1, pp. 80-86, Jan 1997.
DOI: https://doi.org/10.1109/35.568214

[4] Kathy Nagamine, "Worldwide Quarterly Ethernet Switch and Router Trackers Show Modest, Continued Growth for Fourth Quarter and Full Year 2017", IDC(International Data Corporation), Mar 2018.

[5] Lars-Erik Gadde, Lars Huemer, Hakan Hakansson, "Strategizing in industrial networks", Industrial marketing Management, Vol. 32, No. 5, pp. 357-364, July 2003.
DOI: https://doi.org/10.1016/S0019-8501(03)00009-9

[6] Jesse Maida, "Top 5 Vendors in the Managed Industrial Ethernet Switches Market from 2017 to 2021: Technavio", Technavio Research, Jan 2017.

[7] Tak-hui Jeong, "The cryptic story of industrial switches", The Journal of The Institute of Internet, Broadcasting and Communication, Aug 2007.

[8] David Ong, "ICS/SCADA Cybersecurity and IT Cybersecurity : Comparing Apples and Oranges", Attila Cybertech, Dec 2017.

[9] Transparency Market Research, "Industrial Controls System Market - Global Industry Analysis Size Share Growth Trends and Forecast 2015 - 2021", Transparency Market Research, Jun 2015.

[10] Cisco, "Cisco Catalyst 3850 Series Switches Data Sheet", The Journal of The Institute of Internet, Broadcasting and Communication, Cisco, July 2018.

[11] Cisco, "Cisco 4000 Series Integrated Services Routers

Data Sheet", Cisco, Dec 2017.

[12] Moxa, "EDS-P510A-8PoE Series Data Sheet", Moxa, May 2016.

[13] Siemens, "Industrial Ethernet switches SCALANCE X-400 Operating Instructions", Siemens, Sep 2009.

[14] Dae-Hyeon Gwon, Yoon Gwon, Su-Gang Lee, "Industrial Network Trends for Smart Factories", The Journal of The Korean Institute of Communication Sciences, Vol. 33, No. 1, pp. 37-41, Dec 2015.

[15] Thomas Carlsson, "Industrial Ethernet is now bigger than fieldbuses", HMS Industrial Networks, Feb 2018.

[16] Glenn Johnson, "Determinism in industrial ethernet: A technology overview — Part 2", Process Technology, Aug 2009.

[17] Cisco, "Cisco ASA with FirePOWER Services Data Sheet", Cisco, Feb 2018.

[18] 3eTI, "CyberFence CIP datasheet", Ultra Electronics 3eTI, 2018.

[19] Cisco, "Cisco Adaptive Security Appliances and ASA Virtual Security Target", Common Criteria, Oct 2016.

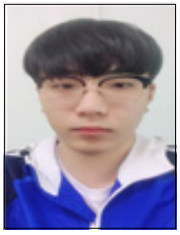
[20] 3eTI, "CyberFence 3e-636 Series Network Security Devices (NDcPP10) Security Target", Common Criteria, Sep 2017.

저 자 소 개

신 동 진(준회원)

• Dong-Jin Shin received BS in Department of Computer Science and MS in Department of Smart Manufacturing Engineering at the Korea Polytechnic University in 2018 and 2020. He is currently studying Phd in Department of Computer Science at AnYang University. His research interests include Big Data, Internet of Things (IoT), Network&System security.

황 승 연(준회원)



• Seung-Yeon Hwang is received his BS in Department of Computer Science at Korea Polytechnic University in 2019. He is currently studying MS in Department of Computer Science at Anyang University. His research interests include Database System, Big Data, Data Analysis, Machine Learning, etc.

오 재 곤(정회원)

• Jae-Kon Oh received his BS and MS at Kwangwoon University in 1994 and Ajou University in 2005, respectively. In 2017, he received his PhD in at Chonbuk University. He is currently a CEO at SEINSystems. His research interests include Database Systems, BigData, Semantic Web, Geographic Information Systems (GIS) and Ubiquitous Sensor Network (USN), etc.

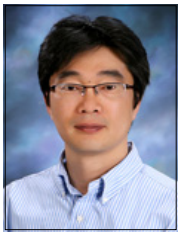
김 정 준(정회원)

• Jeong-Joon Kim received his BS and MS in Computer Science at Konkuk University in 2003 and 2005, respectively. In 2010, he received his PhD in at Konkuk University. He is currently a professor at the department of ICT Convergence Engineering at Anyang University, His research interests include Database Systems, Big Data, Semantic Web, Geographic Information Systems (GIS) and Ubiquitous Sensor Network (USN), etc.

이 용 수(정회원)

• Yong-soo Lee received his MS in Computer Science at Konkuk University in 1989. In 2015, he received his PhD in Information & Control Engineering at Kwangwoon University. He is currently a professor at the Department of software convergence at Yeoju Institute of Technology. He is the Member of the Korea Institute of Internet, Broadcasting & Communication (IIBC). His research interests include Database Systems, Data Mining, BigData, Wireless Sensor Networks and Ubiquitous Sensor Network (USN), etc.

박 경 원(정회원)



• Kyungwon Park received his BS and MS in Mathematics at Chung-Ang University in 1995 and 1998, respectively. In 2004, he received his Ph. D at University of South Carolina . He is currently a professor at the department of Computer Science at Korea Polytechnic University. His research interests include Nonlinear Approximation Theory, Image Analysis, Machine Learning, etc.

※ 이 논문은 ETRI부설연구소의 산업용 네트워크 장비 및 제어용 보안 장비 기술 분석 연구과제로 수행한 연구결과입니다.