# IEC 62443 표준 적용을 통한 산업제어시스템 보안성 강화 연구

진정하*, 김준태*, 박상선* 한근희*
*고려대학교 정보보호연구원
nemoda75@korea.ac.kr, tae8579@gmail.com, sitcs@naver.com, khhan1@korea.ac.kr

# A Study on the Security Enhancement of the Industrial Control System through the Application of IEC 62443 Standards

Jungha Jin*, Juntae Kim*, SangSeon Park*, Keunhee Han*
*Dept. of Institute of Cyber Security & Privacy, KOREA University

요 약

SME(small and medium sized enterprise) 환경의 스마트공장 환경에서는 실제 제조라인에서 동작하는 센서(Sensor) 및 액추에이터(Actuator)와 이를 관리하는 PLC(Programmable Logic Controller), 더불어 그러한 PLC를 제어 및 관리하는 HMI(Human-Machine Interface), 그리고 다시 PLC와 HMI를 관리하는 OT(Operational Technology)서버로 구성되어 있으며, 제어자동화를 담당하는 PLC 및 HMI는 공장운영을 위한 응용시스템인 OT서버 및 현장 자동화를 위한 로봇, 생산설비와의 직접적인 연결을 수행하고 있어서 스마트공장 환경에서 보안 기술의 개발이 중점적으로 필요한 영역이다. 이러한 SME 환경의 스마트공장 보안 내재화를 이루기 위해서는, 스마트공장 SW 및 HW 개발 단계에서 IEC 62443-4-1 Secure Product Development Lifecycle에 따른 프로세스 정립 및 IEC 62443-4-2 Component 보안 요구사항과 IEC 62443-3-3 System 보안 요구사항에 적합한 개발 방법론의 도입이 필요하다.

## 1. 서론

글로벌 보안기업인 포티넷에 따르면 2010년 스턱스넷 공격을 기점으로 SCADA(Supervisory Control And Data Acquisition), 산업제어시스템(ICS: Industrial Control System), 운영기술(OT) 환경을 운영하는 공장, 발전소 등 산업시설·기반시설에 대한 사이버공격이 전세계적으로 지속적으로 증가하여 발생하고 있으며, 미국의 ICS·OT 보안 전문기업인 사이버엑스(CyberX)는 최근 전세계 제조·철강·엔지니어링·화학 분야 200개 이상 기업의 시스템들에 대해 데이터 탈취 등을 노린 지능형지속위협(APT) 공격이 진행중이며, '강남 인더스트리얼 스타일(Gangnam Industrial Style)'이라고 명명된 이 캠페인의 공격 대상 기업 가운데 약 60%가 한국 내 기업으로 조사되어 한국도 ICS·OT 보안에서 예외가 아님이 밝혀지고 있어서, 산업제어시스템에 대한 사이버공격이 증가하고 있는 추세에 비례하여, 대응하는 연구가 다소 미진한 현실이다.[1][2]

특히, 미국에서는 9.11 테러 이후 미국내 기반시설을 대상으로 하는 사이버 공격에 대한 대응 체계를 구축할 것을 대통령 행정명령을 주문하여 국가적인 대응 방안을 제공하기 위해 노력하고 있는 현실이나, 솔라윈즈 사태 등으로 인해 사이버 공격은 현재 진행 중인 상태임을 알 수 있다.[3]

따라서, 본 연구를 통해 국제 표준인 IEC 62443 기반의 보안 레벨을 적용함으로서 산업제어시스템의 필수 보안요소를 적정하게 유지하여 제공하는 방안에 대하여 살펴보고자 한다.

본 논문의 구성은 1장 서론에 이어서, 2장의 관련연구 분석을 통해 IEC 62443 국제 표준에 대하여 살펴보고, 3장의 국제표준 기반의 산업제어시스템 필수보안 요구사항을 도출하여, 4장의 결론에서 적용방안을 제시하고자 한다.

## 2. 관련연구

2장에서는 산업제어시스템 제조시 준용해야하는 필수보안요구사항이 반영된 IEC 62443 시리즈를 분

석하고자 한다. IEC 62443 시리즈는 “산업용 통신 네트워크-네트워크 및 시스템을위한 IT 보안”에 대한 국제 표준 시리즈로서, 여러 운영자, 통합 자 (통합 및 유지 보수를위한 서비스 제공 업체) 및 제조업체의 여러 역할로 구분한 섹션으로 나누어 산업 사이버 보안의 기술 및 프로세서 관련 측면을 각기 다른 역할은 활동에서 보안 위험을 예방하고 관리하기 위해 위험 기반 접근 방식으로 설명하고 있다.[4] IEC 62443 시리즈의 구성은 다음의 그림 1과 같다.


(그림 1) IEC 62443 시리즈.

IEC 62443-2-1은 산업 자동화 및 제어 시스템 (IACS, Industry Automation and Control System)을 위한 사이버보안 관리 시스템 (CSMS, Cybersecurity Management System)을 구축하는 데 필요한 요소를 정의하고 그러한 요소를 개발하는 방법에 대한 지침을 IEC/TS 62443-1-1에 기술된 IACS를 구성하는 것에 대한 광범위한 정의와 범위를 사용하여 제공하고 있다.

IEC 62443-2-2는 산업제어시스템(IACS)의 보호등급을 명시하는 IEC 62443 시리즈의 부분으로 다양한 IACS 환경에서 보호등급을 부여하여 평가의 기반으로 프레임워크 및 구조를 명시하고 있다. IEC 62443-2-2에서 제안하는 프레임워크는 ISO/IEC 27001 같은 다른 표준을 참조할 뿐만 아니라 다른 IEC 62443 시리즈 문서에 명시된 기술적 및 조직적 요구사항을 기반으로 운영중인 IACS의 심층방어를 평가하는 구조를 제공하고, 평가 프로세스는 보호등급을 결정하는 절차뿐만 아니라 프레임워크와 구조를 기반으로 사용되어 진다.

IEC 62443-3-3은 시스템 통합사업자, 제품 공급자 및 서비스 공급자가 제품이나 서비스가 자산 소유자의 목표 보안 수준 요구사항에 맞게 기능적 보안 역량을 제공할 수 있는지 평가하는데 목표 보안 수준 배정에 따라, 개별 제어시스템 요구사항과 개선의 가용성은 특정 사이트 환경에서 자산 소유자의 보안 정책, 절차 및 위험 평가를 기반으로 사용할 수 있다.

IEC 62443-4-1은 산업제어시스템에 사용되는 제품의 안전한 개발을 위한 프로세스 요구사항을 명시하여 안전한 제품을 개발하고 유지하기 위한 안전한 개발 생명주기(SDL, Secure Development Lifecycle)를 정의하고 있으며, 여기에서는 안전한 개발 생명주기는 보안 요구사항 정의, 안전한 설계, 안전한 구현, 검증 및 확인, 결함 관리, 패치 관리 및 제품 폐기를 포함하고 있으며, 신규나 기존 제품의 하드웨어, 소프트웨어나 펌웨어의 개발, 유지 및 폐기를 위한 신규나 기존 프로세스에 적용될 수 있다. 제품의 개발자나 유지보수 담당자에게 적용되지만, 제품의 통합자나 사용자는 대상이 아니다.

IEC 62443-4-2에서는 산업제어시스템(IACS)을 운용하는 조직이 저렴하고 효율적이며 고도로 자동화된 상용 네트워크 서비스를 점점 더 많이 사용하고 있으며, 제어시스템 또한 정당한 업무 요청으로 비IACS 네트워크와 연결이 증가하고 있는 추세임을 고려하여, 개방 네트워킹 기술 및 증가되는 연결 등은 제어시스템 하드웨어 및 소프트웨어에 대한 사이버 공격 기회를 증가시키고 있어서 스마트공장 환경에서의 기술보호를 위해 주의를 갖고 적용하는 것을 중점적으로 다루고 있다.[5]

## 3. 스마트공장 환경에서의 IEC 62443 기반의 산업제어시스템 필수보안 요구사항 도출

앞서 살펴본 IEC 62443 시리즈의 중요 목표는 IACS(Idustrial Automation Control System)의 현재와 향후 취약성을 해결하고 체계적이고 방어 가능한 방식으로 필요 완화를 적용할 수 있는 유연한 프레임워크를 제공하는 것에 있으며, 이룰 위해 IEC 62443 시리즈의 목적이 업무 IT 시스템의 요구사항을 적용한 전사적 보안으로 확장하고, IACS에 필요한 강력한 무결성 및 가용성을 위한 특이 요구사항과 결합시키게 된다.

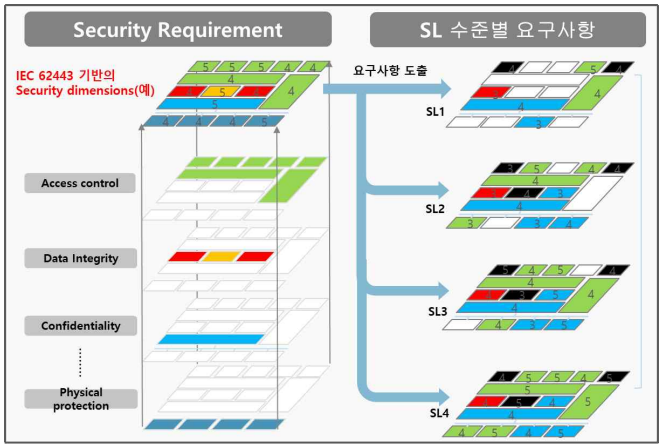
스마트공장 환경에서 기기 인증(Device Certification)을 수행하기 위해 인증(Authentication)과 인가(Authorization) 기능을 구현하여 제공하여야 하고, 이를 위해서는 스마트 공장 기기에 최적화 시킨 X.509 v3(PKI) 기술을 개발하여 적용하는 것과 같은 방법

으로 보안성을 확보하여야 한다.

스마트공장 환경에서 사용되는 데이터의 무결성 및 기밀성을 보호하기 위해서는 기기에 적용 가능한 Cryptogrphy 기술을 개발하여 사용되어야 하며, 이는 국제 표준 규격의 Cryptogrphy 기술을 개발하여 제공함으로써 스마트공장 기기의 Data Protection 기능을 제공하여야 하며, 스마트공장 기기의 열악한 성능상의 이슈를 해결하기 위해 LEA와 같은 국제 표준으로 지정된 경량 암호화 알고리즘의 적용을 고려할 필요가 있다.[6][7]

또한, 스마트공장 환경에서 사용되는 기기의 Acce ss Control 기술개발이 필요한데, 이는 Access Cont rol 제어가 쉽지 않은 스마트공장 기기에 적용이 가능한 SW 기술을 개발하는 것을 포함하여, 스마트공장에 기 설치되어 동작하고 있는 구형 PLC 등의 기기를 보호하기 위한 HW 장비로서 기존 장비에 보안성을 제공할 필요가 있다.

IEC 62443에서는 보안 수준(Security Level, SL)을 1부터 4등급으로 구분하고 있으며, 현재 IEC 624 43-4-1 및 4-2 인증을 획득한 기업은 전세계에서 5 0여개의 기업들이 존재하고 있다. 해당 기업들이 획득한 인증의 수준을 살펴보변, SL1 수준으로만 획득하고 있어서, 스마트공장 환경에서 IEC 62443 SL 수준의 적용은 SL1 수준을 우선적으로 적용하되, 상위 SL 수준에서 정의하고 있는 항목을 차용하여 정리할 필요성이 있다. 예를 든다면, 기기 인증을 위해 사용되는 X.509 v3 기술은 IEC 62443-4-2의 보안 요구사항에서는 SL 2 수준으로 정의되어 있지만, 이를 필수적으로 적용해야 한다면, 해당 요구사항을 포함시킨 내용으로 도출하여 적용해야 한다.

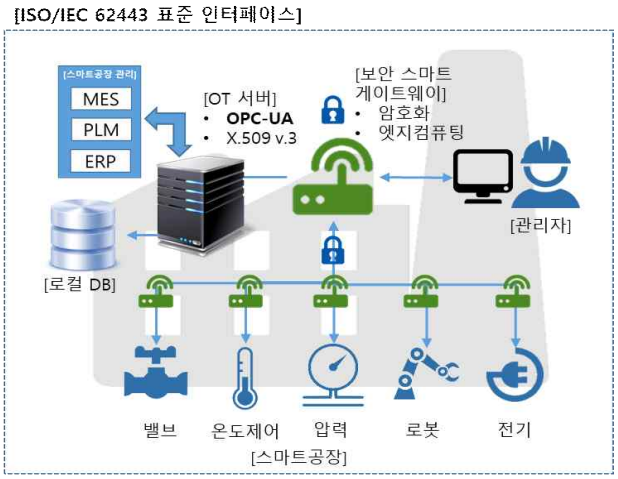



(그림 2) IEC 62443 기반의 보안 수준 적용 예시

## 4. 결론

IEC 62443 기반의 보안 요구사항을 통해 스마트공장 환경에 필수적으로 적용되는 보안 요구사항 도출에 대하여 살펴보았다.

스마트공장 환경에서의 보안은 현재 진행형인 상태이며, IT 영역과 OT 영역의 혼재되어 동작하게 됨에 따라 보안 요구사항을 기존의 방식, 즉 IT 기술에 따른 방식을 적용하기에는 문제가 있으며, 적합한 보안 요구사항을 도출하여 적용하는 것이 매우 중요한 이슈로서, 이를 통해 스마트공장 환경의 보안 내재화를 이룰 수 있다고 판단된다.




(그림 3) IEC 62443 기반의 스마트공장 보안 내재화 예시

앞서 3장에서 설명한 스마트공장의 필수적인 보안 요구사항을 반영하여 스마트공장 환경을 구성하게 되면, 국내 스마트공장 중 비중이 매우 큰 반도체 제조공정, 전력, 수력/원자력, 자동차 제조 공정, 창고, 조선소, 공장 현장, 농업, 의료 등 모든 제조업 분야에 제한 없이 적용 가능하여 스마트공장 환경의 보안 내재화를 확보 할 수 있다.

추가적으로, 본 논문에서 제시하고 있는 분석 모델의 타당성을 검증하기 위해, 실증 연구를 향후 추진하여 객관적인 연구 기준 및 성능 지표 등을 확인하여 객관적인 자료를 기반으로 증빙하고자 한다.

## Acknowledgement

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-01774, IEC 62443 기반의 스마트공장 보안 내재화 및 임베디드 기기 보안 기술 개발)

## 참고문헌

[1] https://www.dailysecu.com/news/articleView.html?idxno=110872

[2] https://journalofcyberpolicy.com/2019/12/17/news-insights-gangnam-industrial-style-apt-campaign-targets-korean-industrial-companies-cyberx/

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

[4] https://www.iec.ch/blog/understanding-iec-62443

[5] https://standard.go.kr/KSCI/standardIntro/getStandardSearchView.do?menuId=919&topMenuId=502&upperMenuId=503&ksNo=KSXIEC62443-4-2&tmprKsNo=KS_C_NEW_2019_3780&reformNo=00

[6] https://www.iso.org/standard/78477.html

[7] https://www.rra.go.kr/ko/reference/kcsList_view.do?nb_seq=1923&cpage=4&nb_type=6&searchCon=&searchTxt=&sortOrder=