IIoT 기반 스마트공장 보안을 위한 국제 표준화 동향

이하늘[1], 이종혁[2]
[1]세종대학교 정보보호학과 & 메타버스 융합전공 석사과정
[2]세종대학교 정보보호학과 & 메타버스 융합전공 교수
haneul@pel.sejong.ac.kr, jonghyouk@sejong.ac.kr

International Standardization Trends for IIoT-based Smart Manufacturing Security

Haneul Lee[1], Jong-Hyouk Lee[2]
[1,2]Dept. of Computer and Information Security
& Convergence Engineering for Metaverse, Sejong University

요 약

OT와 IT가 접목된 스마트공장은 외부망과의 접점이 증가함에 따라 많은 공격자들의 타깃이 되고 있다. 특히, 스마트공장의 가장 많은 공격 경로인 IIoT 기기는 제조 설비에 대한 제어권을 가짐에 따라 작업자의 안전과 생산성에 직접적인 영향을 미쳐 보안 위협 발생 시에 위험도가 높다. 따라서, 스마트공장에서 IIoT를 안전하게 운용하기 위한 보안 표준 마련이 필요하다. 본 논문에서는 주요 국제 표준화 기구 및 단체인 IEC, IIC, ITU-T의 표준 문서를 분석함으로써 IIoT 관점에서 스마트공장 보안을 위해 수행되고 있는 국제 표준화 동향을 분석한다.

1. 서론

기존의 제조 공장은 OT(Operational Technology) 기반의 폐쇄망 구조로 운영되어왔다. 그러나 IIoT(Industrial Internet of Things)와 같은 정보통신기술이 적용된 스마트공장이 제조업에 도입되기 시작하면서 외부망과의 접점이 증가하였다. 스마트공장은 생산성 및 안전성 향상 등의 이점을 가지나, 외부망과의 접점이 증가함으로써 보안 위협 또한 증가하게 되었다. 미국의 기술 회사인 IBM이 2022년 6월에 발표한 보고서에 따르면, 전 세계의 모든 업종 중 제조업이 23%로 가장 많이 사이버 공격을 받는 업종으로 조사되었다[1]. 사이버 공격으로부터 스마트공장을 효과적으로 보호하려면, 이에 관한 국제 표준을 준수할 필요성이 있다. 따라서, 본 논문은 스마트공장 보안을 위한 국제 표준화 동향을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트공장 보안과 관련 표준화 단체에 대해 설명하고, 3장에서는 IEC(International Electrotechnical Commission), IIC(Industry IoT Consortium), ITU-T(International Telecommunication Union Telecommunication Standardization Sector)의 스마트공장 보안 관련 표준화 동향을 소개한다. 마지막으로 4장에서는 논문의 내용을 요약하며 결론을 맺는다.

2. 관련 연구

2.1 스마트공장 보안

스마트공장에서는 제품을 설계하기 위한 도면 관리부터 제조, 운송, 판매, 서비스 제공까지 모든 제품 생명주기에 IT(Information Technology) 시스템을 사용할 수 있다. 이를 위해, 원자재, 기계, 설비, 운송수단, 인적 자원과 같이 스마트공장에서 활용되는 물리적 자원에 RFID(Radio-Frequency Identification) 혹은 바코드를 부착하여 디지털화함으로써 IT 시스템을 통한 관리를 가능하게 한다. 디지털화된 자원의 정보를 집계하고 분석하기 위해 사용하는 IIoT는 스마트공장의 재고관리, 품질관리, 유지보수관리 등의 운용 관리를 지원한다[2]. IIoT를 활용함에 따라 생산성 및 효율성의 향상이 가능하나, IIoT의 도입으로 인해 발생할 수 있는 보안 위협의 위험도는 증가하였다. IIoT는 상태 정보를 수집하는 센싱(sensing) 기능뿐만 아니라, 액추에이터(actuator)를 통해 공장의 설비를 원격으로 제어하는 기능을 가진다. 이러한 특징을 악용하여 공격자는 제품 생산에 직접적인 영향을 미칠 수 있으며, 이에 따라 제조 설비의 가용성을 침해하고, 작업자의 안전에 위협을 가하는 등의 다양한 위협을 발생시킬 수 있다.

스마트공장에서 나타날 수 있는 보안 위협은 장

비 및 시스템의 종류와 역할에 따라 다양하게 발생할 수 있다. 이뿐만 아니라 제품 생산을 위한 제조 과정부터 제품 판매 및 서비스까지 제조 전 과정에 걸쳐 다양한 경로를 통해 보안 위협이 발생할 수 있다. 이러한 스마트공장의 특성에 따라, 유럽사이버보안청(ENISA, European Union Agency for Cybersecurity)에서는 스마트공장의 가치사슬 전반에 걸쳐 장비 및 시스템에 영향을 미칠 수 있는 사이버보안 위협을 <표 1>과 같이 분류하였다[3]. 스마트공장의 장비 및 시스템에는 IIoT, 제어시스템, 네트워크 장비, 클라우드 서비스, 로봇 등 제조 목적을 달성하기 위해 사용되는 모든 OT와 IT 시스템을 포함한다. 이와 같은 자산들은 악의적인 공격자에 의해 활용 및 남용될 수 있으며, 이는 DoS(Denial of Service), 멀웨어, 변조, 타겟 공격, 개인정보 남용, 브루트 포스와 같은 방법으로 가능하다. 또한, 스마트공장의 장비 및 시스템에 대해 중간자 공격 및 세션 하이재킹, IoT 통신 하이재킹, 네트워크 정찰의 방법으로 도청 및 하이재킹이 가능하다.

<표 1> 스마트공장 보안 위협

분류	위협
악의적인 활동/남용	DoS
	멀웨어
	하드웨어 및 소프트웨어 변조
	정보 변조
	타겟 공격
	개인정보 남용
	브루트 포스
	중간자 공격, 세션 하이재킹
도청/하이재킹	IoT 통신 하이재킹
	네트워크 정찰

2.2 관련 국제 표준화 기구 및 단체

스마트공장의 보안에 관하여 국제적으로 표준화를 추진하고 있는 기구 및 단체는 IEC, IIC, ITU-T가 있다. IEC는 국제 표준화 기구로, 전기 및 전자 분야에서 사용되는 기술들에 대해 원론적이고 일반적인 표준화를 수행하고 있다. IEC에서는 스마트공장의 표준화를 위해서 IEC의 다양한 기술위원회 간 협업 강화를 위한 분과위원회인 SyC SM(Systems Committee for Smart Manufacturing)을 설립하여 운영하고 있다[4]. IIC는 산업 현장에서의 사물인터넷 적용과 관련된 기술, 표준, 보안 등을 연구하는 비영리 단체이며, 공식적인 국제 표준화 기구는 아니나 발간하는 출판물들이 표준으로써 제조 산업에 영향력을 미치고 있다. ITU-T는 국제 표준화 기구로, 정보통신 관점에서 다양한 분야에 적용 가능한 표준화를 수행하고 있다. ITU-T는 스마트공장의 표준화를 위한 별도의 위원회는 갖추고 있지 않으나, 보안을 위한 그룹인 ITU-T SG17(Study Group 17)이 존재하며, 스마트공장에 관한 보안은 주로 사물인터넷 보안 분과인 Q6/17에서 논의되는 추세이다[5].

3. 국제 표준화 동향

본 장에서는 2장에서 분석한 내용을 바탕으로 스마트공장 보안을 위한 국제 표준화 동향을 살펴본다. 이를 위해, 스마트공장의 OT 시스템 중 주요 공격 지점이 되는 제어시스템과 IIoT를 중점으로 표준화 현황을 분석한다. <표 2>는 주요 국제 표준화 기구 및 단체의 스마트공장 보안 표준화 동향을 분석한 표이다.

<표 2> 표준화 동향

단체명	문서 번호(약어)	문서 제목
IEC	IEC 62443	Industrial communication networks - Network and system security
IIC	IIC IISF	Industry Internet of Things Security Framework
	IIC TFF	The Industrial Internet of Things Trustworthiness Framework Foundations
	IIC SMM	IoT Security Maturity Model : NIST Cybersecurity Framework 1.1 Mappings
ITU-T	ITU-T X.1352	Security requirements for Internet of things devices and gateways
	ITU-T X.sr-iiot	Security requirements for the industrial Internet of things based smart manufacturing reference model

- IEC 62443: 해당 문서는 자동화 및 제어시스템에 대한 사이버보안을 다루는 시리즈 표준 문서로, 사이버보안에 대해 총 4가지의 범주(일반, 정책 및 절차, 시스템, 구성요소)로 구분한다. 각 범주를 위한

보안 위험 평가, 보안 요구사항 등을 정의한다[7].

- IIC IISF: 해당 문서는 IIoT 보안을 위한 프레임워크를 정의한다. 프레임워크는 보안 및 개인정보 보호 위협과 관련된 위험을 식별 및 평가하고, 이를 완화하는 방법을 설명한다[8].
- IIC TFF: 해당 문서는 OT 및 IT의 시스템 생명주기 전반에 걸쳐 신뢰성을 고려해야 할 필요성을 강조하며, 산업 보안을 위해 고려해야 할 신뢰성의 개념을 정의한다[8].
- IIC SMM: 해당 문서는 NIST(National Institute of Standards and Technology)의 사이버보안 프레임워크 1.1 가이드라인에 기반하여, IoT의 보안 성숙도 모델을 정의한다. 또한, 이를 위한 일반 지침 및 고려사항을 제공한다[9].
- ITU-T X.1352: 해당 문서는 ITU-T Y.4100 권고안에 정의된 IoT 참조 모델과 ITU-T X.1361 권고안에 정의된 IoT 보안 프레임워크를 기반으로 IoT 디바이스 및 게이트웨이의 보안 위협과 취약성을 식별한다. 또한, 보안 위협과 취약성을 완화하기 위한 보안 요구사항을 정의한다[10].
- ITU-T X.sr-iiot: 해당 문서는 ITU-T에서 개발 중인 문서이다. 이는 스마트공장에 관해 정의한 ITU-T Y.4003 문서의 IIoT 기반 스마트공장 참조 모델을 바탕으로, IIoT 기반 스마트공장에서 발생 가능한 보안 위협을 식별하고 이에 대응 가능한 보안 요구사항을 정의한다[11].

4. 결론

본 논문에서는 기존에 폐쇄망으로 운영되어 외부와의 접점이 적었던 공장에, IT를 접목함으로써 악의적인 공격자들의 타깃이 되고 있는 스마트공장을 위한 보안 관련 표준화 동향을 분석하였다. IEC, IIC, ITU-T의 표준화 동향을 분석한 결과, IEC 62443과 같은 제어시스템 보안에 관한 체계적인 표준 문서가 존재하나, 최근 들어 스마트공장에서 두드러지는 공격 경로인 IIoT를 고려한 표준화 현황은 미비한 것으로 나타났다. 또한, 출판된 IIoT 관련 표준 문서들은 주로 보안 프레임워크 혹은 지침과 같은 원론적인 수준의 내용을 담고 있다. 이에 더 나아가 스마트공장의 보안 위협을 탐지 및 대응하기 위한 기술적 수준의 표준이 요구된다. 따라서, 스마트공장 보안에 관한 적극적인 표준화 연구가 필요할 것으로 판단되며, 이를 통해 스마트공장의 보안 강화에 기여할 수 있을 것으로 기대된다.

Acknowledgement

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00796, 상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구). 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 정보통신방송혁신인재양성(메타버스융합대학원) 사업 연구결과로 수행되었음(IITP-2023-RS-2023-00254529).

참고문헌

[1] “스마트공장 사이버 공격 급증”, [Online]. Available: https://biz.chosun.com/it-science/ict/2022/06/, [Accessed: 2024-04-24].

[2] “ITU-T Y.4003 Overview of smart manufacturing in the context of the industrial Internet of things”, [Online]. Available: https://handle.itu.int/11.1002/1000/13634, [Accessed: 2024-03-11].

[3] ENISA, “Good Practices for Security of Internet of Things in the context of Smart Manufacturing”, November 2018.

[4] “Smart manufacturing”, [Online]. Available: https://www.iec.ch/smart-manufacturing, [Accessed: 2024-03-11].

[5] “Question 6/17 (Study Period 2022-2024)”, [Online]. Available: https://www.itu.int/net4/ITU-T/lists/q-text.aspx?Group=17&Period=17&QNo=6&Lang=en, [Accessed: 2024-03-11].

[6] “Integration of DTC® & IIC® Programs”, [Online]. Available: https://www.iiconsortium.org/, [Accessed: 2024-04-24].

[7] “Understanding IEC 62443”, [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443, [Accessed: 2024-04-24].

[8] “Foundational Publications”, [Online]. Available: https://www.iiconsortium.org/foundational-publications/, [Accessed: 2024-04-24].

[9] “Security Maturity Model”, [Online]. Available: https://www.iiconsortium.org/smm/, [Accessed: 2024-04-24].

[10] “ITU-T X.1352 (09/2022)”, [Online]. Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14990, [Accessed: 2024-04-24].

[11] “ITU-T work programme”, [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=19082, [Accessed: 2024-04-24].