정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

5G 기반의 스마트공장 보안 동향 분석

권 순 현*, 김 지 윤**, 임 재 덕***, 유 일 선**

요 약

ICT의 발달과 제조업의 융합으로 4차 산업혁명이 가속화되면서 전통적인 제조공정의 과정이 네트워크화되어 효율화, 지능화, 최적화하는 동시에, 시뮬레이션을 통한 생산 설비 관리 및 개선, 데이터를 통한 시장 분석 등이 가능할 것으로 전망되고 있다. 이러한 높은 부가가치를 갖는 스마트공장 기술은 악의적인 공격자의 주요 목표가 될 것으로 우려되며, 스마트공장에 대한 사이버 공격은 생산 공정 정보, 기밀정보 유출, 매출 손실, 인명 피해 등을 유발할 수 있다. 이에 따라, 스마트공장의 안전한 정착 및 활용을 위하여 국제표준화기구에서는 스마트공장에 특화된 표준의 제정이 진행되고 있다. 본 논문에서는 예상되는 스마트공장의 보안 위협 및 보안 요구사항에 대하여 살펴보고, 이에 대처하기 위한 스마트공장 보안 표준 등을 분석한다.

Ⅰ. 서 론

5G의 등장과 통신기술의 발달은 제조업 분야와 ICT(Information & Communication Technology)의 융합을 기반으로 하는 4차 산업혁명을 가속화시켰다. 이에 따라, 제조설비와 생산 전 과정이 네트워크와 연결되어 생산 프로세스를 개선하고, 시장의 동향과 설비의 관리를 효율적으로 관리할 수 있는 스마트공장이 등장하였다. 한국산업표준 ‘KS X 9001’에서는 스마트공장을 제품의 기획, 설계 생산, 유통, 판매 등 전통적인 제조산업의 전 과정을 AI, 빅데이터, 클라우드 등의 ICT 기술로 통합하여, 최소한의 제조공정 비용과 시간으로 고객 맞춤형 제품 생산을 지향하는 공장으로 정의하고, 생산성 향상, 에너지 절감, 인간 중심의 작업환경 구현, 개인맞춤형 제조, 융합 등 새로운 제조환경에서 능동적인 대응이 가능할 것으로 예상하고 있다[1-3]. 또한, 스마트공장은 네트워크를 활용한 데이터 수집/분석, 생산 프로세스 개선/최적화, 생산시스템 예측 시뮬레이션 등을 통해 제조 혁신을 실현하고 새로운 부가가치를 창출할 수 있을 것으로 기대된다[4].

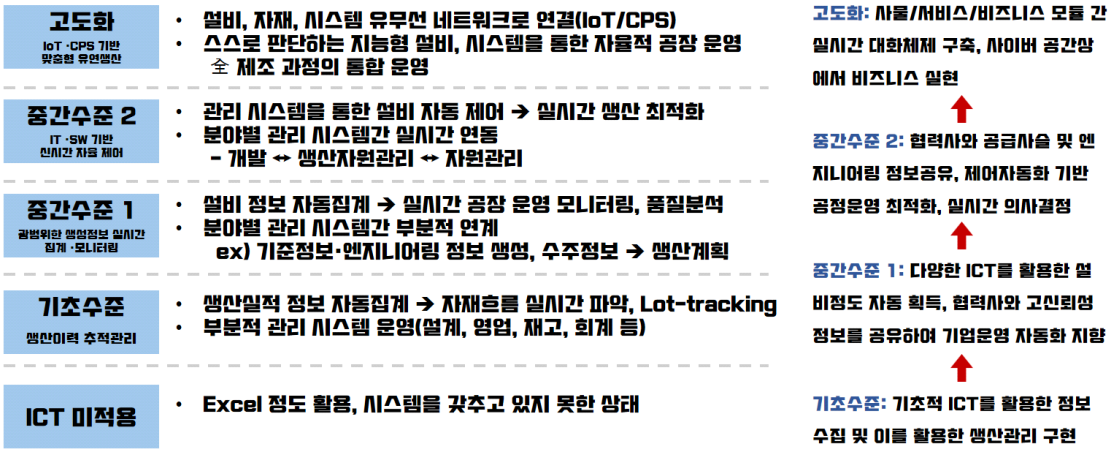
한편, 제조공정의 지능화와 최적화를 가능하게 하는 스마트공장은 새롭고 다양한 보안 위협이 존재하고 이에 따라 새로운 사이버 공격 대상이 될 것으로 우려되고 있다. 특히, 복잡하고 정밀한 스마트공장의 특성상 사이버 공격으로 인하여 일부 설비가 마비될 경우 그 규모와 피해가 클 것으로 예상된다[5]. 따라서, 보안은 스마트공장의 안전한 운영 환경을 위해서 필수적인 요소이다.

스마트공장은 크게 정보통신기술을 기반으로 하는 ICT 환경과 생산기술을 기반으로 하는 OT(Operational Technology) 환경으로 구분된다. 기존 제조 산업의 보안이 OT 환경에 집중된 모습을 보였다면 스마트공장으로의 변화가 이루어지면서 현재 제조 산업에서는 악의적인 공격자가 접근하기 쉬운 ICT 환경에 대한 보안도 중요해 지고 있어, ICT 환경까지 확장된 보안 요구가 높아지고 있다[5,6].

이러한 현장의 요구를 수용하여 국제표준화기구인 IEC(International Electrotechnical Commission) 위원회[7]에서는 IEC 62443과 같은 스마트공장 보안에 관한 표준을 제정하고 있다. 표준을 활용한 일관적인 보안은 스마트공장 보안의 효율을 극대화하고 다양한 보안 솔루션의 적용을 편리하게 한다.

최근에는 보안 표준뿐만 아니라, 스마트공장과 관련한 다양한 연구가 진행 중이다. 우선, 5G 사설망을 적용하여 특정 시설의 보호 및 접근 제어, 서비스 최적화를 기대할 수 있다. 또한, 네트워크 슬라이싱 기술을 활

* LS 글로벌 (tnsgus08@gmail.com)
** 순천향대학교 정보보호학과 (74jykim@sch.ac.kr, isyou@sch.ac.kr)
*** 한국전자통신연구원 (jdscol92@etri.re.kr)



〔그림 1〕 스마트공장 단계별 구성

용해 스마트공장에서 요구되는 환경, 성능, 특성을 수용한 전용 네트워크를 구성할 수도 있다. 5G 사설망 혹은 네트워크 슬라이싱을 활용하여 스마트공장을 구축한다면 이에 특화된 보안을 설계할 필요가 있다.

본 논문의 구성은 다음과 같다. 2장에서는 예상되는 스마트공장 보안 취약점 및 보안 요구사항에 대하여 살펴보고, 3장에서 스마트공장의 보안 표준을 분석한다. 마지막으로, 4장에서 본 논문의 결론을 제시한다.

Ⅱ. 5G 스마트공장

사물인터넷(IoT), 인공지능, 빅데이터, 클라우드 등의 발달된 ICT 기술이 제조 분야와 융합되는 스마트공장이 전 세계적인 산업혁신을 주도하고 있다. 스마트공장은 공장자동화 수준을 넘어서 ICT 기술이 융합된 지능적인 생산체계를 갖춘 소비자 중심의 지능화된 공장을 의미한다. 네트워크를 활용하여 데이터를 수집 및 분석하고, 분석된 데이터에 따라 소비자 맞춤형 제품을 생산하고 피드백을 통한 품질 관리 및 제어를 수행한다. 또한, 에너지, 인력 등의 자원 활용을 효율적으로 수행하고, 생산 원가의 하락 및 제품 경쟁력 강화를 기대할 수 있다.

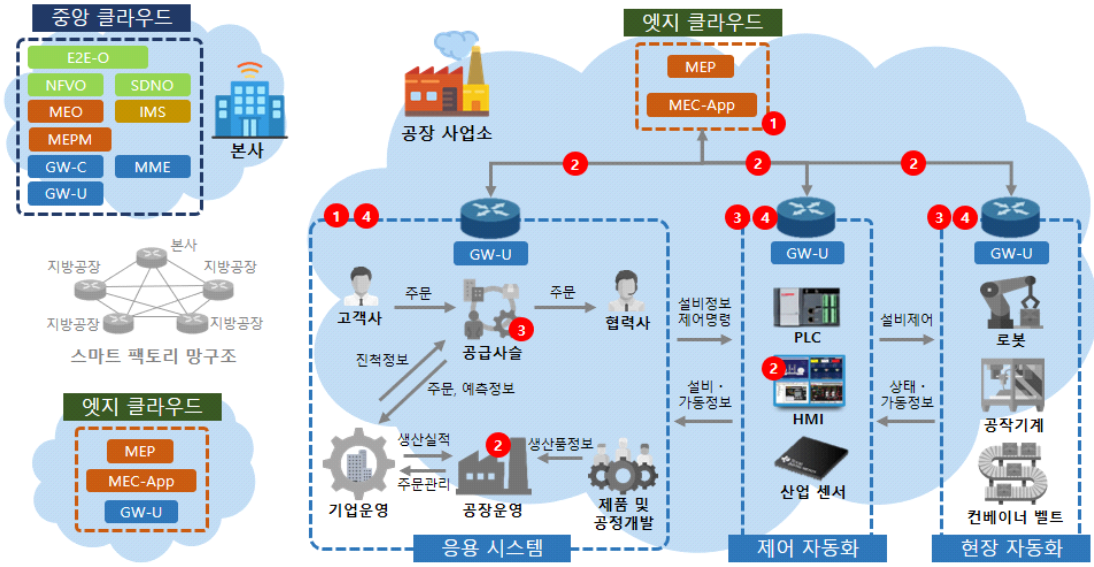
특히, 국내에서는 제조업의 성장 동력 강화를 목표로 제조업과 IT 융합을 통한 생산현장, 제품, 지역생태계를 혁신하고 성공 사례를 조기 창출하여 제조업 전반으로 확산하고자 '제조업 혁신 3.0' 전략을 추진하고 있으며, 스마트공장추진단[8]을 설립해 적극적으로 스마트공장 보급 사업을 진행하고, 정부에서는 [그림 1]과 같이 스마트공장 구현 단계를 정의하여 관련 지원 사업을 진행하고 있다.

또한, 5G에서는 초저지연 특성을 통해 기존 4G에서 발생 가능한 전송지연 문제점이 극복되었으며, 초고속 특성을 통해 스마트공장 내의 많은 기기들이 대용량의 데이터를 지연 없이 빠르게 송·수신 할 수 있게 되었다. 더욱이, 초연결 특성을 기반으로 수많은 센서를 통해 광범위한 공장의 제품·장비 등을 동시에 연결하여 실시간 모니터링 및 제어가 가능하게 되었다. [표 1]은 4G와 5G의 중요 특성을 비교한 것이다.

〔표 1〕 4G와 5G 주요 특징 및 규격 비교

구 분	4G	5G
전송속도	1Gbps	20Gbps
전송지연	10ms	1ms
최대 연결 기기	10^5 /km^2	10^6 /km^2
면적당 처리 용량	0.1 Mbps/m^2	10 Mbps/m^2

기존의 공장은 생산시스템에 필요한 운영 기술인 OT 영역으로 구분되었으며, 네트워크 또한 분야별 폐쇄적인 구조로 되어 있었다. 하지만 현재의 5G 스마트공장은 개방형 네트워크 구조를 가지며, 모든 기기 및 설비가 인터넷에 연결된 형태이므로 상대적으로 많은 보안 위협에 노출되어 국내·외에서 피해사례가 급증하고 있다. 가용성이 최우선되는 스마트공장에서 해킹 등



〔그림 2〕 스마트공장 영역별 보안 위협

의 보안 사고는 엄청난 매출 손실을 유발할 수 있어 이를 위한 보안 대책의 중요성이 강조되고 있다.

2.1. 5G 스마트공장 보안 위협

앞서 설명한 것과 같이 5G 스마트공장은 폐쇄적 구조를 갖는 OT영역에 5G 기반으로 운영되는 IT 기술이 융합되어 개방된 구조를 갖게 되고 OT 영역과 IT 영역 사이에 데이터 송·수신이 가능해짐에 따라 IT 영역에서 발생 가능한 보안위협이 OT 영역으로 전이될 수 있게 되었다. 또한, 개방된 구조의 스마트공장을 대상으로 한 공격은 접점이 다양화 및 지능화 되고, 관리 대상이 대규모화 되었으며, 위협 확산이 가속화되는 등 보안 위협의 규모와 이에 따른 피해가 더욱 커지고 있다[5]. 아래는 최근 5년동안 OT 시스템을 대상으로 발생한 보안 사고 중 일부를 정리한 것이다[6].

- 2019, 노르웨이 알루미늄 생산 업체 랜섬웨어 공격 피해
- 2019, 벨기에 비행기 부품 공급 업체 랜섬웨어 공격 피해
- 2018, 대만 반도체 업체 랜섬웨어 공격 피해
- 2017, 일본 자동차 공장 랜섬웨어 공격 피해
- 2017, 미국 제약회사 랜섬웨어 공격 피해
- 2017, 덴마크 해운 업체 랜섬웨어 공격 피해
- 2015, 독일 철강회사 해킹 공격 피해

〔표 2〕 스마트공장 보안 위협

위협 종류	세부 내용
① 악의적인 활동	- DDoS 공격: 대량 데이터 전송으로 시스템 서비스 방해 - 멀웨어: 악의적 SW 침투 및 무단 실행으로 OT 시스템 등 손상 - 무작위 공격: 암호키 추측을 위한 무작위 시도 및 불법 접근권한 획득 - HW/SW 무단 조작 - 정보 조작, 표적 공격, 개인정보 유출
② 도청	- 중간자 공격: 통신 데이터 유출 혹은 누출 - IoT 통신 프로토콜 하이재킹: 기존 통신 세션 제어 - 네트워크 정보 유출: 내부 네트워크 정보 노출
③ 물리적 공격	- 기기의 물리적 손상 행위로 인한 직간접적인 시설 파괴
④ 고장/오작동	- 센서, 액추에이터 고장 또는 오작동 - 제어 시스템 고장 또는 오작동 - SW 취약점 악용 및 서비스 제공 업체의 실수 또는 중단

위와 같이 OT시스템을 대상으로 점차 지능화되고 증가하는 보안 위협에 효과적으로 대응하기 위해서는 보안 위협의 원인 및 보안 취약점 분석을 통해 보안 대책을 마련하는 것이 중요하다. [그림 2]와 [표 2]는 5G 스마트공장 구조에 기반하여 영역별 발생할 수 있는 보안 위협을 분석한 것이다.

[그림 2]에서 스마트공장은 5G의 구성요소 중 MEC-App(Mobile Edge Computing Application) 기반의 엣지 클라우드로 구성되며, 응용시스템, 제어 자동화, 현장 자동화 영역으로 구분될 수 있다. 구분된 각 영역의 데이터는 CU(Cloud Unit) 및 User Plane 데이터를 처리하는 GW-U에 의해 처리된다. 여기서 응용시스템 영역은 IT영역으로 구분되는데 DDoS 또는 악성코드에 의해 보안 위협이 발생할 수 있으며, 각 영역과 MEC 사이에서 중간자 공격, 하이재킹 등의 보안 위협이 발생할 수 있다.

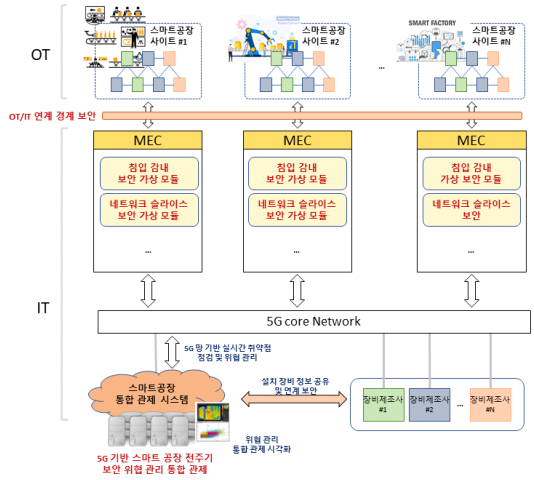
2.2. 5G 스마트공장 보안 요구사항

5G 스마트공장은 일반적인 스마트공장과 달리 공장 내 IT시스템 및 기기들이 5G 환경을 기반으로 구성되어 있어서 이를 고려한 보안 요구사항이 필요하다. [그림 3]은 5G 스마트공장의 개념도를 중심으로 정리된 보안 요구사항을 나타낸 것이며, 크게 네 가지 부분으로 나누어 보안 요구사항을 정의할 수 있다. 이는 다음과 같다.

① 5G 기반 스마트공장 제조 장비의 전 주기 보안 위협을 통합 관제

스마트공장 운영의 가용성 및 안전성을 보장하기 위해서는 제조 장비의 도입부터 폐기 시까지 전 주기에 걸쳐 위협 관리가 이루어져야 하며, 이를 위한 보안 요구사항은 다음과 같다.

- 다양한 제조사와의 안전한 정보 공유 및 정보 유출 방지 체계
- 대규모 제조 장비 위협 관리를 위협 정보 공유 및 관리
- OT영역 경계에서 IT영역과의 연결을 담당하는 MEC 장비 기반의 안전한 데이터 공유 구조
- 방대한 정보를 통해 신속한 정보 제공 및 대응을 위한 실시간 시각화



〔그림 3〕 5G 스마트공장 구조에서의 보안 요구사항 정의

② 5G 엣지 컴퓨팅 보안을 위한 네트워크 슬라이스 보안

5G 스마트공장 내 IoT 장비들은 5G 네트워크에 접근을 위한 1차 인증(Primary Authentication) 이후에 MEC에 장착된 스마트공장 응용 간 별도의 특화된 인증(Secondary Authentication)을 통해 각 응용 별 네트워크 슬라이스를 구성한다. 이 네트워크 슬라이스를 위한 보안 요구사항은 다음과 같다.

- 동일한 자격증명 기반의 1차/2차 인증 연동
- 5G 스마트공장 구조 및 어플리케이션 보안 요구에 따른 다양한 유형의 2차 인증 모델링
- 2차 인증과 5G 스마트공장 네트워크 슬라이스의 연계 및 키 관리
- 가용성 보장을 위한 비신뢰장치-격리 네트워크 슬라이스 관리
- 네트워크 슬라이스 기반 5G 스마트공장 모니터링

③ 스마트공장 가용성 보장을 위한 MEC 기반 위협/침입 감내

스마트공장에서는 가용성이 최우선 보장되어야 하므로 사전에 위협 징후를 탐지하여 대응하는 것이 중요하다. 스마트공장 내 장비 및 센서, 액추에이터 등은 다양한 전용 통신 프로토콜을 사용하므로 OT 내에 침입한 위협 혹은 OT 장비의 오작동 등의 이상 현상을 탐지하기 위해서는 프로토콜 별 전용 위협 대응 모델링 및 사전 탐지 기술이 필요하다. MEC 기반 위협/침입 감내를 위한 보안 요구사항은 다음과 같다.

- 스마트공장 주요 장비별 위협 대응을 위한 장비별 고유 특성 자가 학습
- 스마트공장 표준 프로토콜 기반 보안 위협 사전 예측을 위한 도메인 특화형 고유 특성 자가 학습
- 기존 산업용 프로토콜 기반 보안 위협 사전 예측을 위한 도메인 특화형 고유 특성 자가 학습
- 의미 있는 위협 대응을 위한 자가 학습 모델 기반 지능형 보안 위협 사전 예측 및 대응

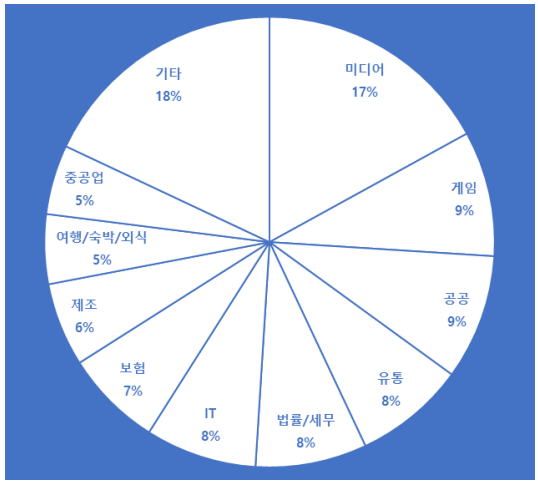
④ OT/IT의 안전한 연계를 위한 경계 보안

5G와 IoT 기반의 스마트공장을 운영하기 위해서는 OT와 IT 영역 간 연결은 필수적이며, 공장 내 기밀 데이터 유출 및 외부 침입을 방지하는 강화된 경계망 보안은 필수이다. 현재는 OT 영역 내부 침입을 원천적으로 차단하기 위해 단방향 GW를 사용하고 있으나 구축 비용이 높고 데이터 선별 적용이 까다롭다는 단점이 있다. 접근 권한에 따라 OT 영역 내 자원 및 데이터 접근에 대한 보안을 위한 경계 보안 요구사항은 다음과 같다.

- OT 영역 가용 자원 및 데이터 보호를 위한 권한 설정 및 자원 접근제어 모델링
- OT 영역 가용 자원 및 데이터 보호를 위한 자동화된 접근제어 정책 관리
- 세분화 된 OT 영역 내 자원/데이터 다단계 접근제어 집행

Ⅲ. 스마트공장 보안 표준 동향

오늘날 국내 제조업 분야에서는 스마트공장의 정착을 위하여 스마트공장 보급확산 사업과 같은 지원을 통해 중소기업을 대상으로 스마트제조 환경을 구축하고 있다. 그러나, 보안 기술을 적용하지 못한 상태의 스마트공장 기술을 보급하고 있어 새로운 네트워크 환경에서 발생할 수 있는 보안위협 및 공격에 취약한 실정이다[9]. 특히, [그림 4]와 같이 전체 사이버 공격 중 스마트공장과 같은 산업제어시스템에 대한 공격의 비중이 6%에 달하고 있다. 이는 2018년도 비해 125%가 증가한 수치로 21만여 건에 달하며 산업제어시스템에 대한 사이버 공격이 점차 증가하고 있음을 알 수 있다[10]. 따라서, 스마트공장의 보안 위협 및 공격을 사전에 방지하고 각 시스템이 상호보완하기 위한 국제표준의 도입이 시급하다.



〔그림 4〕 2019년 사이버 공격 동향 통계

3.1. IEC

국제표준화기구 IEC에서는 스마트공장 보안을 위하여 '산업용 통신 네트워크 - 네트워크 및 시스템 보안'이라는 주제로 IEC 62443 표준의 제정을 진행하고 있다. 5G의 등장으로 스마트공장의 정착이 가속화되면서 IEC 위원회에서는 표준 개발 기간을 단축하기 위하여 미국 ISA(International Society of Automation)[11] 99 위원회에서 제안한 ISA 62443을 IEC 표준안으로 준용하였다.

IEC 62443 시리즈는 총 4개의 하위 문서로 구성되어 있으며 각각 일반, 정책 및 절차, 시스템, 구성요소를 서술하고 있다. 각 하위 문서는 모듈러 보안 구조를 기반으로 설계되어 호환성을 지원하고, 주제에 따라 세부 문서로 나누어 서술하고 있다. IEC 62443 시리즈에 대한 정리는 [표 3]과 같다[6,12].

(1) IEC 62443-1 (일반): 산업용 통신 네트워크의 개념 및 모델, 용어 등의 일반적인 사항에 관하여 규정함.

- IEC 62443-1-1(Terminology, concepts and models): ISA 62443의 개념, 모델, 용어를 소개함.
- IEC 62443-1-2(Master glossry of terms and abbreviations): IEC 62443에서 사용되는 용어 및 약어에 관하여 정의함.

〔표 3〕 IEC 62443 시리즈

상위	하위	세부	주제
IEC 62443	62443-1 (일반)	62443-1-1	개념 및 모델
		62443-1-2	용어 및 약어
		62443-1-3	시스템 보안 적합성 매트릭스
		62443-1-4	IACS 보안 생명주기 및 사용 사례
	62443-2 (정책 및 절차)	62443-2-1	자산 소유자의 보안 프로그램 요구사항
		62443-2-2	IACS 보호수준
		62443-2-3	패치관리
		62443-2-4	서비스 공급자의 보안 프로그램 요구사항
		62443-2-5	자산 소유자의 구현 지침
	62443-3 (시스템)	62443-3-1	IACS 보안 기술
		62443-3-2	보안 위험 평가 및 시스템 설계
		62443-3-3	시스템 보안 요구사항 및 보안 수준
	62443-4 (구성요소)	62443-4-1	안전한 제품개발 생명주기 요구사항
		62443-4-2	기술적 보안 요구사항

- IEC 62443-1-3(System security compliance metrics): IEC 62443의 사이버보안 적합성 측정 기준을 제시함.
- IEC 62443-1-4(IACS security lifecycle and use case): IACS 보안 생명주기를 정의하고 실증 사례를 제시함.

(2) IEC 62443-2 (정책 및 절차): 산업제어시스템을 보유하는 자산 소유자 및 서비스를 제공하는 공급자의 보안 정책 및 절차에 관하여 규정함.

- IEC 62443-2-1(Establishing an IACS security program): IACS를 위한 사이버보안 관리 시스템(CSMS; Cyber Security Management System)을 구성하기 위한 요소를 정의하고, 방법론을 제시함.
- IEC 62443-2-2(Implementation guidance for an IACS environments): IACS 환경을 위한 구현 가이드라인 및 운영 방안을 제시함.
- IEC 62443-2-3(Patch management in the IACS environment): 구축된 IACS의 패치 관리를 위한 요구사항 및 형식을 정의함.
- IEC 62443-2-4(Installation and maintenance requirements for IACS suppliers): IACS 공급 업체의 설치 및 유지보수 요구사항을 정의함.

(3) IEC 62443-3 (시스템): 안전한 산업제어시스템 설계를 위하여 보안 요구사항, 보안 수준, 위험 평가, 설계, 보안 기술에 관하여 규정함.

- IEC 62443-3-1(Security technologies for IACS): IACS에 적용이 가능한 사이버보안 기술 및 제품을 제시하고, 이에 대한 평가를 기술함.
- IEC 62443-3-2(Security levels for zones and conduits): IACS에 대하여 SuC(System under Consideration)를 정의하고 위험평가 및 보안수준의 목표를 수립함. 또한, 보안 요구사항을 문서화하기 위한 요소를 정의함.
- IEC 62443-3-3(System requirements and security levels): 산업제어시스템의 시스템 요구사항 및 보안 수준을 정의하고, IEC 62443 내에서 제시한 보안 요소에서 필요한 서비스 및 기능을 서술함.

(4) IEC 62443-4 (구성요소): 산업제어시스템을 구성하는 장치 및 어플리케이션의 생명주기 요구사항 및 기능적 요구사항에 관하여 규정함.

- IEC 62443-4-1(Product development requirements): 공급자가 제품을 개발 및 공급하기 위해 준수해야 하는 보안개발 생명주기를 정의하고, 이에 대한 요구사항을 기술함.
- IEC 62443-4-2(Technical security requirements for IACS components): 산업제어시스템의 구성요소에 대한 기술적 요구사항(CR)을 정의함.

3.2. 국가기술표준원

국내에서도 스마트공장 분야의 보급과 확산을 위하여 표준화 추진 전략을 수립하고 있다. 국가기술표준원[13]에서는 재단법인 민관합동 스마트공장추진단과의 연계를 통해 업종별 표준 참조모델을 개발하고, 이를 통해 스마트공장의 구성 모델, 기능 요소, 정보 교환 모델, 표준화 항목 및 현황 등에 대한 로드맵 개발을 진행하

〔표 4〕 KS 표준

상위	하위	주제
KS X 9001	9001-1	기본 개념과 구조
	9001-2	용어
	9001-3	운영관리시스템 (진단 평가 모델)
	9001-4	참조 모델(미정)

고 있다. 또한, 국가기술표준원은 스마트공장 보급 및 확산의 국제적 추세를 따라가기 위하여 KS 국가표준 개발을 지원하고 KS 표준을 발간하였다. KS 표준에 대한 정리는 [표 4]와 같다.

(1) KS X 9001-1 (기본 개념과 구조): 국제전기기술위원회(IEC) 전략 그룹(SG8)의 '인더스트리 4.0: 스마트공장'의 프레임워크를 기반으로 작성된 표준임. 스마트공장에 대한 기본 개념 및 구조를 포함하여 목표, 현황, 전략 등에 대하여 분석함.
(2) KS X 9001-2 (용어): 국내외에서 사용되는 스마트공장 관련 용어의 이해를 통일하기 위하여 용어를 정의함.
(3) KS X 9001-3 (운영관리시스템 (진단 평가 모델)): 스마트공장의 운영관리시스템의 설계 및 실행에 필요한 요구사항을 규정함.
(4) KS X 9001-4 (참조 모델): 미정

Ⅳ. 결 론

본 논문은 5G 스마트공장의 개념과 보안 위협, 보안 요구사항, 관련 국내 및 국제 표준에 대하여 분석하였다. 스마트공장은 4차 산업혁명을 이끄는 주요 기술로서 주목받고 있으나 안전한 도입 및 활용을 위해서는 보안에 대한 연구가 보다 필요한 상황이다. 한편, 5G의 등장으로 초고속, 초저지연, 초연결을 활용한 새로운 스마트공장 모델이 등장할 것으로 기대된다. 다만, 5G와 5G 기반의 어플리케이션에서 새롭게 등장할 수 있는 보안 위협에 대한 분석 및 대응방안 연구가 필요하고, 해당 어플리케이션에 특화된 인증 프레임워크 개발이 요구된다. 5G 기반의 스마트공장 서비스의 안전한 도입은 제조, 운영, 통신, 정책, 보안 등의 다양한 분야에서 상호 협력을 통한 기술 개발이 필수적이며, 이를 위하여 관·산·학·연의 적극적인 교류 및 연계가 필요할 것으로 생각된다.

참 고 문 헌

[1] 국가기술표준원, "*스마트공장 - 제1부: 기본 개념과 구조*", KS X 9001-1:2016, June 2016.
[2] 국가기술표준원, "*스마트공장 - 제2부: 용어*", KS X 9001-2:2016, June 2016.
[3] 국가기술표준원, "*스마트공장 - 제3부: 운영관리시스템(진단 평가 모델)*", KS X 9001-3:2016, June 2016.
[4] 조혜지, 김용균, "*스마트공장 기술 및 산업 동향*", 정보통신기술진흥센터 주간기술동향, 1849, pp. 15-25, June 2018.
[5] 배병환, "*주요국 스마트공장 보안 동향 분석 및 시사점*", 정보통신기술진흥센터 주간기술동향, 1920, pp. 14-26, October 2019.
[6] 한근희, "*스마트공장 보안과 표준*", 한국통신학회지(정보와통신), 36(6), pp. 41-46, May 2019.
[7] IEC, https://www.iec.ch/
[8] 스마트공장추진단, https://www.smart-factory.kr/
[9] 한국전자통신연구원, "*스마트 제조 기술 및 표준*", ETRI Insight 표준화동향 2018-01, Jan. 2018.
[10] 길민권, "*안랩, '2019년 사이버 공격 동향 통계' 발표*", 데일리시큐, https://www.dailysecu.com/news/ articleView.html?idxno=98227, Jan. 2020.
[11] ISA, https://www.isa.org/
[12] IEC, "*Industrial communication networks - Network and system security*", IEC 62443-1-1 ~ 62443-4-2, June 2020.
[13] 국가기술표준원, https://www.kats.go.kr/

〈저 자 소 개〉

권 순 현 (Soonhyun Kwon)
정회원
2019년 2월 : 순천향대학교 정보보호학과 석사 졸업
2019년 3월~현재 : LS 글로벌 Associate Consultant
<관심분야> 정보보호, 스마트공장 보안, 5G, 기업보안

김 지 윤 (Jiyoon Kim)
학생회원
2019년 2월 : 순천향대학교 정보보호학과 석사 졸업
2019년 2월~현재 : 순천향대학교 정보보호학과 박사과정 중
<관심분야> 정보보호, 5G, 이동통신 보안, 정형화 검증

임 재 덕 (Jae-Deok Lim)
정회원
2001년 2월 : 경북대학교 전자공학과 석사 졸업
2013년 2월 : 충남대학교 컴퓨터공학과 박사 졸업
2000년 12월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> 사물인터넷 보안, 운영체제 보안, 접근제어, 모바일 보안, 시스템 보안

유 일 선 (Ilsun You)
종신회원
2002년 2월 : 단국대학교 전산통계학과 박사 졸업
2008년 3월 : 한국성서대학교 정보과학부 조교수
2012년 3월 : 한국성서대학교 정보과학부 부교수
2015년 9월 : 순천향대학교 정보보호학과 부교수
2020년 9월~현재 : 순천향대학교 정보보호학과 교수
<관심분야> 인증 및 접근통제, 이동통신보안, 인터넷 보안, 정형화 보안 검증