반도체디스플레이기술학회지 제23권 제2호(2024년 6월)
Journal of the Semiconductor & Display Technology, Vol. 23, No. 2. June 2024.

OT(Operational Technology) 환경에서 스마트팩토리 보안 강화 방안에 관한 연구

김영호*·서광규*†
*†상명대학교 경영공학과

A Study on the Strengthening of Smart Factory Security in OT (Operational Technology) Environment

Young Ho Kim* and Kwang-Kyu Seo*†
*†Management Engineering, Sangmyung Univ., Korea

ABSTRACT

Major countries are trying to expand the construction of smart factories by introducing ICT such as the Internet of Things, cloud, and big data into the manufacturing sector to secure national-level manufacturing competitiveness in the era of the 4th industrial revolution. In addition, Germany is pushing for Industry 4.0 to build a fully automatic production system through the Internet of Things, and China is pushing for the expansion of smart factories to enhance the country's industrial competitiveness through Made in China 2025, Japan's intelligent manufacturing system, and the Korean government's manufacturing innovation 3.0. In this study, considering the increasing security connectivity of smart factories, we would like to identify security threats in the external connection part of smart factories and suggest security enhancement measures based on domestic and international standard security models to respond to the identified security threats. Eventually the proposed method can be applied by accurately identifying the smart factory security status, diagnosing vulnerabilities, establishing appropriate improvement plans, and expanding security strategies to respond to security threats.

Key Words : Smart Factory Security, Operational Technology, IoT, ICS Security, Security Strategy

1. 서 론

글로벌 주요국들은 4차 산업혁명 시대 국가 차원의 산업 경쟁력을 확보하기 위해 AI, IoT, 클라우드, 빅데이터 등 디지털 신기술을 다양한 산업분야에 적용하고 있다 [1]. 특히 제조 분야에 디지털 신기술을 도입하여 스마트팩토리 구축 확산 노력을 기울이고 있는 가운데 우리 정부는 제조혁신 3.0을 수립하여 국가의 산업경쟁력을 높이고자 스마트팩토리 확대를 추진하고 있다.

†E-mail: kwangkyu@smu.ac.kr

스마트팩토리는 “일반 직원들이 업무를 수행하는 업무 영역(Level4, Enterprise Biz System)과 제품 생산을 위한 제어 시스템 운영 관리 영영(Lavel3, Operations Management), 그리고 제조 공정을 제어하고 제품을 생산하는 ICS 영역(Lavel0~2)으로 구성되어 있다” [2]. 업무 영역에 대한 보안 위협으로는 우리가 일반적으로 알고 있는 다양한 IT 보안 위협(해킹, 악성코드 감염, APT 공격 등)이 있다. 산업제어 시스템에 대한 보안 위협은 악의적 공격자가 산업시스템을 직접 공격하기보다는 업무 영역에 우선 침투하여 내부 정보를 수집한 후, ICS 영역을 공격하는 형태로 진행되거나 유지보수 과정에서 악성코드가 전파되는 형태의 위

협이 가해지고 있다. 향후에는 스마트팩토리의 진화로 업무망의 많은 시스템이 공장 내 다양한 장비들과 복잡하게 연결되고 있으므로 스마트팩토리에 대한 IT 보안 위협은 점차 커질 수밖에 없기에 ICS(산업제어시스템) 영역의 보안 위협에 대한 대비는 반드시 필요하다[3].

본 연구는 스마트팩토리에 대한 사이버 보안위협 증가로 IT환경의 보안문제 뿐 아니라 안전과 생명 등 융합 환경에서의 보안문제를 고려하기위해 대외 연계구간의 보안위협을 식별하고, 표준 모델 사례를 분석하여 스마트팩토리 환경의 보안 전략을 제시하고자 한다.

2. OT(Operational Technology) 환경에서 스마트팩토리 보안강화 방법론

2.1 선행연구 조사

먼저 스마트팩토리 보안관련 연구로 정재훈 등 산업제어시스템 중심으로 중소기업용 스마트팩토리 보안 취약점 분류체계 개발하였고[4] 허진 등은 AHP를 활용한 우선순위 분석을 통해 스마트팩토리의 주요 보안 요인을 연구하였다[5].

그리고 국내외 산업보안표준모델과 프레임워크 및 스마트공장 보안 모델은 다음과 같다.

해외 산업 보안 표준 모델 IEC(International Electrotechnical Commission) 62443은 제조, 에너지 분야에 특화된 산업제어 표준모델과 정책, 시스템, 제품 영역별 보안 표준을 정의하였다[2].

NIST(National Institute of Standards and Technology) 800-82는 산업제어 시스템의 보안 강화 절차 및 가이드와 5개 단계별 보안 프레임워크 식별 및 평가 기준을 정의했다 [6].

Purdue Model은 산업제어 시스템의 네트워크 구성 아키텍처 모델과 구성 영역별 보안 경계 및 인터페이스 정의에 대한 모델을 정의했다[7].

국내 KISA(Korea Internet & Security Agency)는 스마트공장 모델로 스마트공장 구성 요소별 보안 위협 식별 및 대응 방안과 IT와 OT 영역별 계층형 보안 아키텍처를 제공하였다[8].

본 연구의 범위는 스마트팩토리 보안전략 표준 모델을 대상으로 스마트팩토리 보안 강화 사례분석, 스마트팩토리 보안관련 국내.외 주요 기준과의 커버리지 비교, 그리고 국내 스마트팩토리 도입 기업에 가장 빠르고 효과적인 보안 적용범위 제시 등 단계별 접근을 수행하여 국내 스마트팩토리에 적용할 수 있는 OT환경에서의 보안 강화 방안을 제시하는 측면에서 선행연구와 차별점을 갖는다.

2.2 스마트팩토리 보안전략 표준 모델 사례 분석

국제 표준 IEC 62443은 4가지의 지침을 정의한다. 첫째는 제어 시스템 사이버 보안을 담당하는 모든 이해관계자가 사용할 수 있는 공통 용어, 개념 및 모델 정의하고 둘째는 자산 소유자가 고유한 비즈니스 및 위험 요구 사항을 충족하는 데 필요한 보안 수준을 결정하도록 지원, 셋째는 3. 제품 및 공급업체 개발 프로세스를 인증하는 메커니즘을 포함하여 제품 개발자를 위한 공통 요구 사항 세트와 사이버 보안 수명 주기 방법론을 확립합니다. 마지막 4번째는 4. 제어 시스템을 보호하는 데 중요한 위험 평가 프로세스 정의한다.

아래의 Table 1은 IEC 62443에서 정의하고 있는 4가지 지침을 나타낸다.

Table 1. ISA/IEC 62443 Series of Standards

Item	Part	Title
General	62443-1-1	Terminology, concepts, and models
	62443-1-2	Master glossary of terms and abbreviations
	62443-1-3	System cybersecurity conformance metrics
	62443-1-4	IACS security lifecycle and use cases
Policies & Procedures	62443-2-1	Establishing an IACS security program
	62443-2-2	IACS security program ratings
	62443-2-3	Patch management in the IACS environment
	62443-2-4	Security program requirements for IACS service providers
	62443-2-5	Implementation guidance for IACS asset owners
System	62443-3-1	Security technologies for IACS
	62443-3-2	Security risk assessment for system design
	62443-3-3	System security requirements and security levels
Component	62443-4-1	Product security development life-cycle requirements
	62443-4-2	Technical security requirements for IACS components

Table 2는 NIST 800-82의 산업 전반에 걸친 위험 관리의 표준으로 여겨지며 정보기술(IT), 산업제어시스템(ICS), 사이버물리시스템(CPS) 및 확장 IoT에 이르는 분야 및 기술 전반에 걸쳐 위험을 관리하기 위해 사용되는 프레임워크를 나타낸다.

Table 2. Structure of a time series framework

Item	Title
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Info Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Table 3은 Purdue 모델로 ICS 시스템들을 견고하게 연결하기 위해서는 네트워크 구조화 모델이 필요하며, 이를 위해 ISA-99에서 PERA(Purdue Enterprise Reference Architecture)로부터 도입해 채택한 모델로 레벨4, 5의 엔터프라이즈 영역은 IT, 레벨0~3 영역은 OT로 구분되며 구체적인 역할은 아래와 같다.

Table 3. Extended Purdue Model with overlaying attributes defined

Zone	Layer		Title
External	Level 5	Enterprise	Enterprise Network (Vendor Support/Cloud Access)
Corporate	Level 4		Email, Internet, Site Business Planning & Logistics
DATA	Level 3.5		Remote gateway services, Application Mirror, Web Services, Reverse Proxy AV Patch Mgm.t
	Level 3	OT	Application server, Engineering, Workstation, Remote Access Server)
Control	Level 2		Operator interface, HMI devices
	Level1		Batch Control, Discrete Control, Drive Control
Safety	Level 0		Sensors, Drives, Actuators, Robots

Table 4는 KISA 스마트공장모델은 IT와 OT 영역별 계층형 보안 아키텍처를 제공하였으며, 스마트 공장에 대한 보안 대상을 식별하여 스마트 공장 구축 간에 갖춰야 할 최소한의 보안 요구사항을 제시하고 있다.

Table 4. KISA Smart factory Mode

Item	Layer		Title
Corporate Mgmt.	4-5	IT	ERP, Mail, Business PC, Backbone
Production Mgmt.	3		Production Management System (MES)
Process control	2	OT	Manufacturing Mgmt. (HMI), Switch
Process Mgmt.	1		Manufacturing control (PLC), Industrial switch, Wireless AP
Field equipment	0		Sensors, Production equipment

2.3 스마트팩토리 보안 전략 및 시사점

스마트팩토리의 디지털화와 자동화로 인해 발생하는 다양한 보안 위협에 대한 표준화된 접근 방식을 통한 보안 위협을 대응하기 위해 보안전략 방안을 수립하였다.

최근 급증하고 있는 랜섬웨어 감염으로 인한 데이터 유실 사례와 바이러스 공격 등에 의한 공장 가동 중단 위험성은 스마트팩토리 보안 강화 요구의 가장 큰 동인이 되었다.

보안강화 전략은 정책 관련 10개 항목(Table 5), 대상 관련 6개 항목(Table 6), 위험 평가 관련 3개 항목(Table 7), 사고 예방 절차 4가지 항목(Table 8)으로 총 23개 항목을 도출 및 적용된다.

Table 5. The policy direction of the smart factory's security strategy

Objects	Title
Default Policy	-Establishment of governance -Defining Security Related Responsibilities and Roles -Physical security measures -External human resources management -Asset classification and processing -Other security-related legal requirements
Dedicated Organization	-Organizing an organization dedicated to smart factories and securing independence -Defining the security responsibilities and roles of members of the organization -Organization of consultations between facility operators and security personnel

Objects	Title
	-Continuous security technology and issue sensing activities
The head of security	-Designation of security manager and working person -Establishment and management of security policy and policy implementation documents -Identification and prioritization of important assets -Smart Factory & OT -Understanding the latest security trends -Implementation of security protection measures, etc. prescribed by other laws and systems
Education/ Training	-Internal management guidelines training -Improve security awareness a written pledge
R&R Designation	-Selection of Security -Management Responsibilities -Security roles and documentation of responsible persons -Specify partner responsibilities and roles -Establishing and supporting management security strategies
System operation procedure	-Reflect requirements and manufacturing environment -Reflecting the latest security issues and technology continuity -Emergency Response and Recovery
Service contract	-Specify responsibilities and permissions within an SLA contract -Operation Human Resources Security Protocols and Training -Monitor access to external partners and authority management -Definition of responsibility in the event of an accident -Regular security activities and reporting of results
Asset management	-System Identification and Management -Specify control items by security level -Technical and physical access control selection -Asset list change history management
Anomaly detection	-Production logs, network/data monitoring -Real-time analysis of security threat scenarios -Application of a control system to ensure visibility -AI-based automated risk analysis and response
Vulnerability analysis	-Check vulnerability test results -Analysis and evaluation of system and software vulnerabilities -Establishment and implementation of identified -vulnerability elimination plans -History management -Physical Access Control and Control Analysis

Table 6. The target direction of the smart factory's security strategy

Objects	Title
Application	-System Design and Implementation from a Security Perspective -Management of the status of security vulnerabilities in the introduction system -Monitoring real-time application events -Simulation Hacking Test and Improvement -Physical Control Plan
Network	-Separation of business network (IT) and process network -Application of Network Control Policy by Security Area -Security policies such as manganese data transmission, One Way communication, etc. -Apply Critical Data Encryption Communication
Equipment PC	-Policy operation of facility PC as a management organization unit -Apply lightweight control measures -Maintain firmware and control PC security patches -Patch plan -Unauthorized Device Network Access control
Server	-Manage key information backups -External connection interface control management -Immediate alarm setting in case of abnormal behavior -Equipment access password management
Data	-Transfer Data Protection -Storage Data Protection -Complete deletion when disposing of equipment -Encryption and encryption key management
Security Solution	-Establishment of measures for physical/network/system/user security system -Regular identification of security vulnerabilities and establishment of countermeasures

Table 7. The risk assessment direction of the smart factory's security strategy

Objects	Title
Attack Scenario	-Security strategy and standard model-based, key risk selection (Physical access, port, support facility, PC, Process control network, external supply network connection, etc.) -Continuous reflection of cyber security issues and technology trends

Objects	Title
Risk assessment	-Standard security model-based threat modeling -Analysis of risk severity, likelihood of occurrence, impact-Extraction and prioritization of risk factors to be managed
Risk management and response	-Establishment of a risk management plan (Risk response objectives, resource allocation, R&R specification, security requirements mapping, and risk minimization) -Monitoring and Continuous Review -Backup and recovery for security incidents

Table 8. The accident prevention procedures direction of the smart factory's security strategy

Objects	Title
Training and training of security incidents	-Training and training before facility system authorization -Accident response training by component -Strengthening Security Awareness Based on Risk Assessment -Training and education reflection of actual accident handling results
Abnormal Behavior Monitoring	-Select the target for monitoring such as sensors, networks, and amount of power -Real-time evaluation and security control -Reflects monitoring of the latest security issues
Vulnerability Analysis Assessment	-Confirmation of security confirmation at the time of introduction -Regular assessment of vulnerabilities -Improvement management of identified vulnerabilities
Audit Logs Management	-Confirmation of control feasibility assessment and compliance with operational procedures -Standard Log Definition and Accountability Traceability -Abnormal behavior monitoring linkage -Cyber Threat Intelligence-Based Analysis

2.4 스마트팩토리 보안 전략을 위한 시사점 도출

본 연구는 국내외 보안 표준 모델을 기준으로 보안정책, 보안전략, 위험평가, 사고 예방 대응 등 보안 전략을 나열하여 기업에 적용이 필요한 보안전략을 물리적 보안, 기술적 보안, 관리적 보안으로 구분하여 전체 35가지 보안 전략 방안을 적용할 수 있도록 도출하였다.

국내외 보안 표준 모델은 매우 복잡하고 상당한 수준의 보안 대응 조치가 필요하다. 반면 Table 9는 OT 영역별 기초적인 보안 통제 조치를 위한 보안 시스템을 제시함으로써 보안 담당자가 보다 쉽게 보안 위협에 대응하기 위한 보안 전략을 수립하고 확장 및 적용하는데 기여할 수 있다.

Table 9. Smart Factory Security Strategy Plan

Item	Security Area	Security system
Physical Security	Manpower Supplies Output Security	Security Surveillance System (CCTV)
		Security System
		Access Control System
		Output security system
Technical Security	Network Security	Network Firewall (FW)
		Intrusion Prevention System (IPS)
		Malicious Site Blocking System (Web Filter)
		Intrusion Detection System (IDS)
		WEB Firewall (WAF)
		Anti-DDoS System
		SSL-VPN
		Anti-Spam System
		Mail Malware Detection
	System Security	Anti-Virus for Server
		Server Detection and Response (EDR)
		Server Access Control (SAC)
		DB Access Control (DAC)
	Application Security	Secure Coding
		cryptographic communication (SSL)
		DB Encryption
	Endpoint Security	Anti-Virus for PC
		Endpoint Detection and Response (EDR)
		Digital Right Management (Document)
		PC Integrated Management
		Patch Management System
		Network Access Control (NAC)
		Data Loss Prevention (DLP)
		Secure Access Service Edge (SASE)
	Production System Security	Equipment Anti-Virus (ICS Anti-Virus)
Administrative Security	Incident Response Security	Two Factor Authentication
		Security Operation
		Web Vul. Scanner
		N/W Vul. Scanner
		Infra Vul. Scanner
		Source Code Scanner

3. 결 론

본 연구 결과를 통해 스마트팩토리를 운영 및 도입하고자 하는 기업은 매우 복잡하고 상당한 수준의 보안 대응 조치가 필요 국내외 표준 보안 모델을 보다 쉽고 체계적인 보안 방안을 마련할 수 있도록 방법론을 제시한다.

본 연구에서 제시한 방법론은 수많은 공장이 트렌드에 발맞춰 기존 제조 환경에서 스마트팩토리로 변화하며 IT와 유사한 사이버 공격의 대상이 되고 있는 시점에서 안전, 초가용성, 생산 효율성 등 목적에 의한 보안 한계와 획일화된 IT 환경과 달리 생산품의 다양성, 산업 장치의 긴 생명주기 등 공장 별 환경이 모두 상이하지만 스마트팩토리 관련 보안 전문 지식을 보유한 인력이 연구에서 제시한 보안전략 및 방법론을 정확히 파악한다면, 공장 보안 현황을 정확히 파악해 취약점을 진단하고, 적절한 개선 방안을 수립하여 보안 위협에 대응하는 보안 전략을 확장하여 적용할 수 있다. 궁극적으로 반도체 및 디스플레산업과 같은 국가중요시설이나 국가핵심기술을 보유한 사업체 등 보안 요구 수준이 높은 시설의 보안 전략 시 폭넓게 활용할 수 있는 자료가 될 것이다.

하지만, 본 연구의 방법론에서는 서로 다른 기술과 산업 등의 융복합으로 인해 여러가지 형태로 존재하던 데이터를 하나의 방법론으로 정형화하였으나 중견 및 중소기업의 경우 대상 범위와 예산에 따라 스마트팩토리 확산이 본격 궤도에 오르고 관련 보안방안 적용사례가 어느 정도 늘어나는 시점에 본 적용방안에 대한 실증적인 연구가 추가로 진행이 필요한 한계점도 있다.

감사의 글

본 논문은 2024년 상명대학교 교내연구비를 지원받아 수행하였음.

참고문헌

1. K.-K. Seo, “Development of Evaluation Framework for Adopting of a Cloud-based Artificial Intelligence Platform”, Journal of the Semiconductor & Display Technology, Vol. 22, No. 3, pp. 136-141, 2023.
2. ISA, ISA/IEC 62443 Series of Standards, 2024.
3. Jun-young Ahn, Seung-hun Lee, Hee-min Park, Hyun-chul Kim, "Development of a Cybersecurity Workforce Management System", Journal of the Semiconductor & Display Technology, vol.20, no.3, pp. 65-70, 2021.
4. Jae-Hoon Jeong, Tae-Sung Kim, "Developing a Classification of Vulnerabilities for Smart Factory in SMEs: Focused on Industrial Control Systems", Journal of the Korea society of system integration, Vol. 21, No. 5, pp. 65-79, 2022.
5. Jin Hoh, Ae Ri Lee, "Investigating Key Security Factors in Smart Factory: Focusing on Priority Analysis Using AHP Method", Information Systems Review, Vol. 22, No. 4, pp. 185-203, 2020.
6. NIST, Guide to Operational Technology (OT) Security - NIST SP 800-82 Rev. 3, 2022.
7. National Petroleum Council (NPC), Topic Paper #4-14 – Purdue Model Framework for Industrial Control System & Cybersecurity Segmentation, 2019.
8. KISA, Smart Factory Security Model Manual, 2022.

접수일: 2024년 6월 7일, 심사일: 2024년 6월 17일,
게재확정일: 2024년 6월 21일