스마트팩토리 영역 및 계층별 보안위협 대응체계 도출 기법

정인수[1], 김득훈[2], 곽진[3]
[1]아주대학교 사이버보안학과 정보보호응용및보증연구실 석박통합과정
[2]아주대학교 소프트웨어융합연구소 박사후연구원
[3]아주대학교 사이버보안학과 교수
jis0727@ajou.ac.kr, dhkim.isaa@gmail.com, security@ajou.ac.kr

A Method for Deriving a Security Threat Response System in Smart Factory Area and Layer

In-Su Jung[1], Deuk-Hun Kim[2], Jin Kwak[3]
[1]ISSA Lab., Dept. of Cyber Security, Ajou University
[2]Inst. for Computing and Informatics Research, Ajou University
[3]Dept. of Cyber Security, Ajou University

요 약

IoT(Internet of Things), 빅데이터, AI(Artificial Intelligence), 클라우드와 같은 ICT(Information and Communications Technology) 기술이 발전함에 따라 ICT와 제조기술이 융합된 스마트팩토리가 발전하고 있다. 이는 2개의 영역과 5개의 계층으로 구성되어 기타 환경들과 상이한 구조를 가지고 있으며, 각 영역·계층별 발생 가능한 보안위협도 상이하다. 또한, 각 영역과 계층이 연결됨에 따라 발생 가능한 보안위협이 증가하고 있으며, 이에 대한 효율적인 대응을 위하여 스마트팩토리 영역·계층별 환경을 고려한 대응체계 마련이 필요한 실정이다. 따라서, 본 논문에서는 스마트팩토리 영역·계층별 발생 가능한 보안위협을 분석하고, 이에 대응하기 위한 대응체계 도출 기법을 제안한다.

1. 서론

최근 ICT(Information and Communications Technology) 기술이 제조산업에 도입됨에 따라 제조공정 자동화 및 지능화를 수행하는 스마트팩토리가 발전되고 있다. 이는 IT(Information Technology) 영역과 OT(Operational Technology) 영역이 연결되고, 각 영역·계층별 장치들이 서로 연결됨에 따라 효율적인 제조공정 과정을 수행한다[1]. 그러나 영역·계층·장치 간의 연결로 인해 스마트팩토리 구조가 복잡해지고, 스마트팩토리 영역·계층별 발생 가능한 보안위협이 증가하고 있다. 이에 대응하기 위해 스마트팩토리 각 영역·계층 구조 분석 및 스마트팩토리 다영역·다계층 환경에 적합한 대응체계 구축이 필요하다. 따라서, 본 논문에서는 스마트팩토리 영역·계층별 발생 가능한 보안위협을 분석하고, 이에 대응하기 위한 대응체계 도출 기법을 제안한다.

본 논문은 2장에서 스마트팩토리와 스마트팩토리 영역·계층별 보안위협을 분석한다. 3장에서는 이에 대응하기 위한 스마트팩토리 보안위협 대응체계 도출 기법을 제안하며, 4장에서 결론을 짓는다.

2. 관련 연구

2.1 스마트팩토리

스마트팩토리는 기존 제조기술에 센서, 클라우드, 빅데이터, 정밀 제어, 모바일 등 다양한 ICT 기술이 융합된 지능형 공장이다. 높은 수준의 자동화 및 지능화된 인프라를 제공함으로써 생산성 향상, 에너지 절감, 안전한 생산환경 구현 등이 가능하다[2]. 스마트팩토리는 2영역(OT, IT), 5계층 구조 아키텍처로 구성되어 있으며, 이는 국내·외 스마트팩토리 산업제어시스템 표준(RAMI 4.0, ISA/IEC 62443, NIST 800-82, Purdue 모델 등)을 통해 구성된다.

다음 <표 1>은 스마트팩토리 2영역, 5계층 구조 아키텍처 구성을 나타낸다. 이는 직접적인 제조공정 과정이 수행되는 OT영역(0~3계층)과

전사업무관리가 수행되는 IT영역(4~5계층)으로 구분된다. 스마트팩토리는 생산 관련 현장 장치로 구성된 0계층, 현장 장치들의 상태정보 수집 및 제어 명령 전달을 수행하는 1계층, 모니터링 및 공정 통제를 수행하는 2계층, 공장 또는 시설 단위로 전체 모니터링을 수행하고 최종 제품을 생산하기 위한 작업을 관리하는 3계층, 스마트팩토리를 관리하고 비즈니스 관련 활동에 필요한 기능을 수행하는 4~5계층으로 구성된다[3].

<표 1> 스마트팩토리 2영역, 5계층 구조 아키텍처 구성

Area	Layer	Layer Name	Component
OT	0	Field Device	Sensor, Actuator, Robot, Production equipment, etc.
	1	Basic Control	PLC, DCS, RTU, IED, etc.
	2	Supervisory Control	SCADA, HMI, OWS, Mobile, etc.
	3	Operations Management	MES, PLM, WMS, POP, Historian, etc.
IT	4~5	Enterprise Biz System	ERP, CRM, SCM, Groupware, etc.

2.2 스마트팩토리 보안위협

스마트팩토리 보안위협은 각 영역·계층별 특성을 기반으로 도출되며, <표 2>을 통해 영역·계층별 스마트팩토리의 보안위협 벡터와 보안위협을 확인할 수 있다. OT영역(0~3계층)의 보안위협은 제조공정 과정에 직접적으로 영향을 미치는 제조 공정 장치에 대한 보안위협이 주로 발생하며, IT영역(4~5계층)의 보안위협은 외부 네트워크와 연결됨에 따라 네트워크 기반 보안위협이 주로 발생한다[3]. 이에 따라, 스마트팩토리 2영역 5계층에서 발생 가능한 보안위협은 총 7가지이며, 이를 보안위협 벡터 7으로 정의한다.

<표 2> 스마트팩토리 영역·계층별 보안위협

Area	Layer	Security Threat Vector	Security Threat
OT	0~3	Physical Access	Physical device damage, process data manipulation and leakage, etc.
OT	0~3	Industrial Control System	malfunction and service interruption, etc.
OT	0~3	Factory Control Network	Seizing software permissions, malfunctioning and disrupting services, etc.
OT, IT	2, 4~5	Factory Work Domain	Ransomware infection, network failure, etc.
OT	0~3	Supply Chain	Ransomware infection, tampering with production information, etc.
OT, IT	0, 2~5	Personnel and Aging Facilities	Malfunction and interruption, manipulation and leakage of process data, etc.
OT, IT	0~5	External Internet	Business network failure, service interruption, information leakage, etc.

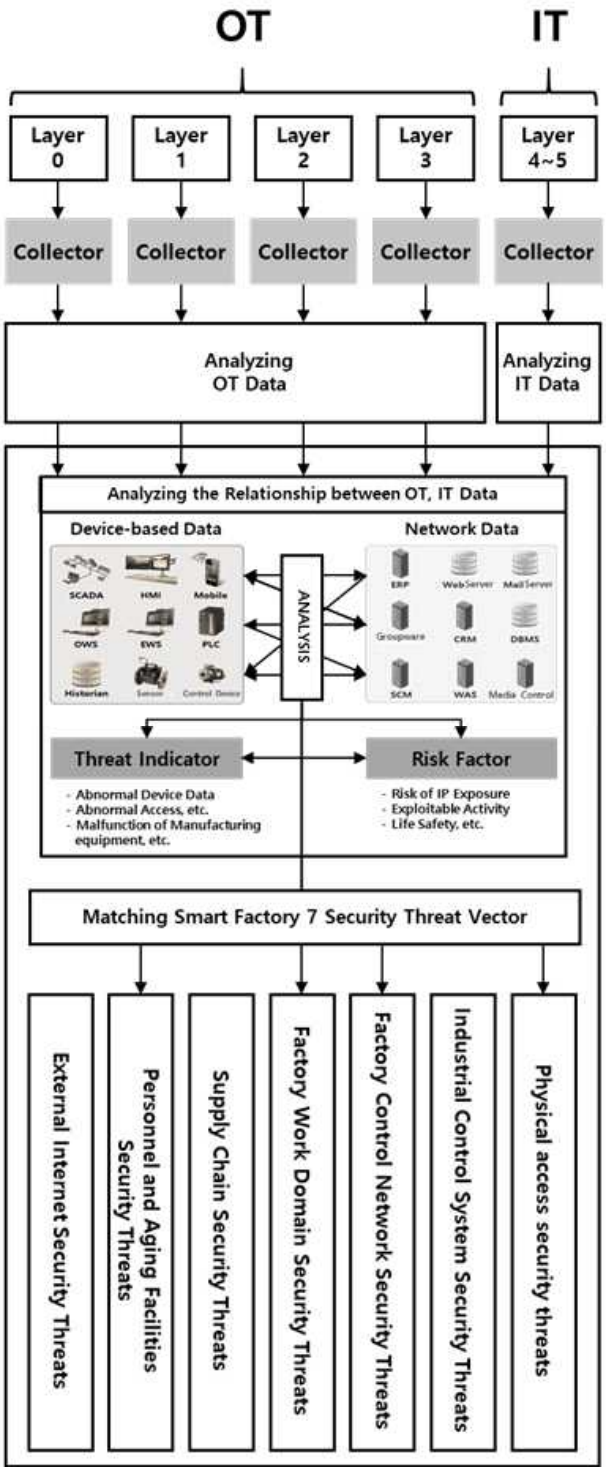
3. 스마트팩토리 보안위협 대응체계

본 장에서는 스마트팩토리 보안위협에 대응하기 위해 (그림 1)과 같은 대응체계 도출 프로세스를 제안한다. 이는 (a) 데이터 수집 및 분석, (b) 데이터 상관관계 분석, (c) 스마트팩토리 보안위협 벡터 7 매칭으로 구성된다.

(a) 스마트팩토리 영역·계층별 데이터 수집 및 분석

스마트팩토리를 구성하는 OT영역(0~3계층) 장치들과 IT영역(4~5계층) 장치들은 영역별로 수행하는 업무에 따라 구분된 특징이 존재하며, 이로 인해 생성되는 영역·계층별 데이터의 종류도 상이하다. OT영역(0~3계층)은 직접적인 제조공정 과정에서의 장치 기반 데이터가 주로 생성되고, IT영역(4~5계층)은 외부 네트워크와 연결되어 전사업무 관리를 수행함에 따라 네트워크 기반 데이터가 주로 생성된다. 각 영역·계층별로 상이한 특징을 가짐에 따라 스마트팩토리 보안위협 대응체계를 도출하기 위해서는 각 계층별 특징을 기반으로 한 데이터를 수집하고 영역별로 데이터를 분석하는 것이 선행되어야 한다. 따라서, 각 계층별로

Collector를 배치하여 생성되는 데이터들을 수집하고, OT영역과 IT영역을 구분하여 데이터 분석을 수행한다.



(그림 1) 스마트팩토리 보안위협 대응체계 도출 기법

(b) 스마트팩토리 영역별 데이터 상관관계 분석

스마트팩토리는 2영역, 5계층 구조로 구성되고, 영역과 계층이 연결됨에 따라 다영역·다계층을 대상으로 한 보안위협이 발생할 수 있다. 이에 따라, 단일 영역·계층에 대한 분석뿐만 아니라 영역·계층 간의 데이터 상관관계 분석이 필요하다. 이를 위해 영역 간 분석기를 배치하고, 스마트팩토리 환경에 대한 위협 지표(비정상 장치 데이터, 비정상 접근 등)와 위험 요소(산업용 네트워크 IP 주소 유출, 인명 사고 등)를 기준으로 상관관계 분석을 수행한다.

(c) 스마트팩토리 보안위협 벡터 7 매칭

스마트팩토리 계층/영역별 특징을 기반으로 한 데이터 분석 결과를 기반으로 스마트팩토리 영역·계층별 보안위협 벡터 7 매칭을 수행한다. 분석된 데이터를 기반으로 해당되는 보안위협 벡터를 매칭한 후 보안위협 대응체계를 도출하기 위해 활용된다.

4. 결론

본 논문에서는 스마트팩토리 보안위협 대응을 위한 대응체계 도출 프로세스를 제안하였다. 스마트팩토리 각 영역·계층별 데이터 특징을 고려한 대응체계 도출 방안을 통해 정확한 보안위협 분석 및 대응에 기여할 수 있을 것이다.

사사문구

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-01806, 스마트공장 보안 내재화 및 보안관리 기술 개발)

참고문헌

[1] Zhan Shi, Yongping Xie, Wei Xue, Yong Chen, Liuliu Fu, and Xiaobo, “Smart factory in Industry 4.0”, Systems Research and Behavioral Science, Vol. 37, No. 4, pp. 607-617, Jun. 2020.

[2] Halenar, Igor, Lenka Halenarova, and Pavol Tanuska, “Communication Safety of Cybernetic Systems in a Smart Factory Environment” MDPI, Machines, Vol. 11, No. 3, Mar. 2023.

[3] 한국인터넷진흥원, “스마트공장 보안 모델”, Dec. 2021.