KIPS Trans. Comp. and Comm. Sys.
Vol.11, No.6 pp.193~204
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2022.11.6.193

A Study on Application Methodology of SPDL Based on IEC 62443 Applicable to SME Environment

Jin Jung Ha† · SangSeon Park†† · Kim Jun Tae†† · Keunhee Han†††

ABSTRACT

In a smart factory environment in a small and medium-sized enterprise (SME) environment, sensors and actuators operating on actual manufacturing lines, programmable logic controllers (PLCs) to manage them, human-machine interface (HMI) to control and manage such PLCs, and consists of operational technology server to manage PLCs and HMI again. PLC and HMI, which are in charge of control automation, perform direct connection with OT servers, application systems for factory operation, robots for on-site automation, and production facilities, so the development of security technology in a smart factory environment is demanded. However, smart factories in the SME environment are often composed of systems that used to operate in closed environments in the past, so there exist a vulnerable part to security in the current environment where they operate in conjunction with the outside through the Internet. In order to achieve the internalization of smart factory security in this SME environment, it is necessary to establish a process according to the IEC 62443-4-1 Secure Product Development Life cycle at the stage of smart factory SW and HW development. In addition, it is necessary to introduce a suitable development methodology that considers IEC 62443-4-2 Component security requirements and IEC 62443-3 System security requirements. Therefore, this paper proposes an application plan for the IEC 62443 based development security process to provide security internalization to smart factories in an SME environment.

Keywords : Small and Medium-sized Enterprise(SME) environment, Cyber Security, Industrial Control System(ICS), IEC 62443, Secure Product Development Lifecycle(SPDL)

중소기업환경에서 적용 가능한 IEC 62443 기반의 개발 보안 생애주기 프로세스 적용 방안 연구

진 정 하† · 박 상 선†† · 김 준 태†† · 한 근 희†††

요 약

SME(small and medium-sized enterprise) 환경의 스마트제조 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 스마트제조 환경에서 보안 기술의 개발이 중점적으로 필요한 영역이다. 하지만, SME 환경의 스마트제조에서는 과거의 폐쇄 환경에서 동작하던 시스템으로 구성되어 있는 경우가 상당하여 인터넷을 통해 외부와 연동되어 동작하게 되는 현재의 환경에서는 보안에 취약한 부분이 존재한다. 이러한 SME 환경의 스마트제조 보안 내재화를 이루기 위해서는, 스마트제조 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. 따라서, 본 논문에서는 SME 환경에서의 스마트제조에 보안 내재화를 제공하기 위한 IEC 62443 기반의 개발 보안 생애주기 프로세스에 대한 적용 방안을 제안한다.

키워드 : 중소기업환경, 사이버보안, 산업제어시스템, IEC 62443, 개발보안생애주기

1. 서 론

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·엔지

※ 이 논문은 2022년도 과학기술정보통신부의 재원으로 IITP의 지원을 받아 수행된 연구임 (No.2021-0-01774, IEC 62443 기반의 스마트공장 보안 내재화 및 임베디드 기기 보안 기술 개발).
※ 이 논문은 2021년 한국정보처리학회 ACK 2021에서 "IEC 62443 표준 적용을 통한 산업제어시스템 보안성 강화 연구"의 제목으로 발표된 논문을 확장한 것임.
† 정 회 원 : 고려대학교 정보보호연구원 연구교수
†† 비 회 원 : 고려대학교 정보보호연구원 수석연구원
††† 종신회원 : 고려대학교 정보보호연구원 연구교수
Manuscript Received : December 31, 2021
Accepted : February 19, 2022
* Corresponding Author : Keunhee Han(khhan1@korea.ac.kr)

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/ licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

니어링·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 대상기업 가운데 약 60%가 한국 내 기업으로 조사되어 한국도 ICS·OT 보안에서 예외가 아님이 밝혀지고 있어서, 산업제어시스템에 대한 사이버공격이 증가하는 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].

이러한 상황에서 스마트제조 환경에서 IEC 62443-4-1의 SPDL(Secure Product Developement Lifecycle)을 적용하는 경우 보안성 내재화를 확보할 수 있다.[4] 하지만, 이러한 보안 개발 생애주기는 중소기업 환경에서의 적용은 어려운 현실이다. 실제 개발 환경에서는 단지 인증만을 위한 접근 방식으로 접근하여 개발을 완료한 이후에 서류상으로 역산하여 작성하고 있어서, 실제 개발 생애주기의 적용을 통한 심층 보안 기능을 확보하는 것은 어려운 현실이다.

따라서, 본 논문에서는 국제 표준인 IEC 62443 기반의 개발 생애주기 프로세스를 중소기업 환경에서 적용하여 스마트제조 환경에서 보안 레벨을 적용하는 방식을 제안함으로써 산업제어시스템의 필수 보안 요소를 적정하게 유지하여 제공하는 방안에 대하여 중점적으로 다루고자 한다. 특히, 전체 개발 생애주기 중에서 위협 식별 및 위험 분석을 어떤 형태로 수행해야 하는지에 대하여 살펴서 개발 요구사항 도출에 대하여 중점적으로 정리하고자 한다.

본 논문의 구성은 1장 서론에 이어서, 2장의 관련 연구 분석을 통해 IEC 62443 국제 표준에 대하여 살펴보고, 3장의 국제표준 기반의 중소기업환경에서 적용 가능한 개발 보안 생애주기 프로세스 수립을 위한 산업제어시스템 필수보안 요구사항을 만족하는 위험 식별 방안을 도출하여, 4장의 결론에서 적용 방안을 제시하고자 한다.

2. 관련 연구

2장에서는 산업제어시스템 제조시 준용해야하는 필수보안 요구사항이 반영된 IEC 62443 시리즈를 분석하고자 한다. IEC 62443 시리즈는 "산업용 통신 네트워크 및 시스템을 위한 IT 보안"에 대한 국제 표준 시리즈로서, 여러 운영자, 통합 자 (통합 및 유지 보수를 위한 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.[5]

IEC 62443 시리즈는 ISO(International Organization for Standardization)에서 등록 및 관리하고 있으며, 미국의 ISA(International Society of Automation)에서는 동일한 표준번호를 사용하는 ISA 표준에 대하여 IEC 번호와 동일하게 사용하고 있으나 표준명을 별도로 부과하여 등록 및 관리하고 있다. IEC 62443 시리즈의 연관 구성은 다음의 Fig. 1과 같다.

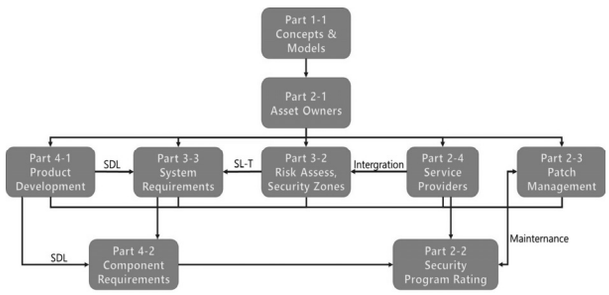

Fig. 1. Structure of the IEC 62443 Series

2.1 IEC 62443 Part 1

IEC 62443 Part 1은 IEC 62443의 기본으로 일반적인 사항을 다루고 있으며, 해당 표준에 대한 일반적 개요 및 용어 등을 포함하는 전반적인 표준의 구성 등에 대하여 포괄적인 설명을 포함하고 있다. IEC 62443의 Part 1은 4개의 세부 항목으로 구성되어 있다.

1) IEC 62443-1-1[6]

Part 1-1은 IEC 62443 시리즈 표준의 전체에 걸쳐서 사용되는 전문용어와 각 개념 및 모델들에 대한 소개를 포함하고 있다. 일반적인 사이버보안 요소들중, 산업 자동화 및 제어시스템(IACS: Industrial Automation and Control Systems)에 적용 가능한 부분과 오직 산업 자동화 및 제어시스템(IACS)에서만 적용 가능한 개념과 모델에 대한 정의를 포함하고 있으며, 7개 기반 요구사항 (FR, Foundational requirements)을 기반으로 정의되어 있고, 이는 식별 및 인증(FR1), 사용제어(FR2), 시스템 무결성(FR3), 데이터 기밀성 (FR4), 데이터 제한성(FR5), 응답성(FR6), 자원가용성(FR7)으로 구성된다. 산업 자동화 및 통제시스템에서의 보안 수준은 상기 7가지의 기반 요구사항에 따라 결정하게 된다.

2) IEC 62443-1-2

Part 1-2는 IEC 62443의 표준에서 사용하는 주요 용어와 약어에 대한 전반적인 설명과 정의로 구성되어 있다. IEC 62443-1-2에서는 139개 용어와 26개 약어가 설명되어 있으며, ISA 99에서 개정하고 있는 문서에는 117개 용어 14개 약어가 설명되고 있어서 IEC 62443 & ISA 62443 Series 문서 전체를 통해서는 약 400여개 용어와 280여개의 약어를 설명하고 있다.

3) IEC 62443-1-3

Part 1-3에서는 산업 자동화 및 제어시스템(IACS)에 대하

여 우선순위가 높은 시스템에 대한 사이버보안 적합성 측정 기준을 정의하고 있으며, 적합성 측정 항목은 IEC 62443 시리즈의 다른 부분에 명시된 산업 자동화 및 제어시스템(IACS) 요구사항을 준수하는지에 대한 측정 진행, 안전한 산업 자동화 및 제어시스템(IACS) 제품 및 서비스 개발 관리, 시스템의 배치 수명 전반에 걸쳐 사용자 지정한 서비스 품질을 모니터링하고 관리 진행, 시스템, 하위 시스템 및 구성요소가 서비스에서 제거될 때 보안 처분 확인, 법규 준수 기관에서 사용할 시스템 측정 제공과 같다.

4) IEC 62443-1-4

Part 1-4에서는 산업자동화 및 제어시스템(IACS)에 대한 보안적 측면의 생애주기(Lifecycle)을 정의하고 이에 대한 실증사례를 설명하고 있다. 하지만, IEC 62443 표준 시리즈의 일부로 제안되었으나, 현재까지 전반적인 표준에 대한 개발이 진행되지 않고 있다.

2.2 IEC 62443 Part 2

IEC 62443 Part 2는 정책과 절차(Policy & Procedure)를 다루고 있어서, 산업자동화 및 제어시스템(IACS)을 보유하는 조직에 대한 전반적인 보안정책과 기업보안을 위한 전반적인 절차에 대해 규정하고 있다.

1) IEC 62443-2-1[7]

Part 2-1은 산업자동화 및 제어시스템(IACS)의 자산소유자를 위한 보안요구사항을 다루고 있어서, 산업자동화 및 제어시스템(IACS)을 위한 사이버보안 관리 시스템(CSMS: Cyber Security Management System)을 구축하는 데 필요한 핵심 보안요소를 정의하고, 이 보안요소를 통하여 개발하는 방법에 대한 전반적인 지침을 제공하고 있다. 여기서는, 산업자동화 및 제어시스템(IACS)와 일반 비즈니스 및 정보 기술 시스템 간 중요한 차이점에 대하여 정의하고 있어서, ISO/IEC 27001 및 27002에서 정의하고 있는 보안표준과 산업자동화 및 제어시스템(IACS) 사이버보안 관리에 대한 일관성을 유지하기 위하여 작성이 필요하다. 산업자동화 및 제어시스템(IACS)의 사이버보안 위험이 HSE(Health, Safety and Environmental)에 영향을 미칠 수 있는 개념을 소개 및 포함하고 있다.

2) IEC 62443-2-2

Part 2-2는 산업자동화 및 제어시스템(IACS) 보안관리시스템을 위한 적용 가이드로서 산업자동화 및 제어시스템(IACS) 보안관리시스템의 구현 지침을 포함하고 있다. 설계 및 구현 후 보안관리시스템 운영 방안 기술에 대한 설명을 포함하고 있으나, 현재 개발 작업 진행중에 있어서 완료 시점은 미정인 상태이다.

3) IEC 62443-2-3[8]

Part 2-3은 산업자동화 및 제어시스템(IACS) 환경에 대한 패치 관리에 대하여 다루고 있다. IT 기반과 다른 산업자동화 및 제어시스템(IACS)의 보안 환경에서 패치 관리를 위한 특수한 요구사항을 포함하여 산업자동화 및 제어시스템(IACS) 구축 완료 후, 패치 관리의 단계상에서 자산소유자와 산업자동화 및 제어시스템(IACS)의 제품공급자에 대한 요구사항에 관하여 기술하고 있고, 각 자산소유자 또는 제품공급자 간 보안패치에 관련된 정보 교환 시 활용 가능한 데이터 형식을 제공하고 있다.

4) IEC 62443-2-4

Part 2-4는 산업자동화 및 제어시스템(IACS) 공급자를 위한 설치 및 유지보수 요구사항을 다루고 있으며, 산업자동화 및 제어시스템(IACS) 공급 업체의 설치 및 유지관리 요구사항에 대하여 중점적으로 다루고 있다.

5) IEC 62443-2-5

Part 2-5는 산업자동화 및 제어시스템(IACS)의 자산 소유자에 대한 구현 가이드로서, 현재 개발 작업 진행 중에 있으며, 완료 시점은 미정인 상태이다.

2.3 IEC 62443 Part 3

IEC 62443 Part 3에서는 시스템에 대해서 중점적으로 다루고 있으며, 시스템 통합을 위한 산업제어시스템에 대한 보안기능 요구사항을 규정하고 있다. 제어시스템 역량 보안등급 및 SL-C(제어시스템)의 요구사항 정의를 포함하여, IEC TS 62443-1-1에 서술된 7가지 기본 요구사항(FR)과 관련된 상세한 기술적 제어시스템 컴포넌트 요구사항(SR)을 제공하고 있으며, 이러한 요건은 산업 자동화 및 제어시스템(IACS) 커뮤니티의 다양한 구성원들이 특정 자산에 대한 적절한 제어시스템 목표 SL-T(제어시스템)를 개발하면서 고려중인 시스템(SuC)에 대해 정의된 구역 및 도관과 함께 사용되어진다. 산업제어시스템의 위험을 줄이는 데 필요한 강도를 가진 IEC 62443-1-1에서 정의된 기본적인 요구사항(FR1~FR7)을 선택하여 설계 및 구현에 사용되고 있으며, IEC 62443-1-1에서 정의된 7가지 요구사항은 제어시스템 성능 SL, SL-C(제어시스템)의 기초로 사용된다.

1) IEC 62443-3-1[9]

Part 3-1은 산업자동화 및 제어시스템(IACS)의 보안 기술을 중점적으로 다루고 있으며, 산업자동화 및 제어시스템(IACS)에 효과적으로 적용할 수 있는 다양한 사이버보안 도구, 완화 대응책, 기술에 대한 현재 평가(assessment)를 제공하고 있다. 제어시스템 중심의 사이버보안 기술의 여러 범주와 해당 범주에서 사용할 수 있는 제품 유형, 자동화된 산업자동화 및 제어시스템(IACS) 환경에서 이러한 제품을 사용하는 데 따른 위협 및 취약점에 관련된 장·단점, 사이버보안 기술 제품 및 대책을 사용하기 위한 예비 권장사항 및 지침 등을 포함하고 있으며, 다 수의 항목 및 구성은 서로 동일하며 내용 또한 유사하나, 일부의 항목 및 내용은 서로 상이함을 포함하고 있다. 다음의 Table 1에서는 62443-3-1 표준에 대하여 IEC와 ISA에서의 차이점을 설명하고 있다.

Table 1. IEC 62443-3-1 and ISA 62443-3-1 Comparison

No.	IEC/TR 62443-3-1: 2009	ISA-TR 62443-3-1: Revision 2 Draft
1	Scope	Scope
2	Normative references	Purpose
3	Terms, definitions and acronyms	General Terms and Definitions
4	Overview	Overview
5	Authentication ans authorization technologies	Authentication ans Authorization Technologies
6	Filtering/blocking/access control technologies	Network Protection Technologies
7	Encryption technologies and data validation	Encryption Technologies and Data Validation
8	Management, audit, measurement, monitoring and detection tools	Management, audit, measurement, monitoring and detection tools
9	Industrial automation and control systems computer software	Remote Access Technologies
10	Physical security controls	Cybersecurity Program Context

2) IEC 62443-3-2[10]

Part 3-2는 영역과 통신 구간의 보안 수준에 대한 정의를 포함하고 있어서, 산업자동화 및 제어시스템(IACS)에 대한 시스템 구성(SuC: System under Consideration)을 정의하고, SuC를 구역으로 나누어 위험을 평가하고, 보안수준목표(SL-T)를 수립하여, 보안 요구사항을 문서화하기 위한 요구사항을 정의하고 있다. 위험도 평가에서 요구되는 보안대책과 회사 또는 시설별 정책, 표준 및 관련 규정에 근거한 보안 요구사항을 사이버보안 요구사항 명세서로 문서화하도록 요구하고 있으며, 여기에는 고려 대상 시스템 설명, 구역 및 연결 구성도, 위협 환경 및 위험 평가의 대책과 같은 정보가 포함되게 된다. 위험 평가 프로세스의 핵심 단계는 검토 중인 시스템을 별도의 구역과 전송로로 분할하는 것으로서 목적은 사이버보안 위험을 줄이는 일련의 공통 보안 요구사항을 확립하기 위해 공통의 보안 특성을 공유하는 자산을 식별하는 것이다.

3) IEC 62443-3-3[11]

Part 3-3은 시스템에 대한 보안 요구사항과 보안 수준에 대해서 다루고 있으며, IEC 62443-2-1에서 제시하고 있는 보안 프로그램이 수립되어 있다는 전제하에 62443-2-1에서 요구하는 위험 평가 핵심 단계에서 실제로 필요한 서비스 및 기능을 식별하는 데 있으며, 고려 대상 시스템, 구역 또는 통신 시스템에 의도된 방식으로 취약성과 기능이 없다는 신뢰도의 척도로 정의하고 있는 보안 수준(SecurityLevel, SL)은 다음과 같이 4단계로 구분하고 있다.

a) SL 1: 도청 또는 일반 노출을 통한 정보의 인가받지 않은 공개를 방지.
b) SL 2: 낮은 자원, 일반 기술 및 낮은 동기의 단순한 수단을 사용하여 능동적으로 검색하는 개체에게 정보의 인가 받지 않은 공개를 방지.
c) SL 3: 적당한 자원, 산업자동화 및 제어시스템(IACS) 특정 기술 및 적당한 동기의 뛰어난 수단을 사용하여 능동적으로 검색하는 개체에게 정보의 인가 받지 않은 공개를 방지.
d) SL 4: 광범위한 자원, 산업자동화 및 제어시스템(IACS) 특정 기술 및 높은 동기의 뛰어난 수단을 사용하여 능동적으로 검색하는 개체에게 정보의 인가 받지 않은 공개를 방지

다음의 Table 2에서는 62443-3-3에서 ICS 설계 원리에 대하여 설명하고 있다.

4) IEC 62443-3-4

Part 3-4는 제품 개발에서의 요구사항을 다루고 있으며, 현재 개발 예정 중인 상태이다.

2.4 IEC 62443 Part 4

IEC 62443 Part 4에서는 산업제어시스템을 구성하는 제어기기, 장비, 애플리케이션의 보안을 취급하는 장비 업체를 위한 보증 요구사항과 기능 요구사항에 관해 규정하고 있다.

1) IEC 62443-4-1[4]

Part 4-1은 제품 개발 요구사항을 다루고 있어서, 보안 개발 생애주기(SDL: Secure Development Lifecycle)를 정의하며 그에 따른 요구사항을 기술하고 있다. 제품공급자는 본

Table 2. IEC 62443-3-3 ICS Design Principle

SL	Definition	method	resource	technique	motivation
1	Protection against accidental or accidental violations	simple	Low	General	Low
2	Protect against intentional violations using low resources, general skills and simple means of low motivation				
3	Use sophisticated means to avoid intentional violations through intermediate-level resources, IACS-related skills, and intermediate-level motivation	Sophisticated	Middle	each IACS	Moderate
4	Prevent intentional violations using sophisticated means with top-level resources, IACS-related skills, and top-level motivation	Sophisticated	Expansion	Sophisticated	High

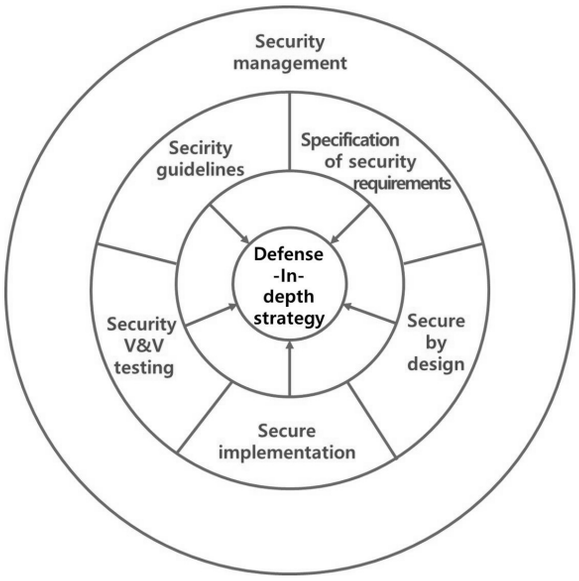

Fig. 2. Deep Security Strategy of Secure Product Development Life Cycle[4]

표준을 준수하는 프로세스를 통해 제품을 개발하고, 제품은 단일 부품이 될 수도 있고, 여러 부품으로 이루어진 시스템이 될 수도 있으며, 보안관리를 위하여 다양한 요구사항들과 프로세스들이 존재하여 이는 보안제품개발의 생애주기에 있어서 심층 보안 및 방어전략으로 활용되게 된다. 다음의 Fig. 2는 62443-4-1에서 다루는 시큐어 바이 디자인(secure by design) 원칙이 제품의 심층 방어 전략에 어떻게 영향을 끼치는지를 나타내고 있다. 보안관리 실행은 그 실행이 준수되고 관리되도록 모든 실행 전반에 걸쳐 적용되기 때문에 가장 바깥쪽 원에 위치되어진다. 두 번째 원에 보이는 다른 실행은 종종 반복적 패턴으로 개발 생애주기 전반에 걸쳐 적용된다. 이런 실행 각각은 보안 개발 생애주기를 따른 주요 결과를 나타내기 때문에 원 중심에 나타내고 있는 전체 심층 방어 전략에 영향을 발생시킨다. 결함 관리와 보안 업데이트 관리는 보안 구현에 검증된 보수를 제공하며, Fig. 2의 전체 보안관리 분류 아래에 위치된다.

다음의 Table 3에서 나타내고 있는 것은 개발 성숙도 모델(CMMI: Capability Maturity Model Integration)과 62443-4-1을 비교하여 설명하고 있다.

2) IEC 62443-4-2[12]

Part 4-2는 산업자동화 및 제어시스템(IACS) 구성요소, 다시 말해 컴포넌트의 기술적 보안 요구 사항을 중점적으로 다루고 있다. 특히, 4-2는 앞선 62443-3-3과 연계되어 사용되며, IEC 62443-1-1에 기술된 7개 기초 요구사항 (FR)과 관련된 상세한 기술 제어시스템 구성요소에 대한 요구사항(CR)을 제공하고 있다. 다음의 Table 4에서는 IEC 62443-4-2에서의 보안 요구사항과 보안 수준에 대하여 정의한 내용을 설명하고 있다.

3) IEC 62443-4-3

Part 4-3은 네트워크 디바이스에 대한 내용으로서 현재 개발 진행 중에 있다.

Table 3. CMMI-Development Model Comparison

Lv.	CMMI -DEV	IEC 62443-4-1	IEC 62443-4-1 Description
1	Initial	Initial	Product providers generally perform product development in an undocumented (not fully documented) arbitrary manner. As a result, continuity between projects and repetition of processes may not be possible.
2	Managed	Managed	At this level, product providers have the ability to manage product development in accordance with documented policies (including objectives). The product provider also has evidence showing that the staff to perform the process are trained with expertise and follow documented procedures to perform. However, at this level, organizations do not have the experience of developing products with all documented policies. This is a case where the organization updates the procedure in compliance with this document, but not yet applies all procedures to actual execution. The development principle reflecting maturity level 2 helps to check whether it is repetitive even when it is difficult to implement development. If this implementation is properly prepared, the implementation will be carried out and managed according to a documented plan. NOTE: At this level, the CMMI and IEC 62443-4-1 maturity models are essentially the same except that IEC 62443-4-1 recognizes a significant delay between process definition/regulation and execution. Therefore, the execution-related aspect of CMMI-DEV level 2 is postponed to level 3.
3	Defined	Defined (Skilled)	The performance of level 3 product developers can be repeatedly seen throughout the supplier organization. The process is executed and evidence exists to show the occurrence of this process. NOTE: At this level, the CMMI and IEC 62443-4-1 maturity models are essentially the same except that the execution-related aspects of CMMI-DEV level 2 are included in this level. Therefore, the process of level 3 is a level 2 process in which the supplier executes at least one product.
4	Quantitatively Managed	Improvement	At this level, IEC 62443-4-1 combines CMMI-DEV levels 4 and 5. Using suitable process metrics, the product provider controls the product's efficiency and performance and shows continuous improvement in these areas.
5	Optimizing		

Table 4. IEC 62443-4-2 Define Security Requirements and Security Levels

62443-4-2				
SR(Security Requirements) and RE(Requirement Enhancement)	SL1	SL2	SL3	SL4
	48	93	116	122
FR 1 - Identification and Authentication Control (IAC)				
CR 1.1 - Human user identification and authentication	o	o	o	o
RE (1) Unique identification and authentication		o	o	o
RE (2) Multifactor authentication for all interfaces			o	o
CR 1.2 - Software process and device identification and authentication		o	o	o
RE (1) Unique identification and authentication			o	o
CR 1.3 - Account management	o	o	o	o
CR 1.4 - Identifier management	o	o	o	o
CR 1.5 - Authenticator management	o	o	o	o
RE (1) Hardware security for authenticators			o	o
NDR 1.6 - Wireless access management	o	o	o	o
RE (1) Unique identification and authentication		o	o	o
CR 1.7 - Strength of password-based authentication	o	o	o	o
RE (1) Password generation and lifetime restrictions for human users			o	o
RE (2) Password lifetime restrictions for all users (human, software process, or device)				o
CR 1.8 -Public key infrastructure certificates		o	o	o
CR 1.9 - Strength of public key-based authentication		o	o	o
RE (1) Hardware security for public key-based authentication			o	o
CR 1.10 - Authenticator feedback	o	o	o	o
CR 1.11 - Unsuccessful login attempts	o	o	o	o
CR 1.12 - System use notification	o	o	o	o
NDR 1.13 - Access via untrusted networks	o	o	o	o
RE (1) Explicit access request approval			o	o
CR 1.14 - Strength of symmetric key-based authentication		o	o	o
RE (1) Hardware security for symmetric key-based authentication			o	o
FR 2 - Use control(UC)				
CR 2.1 - Authorization enforcement	o	o	o	o
RE (1) Authorization enforcement for all users		o	o	o
RE (2) Permission mapping to roles		o	o	o
RE (3) Supervisor override			o	o
RE (4) Dual approval				o
CR 2.2 - Wireless use control	o	o	o	o
CR 2.3 - Use control for portable and mobile devices				
SAR 2.4 - Mobile code	o	o	o	o
RE (1) Mobile code authenticity check		o	o	o
EDR 2.4 - Mobile code	o	o	o	o
RE (1) Mobile code authenticity check		o	o	o
HDR 2.4 - Mobile code	o	o	o	o
RE (1) Mobile code authenticity check		o	o	o
NDR 2.4 - Mobile code	o	o	o	o
RE (1) Mobile code authenticity check		o	o	o
CR 2.5 - Session lock	o	o	o	o
CR 2.6 - Remote session termination		o	o	o
CR 2.7 - Concurrent session control			o	o
CR 2.8 - Auditable events	o	o	o	o
CR 2.9 - Audit storage capacity		o	o	o
RE (1) Warn when audit record storage capacity threshold reached			o	o
CR 2.10 - Response to audit processing failures	o	o	o	o
CR 2.11 - Timestamps		o	o	o
RE (1) - Time synchronization		o	o	o
RE (2) - Protection of time source integrity				o
CR 2.12 - Non-repudiation	o	o	o	o
RE (1) - Non-repudiation for all users				o
EDR 2.13 - Use of physical diagnostic and test interfaces		o	o	o
RE (1) Active monitoring			o	o
HDR 2.13 - Use of physical diagnostic and test interfaces		o	o	o
RE (1) Active monitoring			o	o
NDR 2.13 - Use of physical diagnostic and test interfaces		o	o	o
RE (1) Active monitoring			o	o
FR 3 - System integrity(SI)				
CR 3.1 - Communication integrity	o	o	o	o
RE (1) Communication authentication		o	o	o
SAR 3.2 - Protection from malicious code	o	o	o	o

Table 4. (Continued)

62443-4-2				
EDR 3.2 - Protection from malicious code	o	o	o	o
HDR 3.2 - Protection from malicious code	o	o	o	o
RE (1) Report version of code protection		o	o	o
NDR 3.2 - Protection from malicious code	o	o	o	o
CR 3.3 - Security functionality verification	o	o	o	o
RE (1) Security functionality verification during normal operation				o
CR 3.4 - Software and information integrity	o	o	o	o
RE (1) Authenticity of software and information		o	o	o
RE (2) Automated notification of integrity violations			o	o
CR 3.5 - Input validation	o	o	o	o
CR 3.6 - Deterministic output	o	o	o	o
CR 3.7 - Error handling	o	o	o	o
CR 3.8 - Session integrity		o	o	o
CR 3.9 - Protection of audit information		o	o	o
RE (1) Audit records on write-once media				o
EDR 3.10 - Support for updates	o	o	o	o
RE (1) Update authenticity and integrity		o	o	o
HDR 3.10 - Support for updates	o	o	o	o
RE (1) Update authenticity and integrity		o	o	o
NDR 3.10 - Support for updates	o	o	o	o
RE (1) Update authenticity and integrity		o	o	o
EDR 3.11 - Physical tamper resistance and detection		o	o	o
RE (1) - Notification of a tampering attempt			o	o
HDR 3.11 - Physical tamper resistance and detection		o	o	o
RE (1) - Notification of a tampering attempt			o	o
NDR 3.11 -Physical tamper resistance and detection		o	o	o
RE (1) - Notification of a tampering attempt		o	o	o
EDR 3.12 - Provisioning product supplier roots of trust(RoT)			o	o
HDR 3.12 - Provisioning product supplier roots of trust(RoT)		o	o	o
NDR 3.12 - Provisioning product supplier roots of trust(RoT)		o	o	o
EDR 3.13 - Provisioning asset owner roots of trust(RoT)		o	o	o
HDR 3.13 - Provisioning asset owner roots of trust(RoT)		o	o	o
NDR 3.13 - Provisioning asset owner roots of trust(RoT)		o	o	o
EDR 3.14 - Integrity of the boot process	o	o	o	o
RE (1) Authenticity of the boot process		o	o	o
HDR 3.14 - Integrity of the boot process	o	o	o	o
RE (1) Authenticity of the boot process		o	o	o
NDR 3.14 - Integrity of the boot process	o	o	o	o
RE (1) Authenticity of the boot process		o	o	o
FR 4 - Data confidentiality(DC)				
CR 4.1 - Information confidentiality	o	o	o	o
CR 4.2 - Information persistence		o	o	o
RE (1) Erase of shared memory resources			o	o
RE (2) Erase verification			o	o
CR 4.3 - Use of cryptography	o	o	o	o
FR 5 - Restricted data flow (RDF)				
CR 5.1 - Network segmentation	o	o	o	o
NDR 5.2 - Zone boundary protection	o	o	o	o
RE (1) Deny all, permit by exception		o	o	o
RE (2) Island mode			o	o
RE (3) Fail close			o	o
NDR 5.3 - General-purpose person-to-person communication restrictions	o	o	o	o
FR 6 - Timely response to events (TRE)+				
CR 6.1 - Audit log accessibility	o	o	o	o
RE (1) Programmatic access to audit logs			o	o
CR 6.2 - Continuous monitoring		o	o	o
FR 7 - Resource availability (RA)				
CR 7.1 - Denial of service protection	o	o	o	o
RE (1) Manage communication load from component		o	o	o
CR 7.2 - Resource management	o	o	o	o
CR 7.3 - Control system backup	o	o	o	o
RE (1) Backup integrity verification		o	o	o
CR 7.4 - Control system recovery and reconstitution	o	o	o	o
CR 7.5 - Emergency power				
CR 7.6 - Network and security configuration settings	o	o	o	o
RE (1) Machine-readable reporting of current security settings			o	o
CR 7.7 - Least functionality	o	o	o	o
CR 7.8 - Control system component inventory		o	o	o

4) IEC 62443-4-4

Part 4-4는 애플리케이션과 데이터 및 기능에 대한 내용으로 개발 예정 중에 있다.

3. IEC 62443 기반 개발 보안 생애주기 프로세스

앞선 2장에서 살펴본 IEC 62443 국제 표준 시리즈 중에서 IEC 62443-4-1 기반에서 언급하고 있는 생애주기를 적용하여 개발 프로세스 수립을 통해 심층 방어 체계의 구축이 가능해진다[4]. 실제로 IEC 62443-4-1에서는 IEC 24748 기반으로 개발 생애주기를 언급하고 있으며, 이는 기존의 ISO 15288의 시스템 개발 생애주기 및 ISO 12207의 SW 개발 생애주기를 포함하고 있으며, 추가적으로 ICS(Industrial Control System) 환경에서의 보안 개발을 위한 프로세스를 정의하고 있다[13-15].

3.1 개발 보안 생애주기 프로세스

다음의 Fig. 3을 살펴보면 개시 단계부터 운영 단계까지의 개발 프로세스에 대하여 각 단계에서 수행되어야 하는 프로세스를 정의하고 있다. 62443-4-1에서 제시하는 SPDL에서는 개시 단계 이후에 분석 단계로 넘어가게 되는 경우 위협 분석을 수행하여야 하고, 만일 위협 분석이 제대로 수행되지 않는 경우 다시 개시 단계로 회귀하여 요구사항 식별을 통해 위협 분석을 재 수행하게 되는 순환구조로 구성되게 된다. 위협 분석이 정상적으로 수행되게 되면 설계 단계로 넘어가게 되는데 이 단계에서는 시큐어 바이 디자인(secure by design)에 따른 보안 설계를 수행하게 되고, 설계가 완료되면 구현 단계로 넘어가서 실제 구현에 들어가게 된다. 이처럼 세부 단계에서의 프로세스가 유기적으로 연동되어 순환구조로 구성되어 개발 생애주기를 형성하게 되고, 개선 및 유지보수와 폐기 단계까지를 적용하여 심층 방어 구조를 확보할 수 있게 되는 것이다.

3.2 중소기업에 적용 가능한 개발 생애주기 모델

상기와 같이 IEC 62443-4-1 기반의 SPDL 프로세스를 확립하고, 그 다음에 IEC 62443-4-2 컴포넌트에 대한 보안 요구사항과 IEC 62443-3-3의 시스템에 대한 보안 요구사항에서 정의하고 있는 보안 수준(SL)의 적용을 통하여 ICS 환경에서 사용되는 HW 및 SW 개발에서 보안성 확보가 가능해진다[11,12]. 실제 중소기업 환경에서 적용이 가능하도록 IEC 62443-4-1 SPDL 기반으로 정리한 개발 보안 생애주기 프로세스와 프로세스 진행에서의 산출 내용을 정리하면 Fig. 4와 같이 도출되어 진다. 개발을 위한 프로세스를 62443-4-1 SPDL 프로세스에 따라서 수립하고, 제품에 대한 보안 요구사항을 제시하고 있는 62443-4-2 및 62443-3-3에 맞추어 보안 수준을 정의하여 사용함으로써 중소기업환경에서의 개발 보안 프로세스 수립이 가능해진다. Fig. 4의 상단 부분이 62443 표준 기반의 개발 프로세스를 수립하는 내용이고, 하단 부분은 실제 중소기업 환경에서 각 프로세스에서의 해당되는 활동을 명시하고 있다.

3.3 개발 생애주기 모델에서의 적용 양식

상기와 같은 보안 개발 생애주기에서 IEC 62443-4-1 프로세스를 원활하게 적용하기 위해서는 우선으로 위협 분석 및 위험 평가를 수행되어야 하며, 이를 위해서 개발물에 대한 위협 사항을 식별하고 이를 기반으로 위험을 평가하여 관리를 수행되어야 한다[17]. 위험을 평가하여 관리하기 위해서는 기획 단계에서 개발 요약서 및 개발 기준서 등의 문서를 작성하여 적용해야 한다. 이러한 문서 작성을 통해 개발 생애주기에서의 프로세스를 적용하게 되는 것이고, 식별된 위협에 대한 위험을 분석하고 평가하기 위해서는 TARA(Threat Analysis and Risk Assessment)를 통해 대응 방안을 수립하여야 한다.

1) 개발 요약서

개발 요약서는 기획 단계에서 제품의 개발에 대하여 기본적으로 준비되어야 하는 문서로 개발 준비와 실제적 개발을 위하여 내부적 보고 및 관련 부서들과의 협력을 위한 다양한 사항에 관한 내용을 포함하고 있다. 개발 요약서에 포함되는 내용에는 다음과 같은 내용이 해당된다.

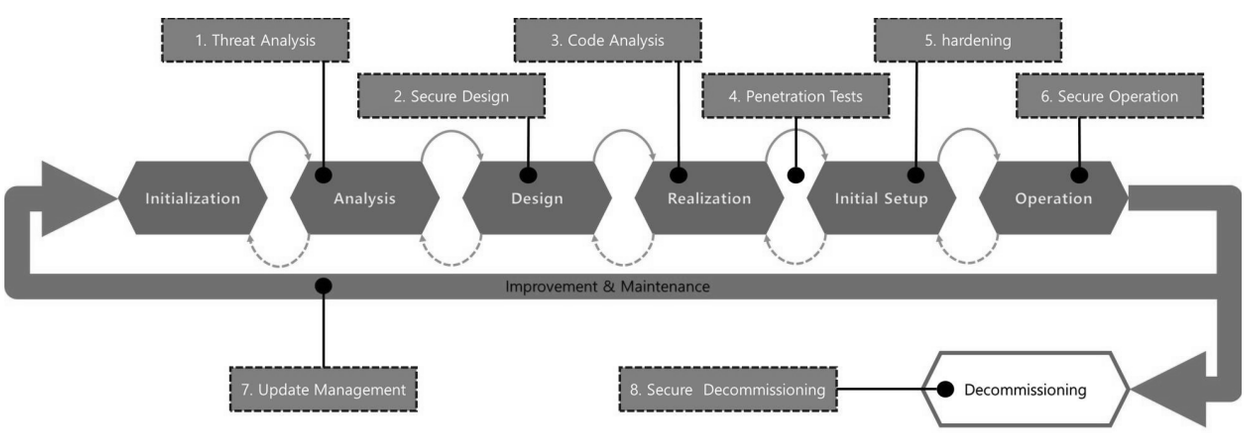

Fig. 3. Secure Development Lifecycle with Mapping to Practices of IEC 62443-4-1[16]

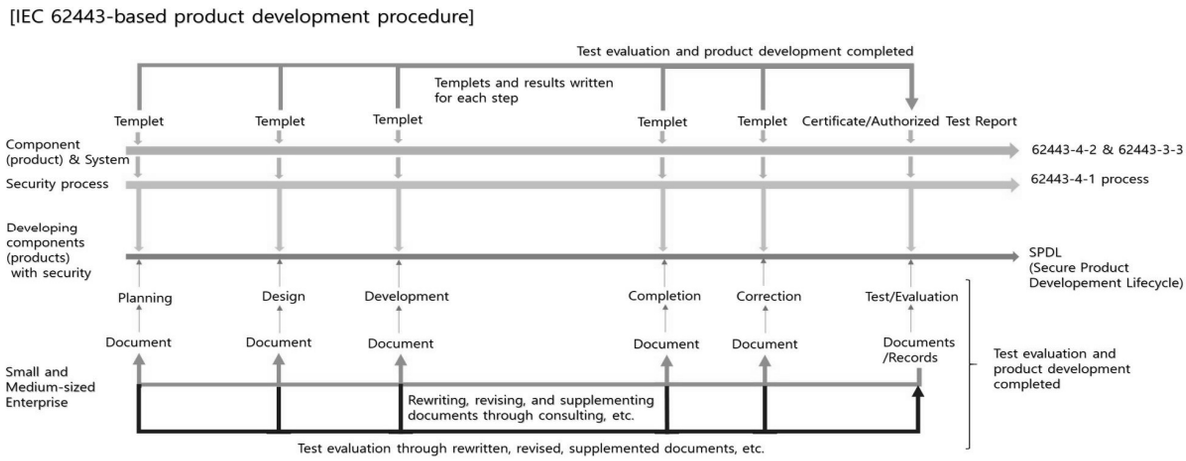

Fig. 4. IEC 62443-4-1 based SPDL Process Applicable to Small and Medium-sized Enterprise Environments

a) 개발 방법: 프로젝트 관련 개발의 진행을 내부 또는 부서에서 “자체”적으로 할 것인지, 외부 또는 타 부서와의 “기술협력”을 통할 것인지, 또는 ”자체“ 및 ”기술협력“을 동시에 진행하는 방식으로 할 것에 대한 선택 및 표기
b) 등급 구분: 과제의 중요도에 따라 A에서 J까지 중 1개를 선택 및 표기
c) 보안과제: 과제의 중요성 및 보안성의 유무에 따라 “적용” “미적용” 중 선택하여 명기
d) 개발 구분: 프로젝트의 목적 및 방향 등에 따라 목적을 기반으로 “제품”, “기술”, “탐색”, “기술지원” 중 선택하여 명기
e) 설계 이관: 프로젝트에 관련된 제품 또는 관련된 부분에 대한 설계의 이관 여부를 결정 표기
f) 연구개발 개요: 프로젝트에 관련된 전체적인 목적과 시장 및 기술 동행, 예상 시장 등에 대한 전반적인 사항에 대한 기술
g) 연구개발 내용: 프로젝트를 위한 연구개발에 대한 세부적인 사항에 대한 기술
h) 대상 기종 및 개발 SPEC: 연구개발에 있어서 진행하려는 제품 또는 내용에 대한 기종의 기술과 관련된 국내외 기술 또는 표준 등에 대한 규격을 정리 및 기술
i) 요구/인증 규격: 제품 또는 기술 개발에 있어서 시장 또는 고객 등으로부터 요구되는 요구사항 및 시험/평가 등을 위한 국내외/민간 인증의 규격 등에 대한 기술
j) 구조도 및 시스템 구성: 제품 및 기술의 개발에 관련된 개념적 또는 세부적인 구조를 도식화하고 시스템 등의 구성에 대한 전반적인 사항을 표기
k) 기대효과: 프로젝트 및 연구개발에 따른 산출물이 기업 또는 시장 등의 환경에 기여하는 효과 등에 대한 정략적 표기 또는 정성적 설명 등을 포함하는 다양한 사업화 분야의 정보 및 내용을 기술
l) 개발기간: 프로젝트에 소요되는 전반적인 기간을 표기하며 최소 “착수”부터 “완료” 단계까지의 각 단계별 소요기간에 대한 표기
m) 부족 기술 대응 방안: 자체적 또는 기업 내부적인 기술 자원 등의 다양한 자산 및 기술의 부족 발생시, 연구개발의 성공을 위하여 필요한 자원의 확보 및 대체 등을 위한 전략적 계획의 기술
n) 기술 확보 계획: 부족 기술에 대하여 내외부로부터 습득하기 위한 전략적 방안에 대하여 방안을 기술
o) Open R&D 계획: 내부 또는 외부의 일반적인 기술의 도입을 통하여 대체가 불가는 또는 어려움의 발생시, R&D를 내부 또는 외부에 공개하고 이에 대한 참여 기업, 대학, 타 연구부서 등의 협력을 위한 대응 계획 수립
p) 보안 Context: 연구개발에 있어서 발생되는 산출물(예: 제품)에 대한 설치 및 구축, 운영 등을 위한 전반적인 내용의 기술과 설치 도면, 표 등을 활용하여 제품의 사용성에 대한 기술
q) 제품의 보안 Context: 제품의 개발 완료후, 적용을 위하여 사용되는 보안 환경 및 구성 등에 대한 전반적인 시스템 환경에 대하여 그림, 표 등을 활용한 기술을 포함.
r) 제품의 Context: 제품 자체의 구조적, 성능적 내용 등에 대한 전반적인 사항을 정리하고 그림, 다이어그램, 표 등을 사용하여 제품의 내적 내용에 대한 기술
s) 제품의 외부 인터페이스: 연구 개발된 제품의 설치를 위하여 필요한 외부의 인터페이스(I/O)에 대한 내용을 정리 및 기술하며, 각 제품의 설치에 따른 “ID”, “외부 인터페이스 명칭” 이에 대한 전반적인 “설명”과 설치되는 제품의 “종류” 등에 대한 다양한 정보를 기술

2) 개발 기준서

개발 기준서는 실제적인 연구 및 제품 개발을 위하여 준비되는 기술 문서의 양식으로 전반적인 결과물, 다시말해 제품에 대한 다양한 기능, 성능, 디자인 등의 내용을 포함하고 있으며, 실제적인 제품의 출고를 위한 내용 등을 포함하게 된다. 개발 기준서에는 기본적인 사항으로 내부 관리용 문서번호를 포함한 개발명, 작성자 등의 정보가 포함되며 내부 승인을 위한 서명란이 있으며, 개정 이력을 관리하기 위해 해당 개발 기준서의 내용에 대한 변경, 수정 등의 발생에 따른 관

Asset		Threat		Cybersecurity property			Impact rating					ATTACK VECTOR-BASED APPROACH
							Impact classification				Impact rating	
				Confidentiality	Integrity	Availability	Safety	Operational	Financial	Privacy		
ID	Asset	ID	Threat	C	I	A	S	O	F	P	IR	AVA
E1	Send and receive payment information	Threat-001	Attacker can spoof user and receive the displayed approval result	Low (L)	Low (L)	Low (L)			Moderate			Network (N)

ATTACK POTENTIAL-BASED APPROACH					CVSS-BASED APPROACH				Final Risk	Cybersecurity Requirement	
Elapsed Time	Expertise	Knowledge of the item or component	Window of opportunity	Attack Tool (equipment)	Attack vector value	Attack complexity value	privileges required	User interaction			
ET	Ex	KIC	WO	AT	AVV	ACV	PR	UI		ID	Description
< 1 week (0)	Layman: 0	Public information: 0	Easy: 1	Standard: 0	0.85	0.00			5.85	CSRQ-0001	Charger shall not grant execute permission on the pages allocated in the data area

Fig. 5. IEC 62443-4-1 based Threat Analysis and Risk Identification Tool Example

리를 위한 개정 이력을 표기하여 관리하게 된다. 특히, 개발된 제품의 성능, 구조, 품질보증, 포장 등에 대한 전반적인 제품 출고를 위한 기준을 중심으로 각각의 단계별 개발기준, 설계입력자료, 검증 방법 등에 관한 내용을 포함하게 되며, 여기서 제품이라 함은 제조품에 대하여는 물리적 형상을 가진 물건을 의미하며, 소프트웨어의 경우는 패키지를 포함하는 무형적 기능을 갖는 것을 의미하게 된다. 개발 기준서에 포함되는 내용에는 다음과 같은 내용이 해당된다.

a) 성능: 제품의 기본적인 성능에 대하여 기술 (그림, 도표 등의 사용)
b) 재료: 제품의 제작에 있어서 사용되는 유/무형적 재료에 대하여 기술 (예: 물리적 제품의 경우 플라스틱 등, 소프트웨어 개발의 경우, 개발 도구 및 솔루션, 환경 등, 그림/도표 사용)
c) 부품 공용화율, 유용화율: 제품 개발에 있어서 기존 제품의 부품 활용 및 공유 비율 등 관련 환경 상황, 제품 등의 사용에 대한 내용 기술 (예: A 제품에서 사용되는 부품의 전체 사용 또는 수정 사용 등, 소프트웨어 개발의 경우, 기존 제품의 모듈 등의 사용)
d) 운전성: 제품의 사용에 대한 내용 기술 (소프트웨어의 경우, UI에 대한 내용 기술 및 포함)
안전성: 제품의 사용에 따른 안전에 관련된 사항 정리
e) 기능 정의: 제품의 기능, 성능, 사용 등에 대한 내용의 정리를 포함. 소프트웨어의 경우 요구사항 및 기능 등에 대한 정의 표함.
f) 구조: 제품의 전체적인 기능, 성능을 포함하는 물리적, 유형적 모습을 정리
g) 외관: 제품의 물리적 외형을 표기하며, 소프트웨어의 경우, UI를 포하는 메뉴 등을 정리
h) 신뢰성: 제품의 성능, 기능 등을 기반으로 오작동 등에 대한 부분을 정리
i) 보전성: 제품의 유효기간 등 및 제품의 보관 방법 등에 관한 내용 정리. 소프트웨어의 경우, 버전 등의 내용과 업데이트, 패치 등에 대한 관리적 측면의 내용 정리
j) 포장: 제품의 출고 및 판매 등을 위한 포장 방식의 내용 정리

3) 위협 분석 및 대응 방안 수립

상기의 개발 요약서와 개발 기준서를 작성하여 식별된 위협에 대하여 위협 분석 및 위험 평가(TARA: Threat Analysis and Risk Assessment)를 통해 위협을 분석하고 대응 방안을 수립하여 관리하여야 한다. 위협 분석 및 위험 평가(TARA)는 사이버 보안에 영향을 주는 위협이 존재하고, 그 위협의 위험 수준이 어느 수준인지를 평가하여, 그에 대한 대책안을 설계에 반영하기 위한 첫 번째 단계이며, 본 분석 활동을 통해 사이버 보안의 목적과 요구사항을 도출할 수 있다. 위협 분석 및 위험 평가(TARA)를 수행하는 방법은 다양하게 존재하며, 본 논문에서는 차량용 사이버보안 국제표준인 ISO/SAE 21434에서 사용하고 있는 위협 분석 및 위험 평가(TARA)를 ICS 환경에 맞추어 수정하여 사용하고자 한다[18]. Fig. 5에서 나타내고 있는 샘플은 IEC 62443-4-1 프로세스에서 사용가능하도록 수정한 위협 분석 및 위험 평가 양식이다. 샘플 양식을 살펴보면 식별된 자산에 대한 위협은 MITRE에서 제공하고 있는 CVE(Common Vulnerabilities and Exposures) 데이터나 Microsoft에서 제공하고 있는 STRIDE 모델로서 도출할 수 있고, 이를 기반으로 기밀성과 무결성, 그리고 가용성에 대한 중요도를 산정하게 되는데, 이때 산정되는 보안 중요도는 높은 수준에 맞추어 조정하게 된다[19,20]. 예를 들면, 기밀성과 무결성은 Low로 설정한다고 하더라도, 가용성에서 High로 설정하게 되면 전체의 보안 중요도는 High로 관리하도록 한다. 이후에 해당 위협이 네트워크 기반인지, 아니면 로컬 혹은 물리적인 연결인지를 설정하여 점수를 산정하고, 위협의 복잡도를 산정하여 점수화시킴으로서 전체 위험 분석을 수행하여 관리하게 된다.

3.4 IEC 62443 기반의 SME 환경 필수보안 요구사항 도출

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

3.3절에서 살펴본 개발 프로세스에서의 위협 식별 단계에서 TARA를 통해 위협을 분석하고 평가하여 관리를 수행하여야 하는데, 이때 실제 개발 단계에서의 보안 요구사항과의 맵핑을 통해 필수보안 요구사항을 관리하여야 한다. 하나의 예를 들면, 스마트제조 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 방법으로 보안성을 확보하여야 한다. 이를 위해서는 스마트제조 환경에서 사용되는 데이터의 무결성 및 기밀성을 보호하기 위해 기기에 적용 가능한 암호화 기술을 개발하여 사용되어야 하며, 이는 국제 표준 규격의 기술을 개발하여 제공함으로써 스마트제조 기기의 데이터 보호 기능을 제공하여야 한다. 하지만, 스마트제조 환경에서 사용되어지는 기기의 열악한 성능상의 이슈를 해결하기 위하여 LEA(Lightweight Encryption Algorithm)와 같은 국제 표준으로 지정된 경량 암호화 알고리즘의 적용을 고려할 필요가 있다[21,22]. 또한, 스마트제조 환경에서 사용되는 기기의 접근 제어 기술 개발이 필요한데, 이는 접근 제어 관리가 쉽지 않은 스마트제어 기기에 적용이 가능한 SW 기술을 개발하는 것을 포함하여, 스마트제조 환경에서 사용되는 구형 PLC(Programmable Logic Controller) 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 62443-4-1 및 4-2 인증을 획득한 기업은 전세계에서 50여개의 기업들이 존재하고 있다. 해당 기업들이 획득한 인증의 수준을 살펴보면, SL1 수준으로만 획득하고 있어서, 스마트공장 환경에서 IEC 62443 SL 수준의 적용은 SL1 수준을 우선적으로 적용하되, 상위 SL 수준에서 정의하고 있는 항목은 필요시 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.

4. 결 론

중소기업환경에서 적용 가능한 IEC 62443 기반의 개발 보안 생애주기 프로세스 적용 방안에 대하여 살펴보았다. 스마트제조 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 이루어야 한다. 이를 위해서는 개발 프로세스를 수립하고 기획 단계에서부터 3장에서 언급하고 있는 요약서 및 기준서, 그리고 TARA를 통해 위협을 식별하고 분석하여 관리가 되어야 한다. 식별된 위협에 대해서는 IEC 62443 기반의 SME 환경 필수보안 요구사항 도출을 통해 적용함으로써 중소기업환경에서 개발에 사용되는 프로세스로 관리가 되어야 한다. 국내 대기업 환경에서는 자체적으로 이러한 IEC 62443 기반의 개발 보안 생애주기 프로세스를 구축하여 운영중이거나, 자체 프로세스에 맞춘 프로세스를 개발하여 적용하고자 노력중에 있다. 하지만, 실제 중소기업 환경에서 IEC 62443 기반의 프로세스를 통해 개발 생애주기를 적용하는 것은 현실적으로 많은 어려움이 존재함에 따라, 본 논문에서 제안하고 있는 위협 분석 및 위험 평가 도구에 대한 교육 및 가이드 작성이 우선적으로 필요할 것으로 판단된다. 따라서, 향후 본 논문을 통해 도출된 위협 분석 및 위험 평가 도구 등에 관한 추가적인 연구를 진행하여 실제 중소기업환경에서 더 쉽게 적용이 가능한 방안을 도출하고자 한다.

References

[1] M. K. Gil, “In 2021, the first year of OT security... Co-operation between ICS operators, manufacturers, and security vendors is essential” [Internet], https://www.dailysecu.com/news/articleView.html?idxno=110872.

[2] Hugh Taylor, “News Insights: Gangnam Industrial Style: Apt Campaign Targets Korean Industrial Companies - Cyberx” [Internet], https://journalofcyberpolicy.com/2019/12/17/news-insights-gangnam-industrial-style-apt-campaign-targets-korean-industrial-companies-cyberx/.

[3] The White House, “FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks” [Internet], 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] IEC 62443-4-1:2018, “Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements,” Jan. 15, 2018.

[5] IEC Editorial Team, “Understanding IEC 62443” International Electrotechnical Commission News & blogs, Feb. 26, 2021, [Internet], https://www.iec.ch/blog/understanding-iec-62443.

[6] IEC TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, Jul. 30, 2009.

[7] IEC 62443-2-1:2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program, Nov. 10, 2010.

[8] IEC TR 62443-2-3:2015, Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment, Jun. 30, 2015.

[9] IEC TR 62443-3-1:2009, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems, Jul. 30, 2009.
[10] IEC TR 62443-2-3:2015, Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment, Jun. 30, 2015.
[11] IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, Aug. 7, 2013.
[12] IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, Feb. 27, 2019.
[13] ISO/IEC/IEEE 24748-1:2018, Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management, Nov. 2018.
[14] ISO/IEC/IEEE 15288:2015, Systems and software engineering — System life cycle processes, May 2015.
[15] ISO/IEC/IEEE 12207:2017, Systems and software engineering — Software life cycle processes, Nov. 2017.
[16] Kilian Marty, "How to implement Cyber Security acc. to IEC 62443," CertX, Nov. 12, 2020, https://certx.com/cybersecurity/how-to-implement-cyber-security-acc-to-iec-62443-ep-4-penetrations-tests.
[17] J. J. Ha, J. T. Kim, S. S. Park, and K.h. Han, "A study on threat analysis and risk assessment in a smart manufacturing environment based on IEC 62443," *KICS Fall Conference 2021*, Nov. 18, 2021.
[18] ISO/SAE 21434:2021, Road vehicles — Cybersecurity engineering, August, 2021
[19] The MITRE Corporation, CVE Program [Internet], https://www.cve.org/.
[20] A. Shostack, "Experiences threat modeling at microsoft," *MODSEC@ MoDELS 2008*, 35, 2008.
[21] ISO/IEC 29192-2:2019, Information security — Lightweight cryptography — Part 2: Block ciphers, Nov. 2019.
[22] KS X 3246:2016, 128-bit block cipher LEA, Oct. 20. 2016.

진 정 하

https://orcid.org/0000-0001-5303-7673
e-mail : nemoda75@korea.ac.kr
2002년 금오공과대학교 전자통신공학과(학사)
2006년 건국대학교 정보보안전공(석사)
2020년 건국대학교 정보보안전공(박사)
2020년 ~ 현 재 고려대학교 정보보호연구원 연구교수
관심분야 : 융합 보안, 사이버 보안, IEC 62443 표준

박 상 선

https://orcid.org/0000-0002-5832-6631
e-mail : sitcs@naver.com
1990년 인천대학교 전자공학과(학사)
1996년 Wollongong UNIV. 컴퓨터공학(석사)
1997년 Wollongong UNIV. 정보통신공학(석사)
2001년 Wollongong UNIV. 정보통신공학(박사)
2001년 ~ 2004년 ㈜한국심트라 영업본부팀장
2005년 ~ 2007년 (사)한국전자지불산업협회 기획연구부장
2007년 ~ 2015년 ㈜아이씨티케이 기술기획실장
2011년 ~ 2015년 한양대학교 융합전자공학부 겸임교수
2016년 ~ 2021년 한국시스템보증㈜ 기업부설연구소 이사
2021년 ~ 현 재 고려대학교 정보보호연구원 수석연구원
관심분야 : 융합 보안, 사이버 보안, IEC 62443 표준

김 준 태

https://orcid.org/0000-0002-8705-4196
e-mail : tae8579@gmail.com
2014년 경남대학교 컴퓨터공학과(학사)
2017년 건국대학교 IT융합정보보호학과(석사)
2020년 건국대학교 컴퓨터공학과(박사수료)
2017년 ~ 2019년 ㈜아이티센 아키/클라우드팀
2021년 ~ 현 재 고려대학교 정보보호연구원 수석연구원
관심분야 : 융합 보안, 사이버 보안, IEC 62443 표준

한 근 희

https://orcid.org/0000-0001-6385-0617
e-mail : khhan1@korea.ac.kr
1986년 서울과학기술대학교 컴퓨터공학과(학사)
1988년 한양대학교 정보보호전공(석사)
2006년 고려대학교 정보보호전공(박사)
2006년 ~ 2012년 행정안전부, 국가정보자원관리원 사이버안전과장
2013년 ~ 2017년 고려대학교 정보보호대학원 산학협력중점교수
2017년 ~ 2019년 건국대학교 소프트웨어학과 교수
2019년 ~ 현 재 고려대학교 정보보호연구원 연구교수
관심분야 : 융합 보안, 사이버 보안, IEC 62443 표준