논문 19-44-05-21 The Journal of Korean Institute of Communications and Information Sciences '19-05 Vol.44 No.05
https://doi.org/10.7840/kics.2019.44.5.943

4차 산업혁명 시대의 산업 제어시스템 보안성 평가 방안 연구

김 우 년◆, 박 응 기*, 김 신 규*

A Study on a Cybersecurity Evaluation Method for Industrial Control Systems in the 4th Industrial Revolution Era

Woonyon Kim◆, Eung-Ki Park*, Sin-Kyu Kim*

요 약

4차 산업혁명으로 공장은 공개 상용 ICT 기술이 적용되고 다른 네트워크와 연결된 스마트공장으로 발전하고 있다. 이러한 스마트공장의 현장 자동화 분야에 이용되는 산업 제어시스템 역시 다른 네트워크와 연결되고 이더넷 및 무선 통신 기술을 활용함으로써 보안위협이 증가되고 있다. 본 논문은 스마트공장에서 사용되는 산업 제어시스템의 증가하는 보안위협에 대응하기 위한 방안으로써 산업 제어시스템 보안성 평가 방안을 제시하였다. 산업 제어시스템 보안성 평가 방안은 구성요소에 대한 평가와 운영 전 구축단계의 평가로 구분하였다. 구성요소 보안성 평가는 국내 산업 제어시스템 시장 환경을 고려하여 국제적으로 통용되는 IEC 62443-4-2 표준 기반의 보안성 평가 방안을 제시 하였다. 또한 구축단계 보안성 평가는 국내 사이버 보안위협과 규제 현실을 반영하여 자체적인 기준을 기반으로 운영기관의 보안관리 프로세스와 취약점을 평가하는 방안을 제시하였다. 이러한 방안을 추진함으로써 스마트공장 구축 시에 보안성이 확보된 구성요소를 도입하고, 운용하기 전 보안관리 프로세스를 적용함으로써, 스마트공장의 보안성을 확보할 수 있을 것으로 기대된다.

Key Words : Smart Factory Security, ICS Security, SCADA Security, ICS Cybersecurity Evaluation

ABSTRACT

With the 4th industrial revolution, a factory is evolving into a smart factory with open commercial ICT technologies and connecting to other networks. Industrial control systems used in the automation field of the smart factory are also connected to other networks, so cybersecurity threats are increased because of utilizing Ethernet and wireless communication technologies. In this paper we present an industrial control system security evaluation method as a countermeasure against increasing security threats of the ICSs used in smart factories. We propose two evaluation types, one is a component evaluation and the other is pre-commissioning evaluation. The component security evaluation is based on internationally accepted IEC 62443-4-2 standard by considering domestic ICS market environment. In addition, the pre-commissioning evaluation is based on Korea's unique requirements, reflecting the domestic cyber security threats and regulatory. This process also assesses the security management process of it and vulnerabilities of the operational readiness. By implementing these ICS evaluation schemes, smart factories are built with the design-by-security components. And by applying the security management process and vulnerability assessment to smart factories at pre-commissioning stage, we anticipate that smart factories will be more secure.

◆ First Author : The Affiliated Institute of ETRI, wnkim@nsr.re.kr, 정회원
* The Affiliated Institute of ETRI, ekpark@nsr.re.kr, 정회원; skkim@nsr.re.kr
논문번호 : 201902-448-0-SE, Received January 31, 2019; Revised April 2, 2019; Accepted April 2, 2019

Ⅰ. 서 론

4차 산업혁명으로 스마트공장에 대한 관심이 고조되고 있다. 스마트공장은 제조업과 ICT 기술의 융합으로 기계 스스로 시뮬레이션을 통해 자동 생산하는 시스템이 구축된 공장을 의미한다[1]. 스마트공장은 국내 제조업의 경쟁력을 높이는 유일한 기술로 인식되고 있으며, 4차 산업혁명 변화의 가장 중심에 있다고 보고 있다[2]. 산업부의 민관합동 스마트공장 추진단은 2025년까지 스마트공장 3만개를 보급·확산한다는 계획아래 2019년 1월 기준으로 4,431개의 스마트공장 구축 지원을 완료하였고 572개는 구축 지원이 진행 중인 등 총 5,003개의 스마트공장 구축을 지원하고 있다[3]. 스마트공장은 현장 자동화, 공장운영, 기업자원관리, 제품개발, 공급사슬관리의 다섯 분야에 대해 ICT 기술의 활용 수준에 따라 ICT 미적용, 기초수준, 중간 수준1, 중간 수준2, 고도화의 다섯 수준으로 구분된다[4]. 이들 중에서 현장 자동화 분야는 ICT 기술이 적용된 산업 제어시스템을 이용하여 물리적인 설비의 상태 정보를 수집 및 분석하고 자동화 운전을 수행하는 분야이다.

산업 제어시스템은 산업설비로부터 더 짧은 주기로 더 많은 데이터를 유·무선 통신으로 수집하여 저장하고, AI 기술을 이용하여 빅데이터를 분석함으로써 산업설비의 운영 효율성을 제고하고 자율운전이 가능한 방향으로 발전하고 있다. 실제 미국의 GE사는 이러한 기술이 탑재된 디지털발전소 솔루션을 보급하여 고장을 10배 이상 더 일찍 발견하고 부정확한 진단을 75%까지 줄였으며, 설비의 효율 분석, 센서의 건전성 검증, 효율이 낮은 설비의 개선방안을 가이드 하는 등 운영 효율성을 높였다[5].

4차 산업혁명 이전에도 에너지 시설, 교통시설, 수처리 시설, 제조 공장의 제조시설 등은 산업 제어시스템에 의해 운영되었다. 전통적인 산업 제어시스템은 폐쇄망에서 비공개 전용 운영체제, 전용 소프트웨어, 전용 통신기술을 사용함으로써 상대적으로 사이버보안 측면에서 안전하다고 여겨졌다. 그러나 2010년 Stuxnet 악성코드, 2014년 블랙 에너지 APT 공격, 2015년 우크라이나 전력망 공격, 2016년 CrashOverride 등 실제 산업 제어시스템을 대상으로 다양한 형태의 사이버공격이 발생하여 더 이상 사이버보안의 안전지대가 아님이 확인되었다. 또한 앞으로 구축되는 스마트공장의 산업 제어시스템은 상용 운영체제, 상용 소프트웨어, 이더넷 통신, 무선 통신 등의 ICT 기술을 적극 도입하고, 네트워크로 상호 연결됨으로써 지금보다 더 많은 사이버 보안위협에 노출될 것으로 예상된다.

산업 제어시스템은 물리적인 산업설비를 모니터링하고 제어하여 산업 프로세스를 실행하기 때문에 사이버 보안위협으로 인한 오동작, 중단 등으로 인해 물리적인 피해 파급 효과가 발생할 수 있다. 또한 이로 인해 사람의 건강과 안전, 환경오염 등의 심각한 피해가 발생할 수 있다. 따라서 산업 제어시스템 보안은 가용성을 최우선으로 무결성과 기밀성을 보장하는 순서로 고려해야 한다[6]. 이를 위해서는 산업 제어시스템을 구성하는 센서/디바이스, 네트워크, 플랫폼, 애플리케이션이 보안 요구사항을 만족하도록 개발되었는지, 구축된 산업 제어시스템이 안전하게 운용하도록 준비되었는지 보안성을 평가하는 것이 필요하다. 이는 산업 제어시스템의 구성요소 개발 및 구축단계부터 보안을 고려하지 않을 경우 운용단계에서 가용성의 문제로 인해 보안패치 설치, 백신 설치 및 업데이트와 같은 기술적 보안대책을 적용하기 어렵기 때문이다.

본 논문은 산업 제어시스템을 구성하는 구성요소와 신규 구축된 산업 제어시스템의 보안성 평가 방안을 제시한다. 해외에서는 산업 제어시스템에 대한 보안성을 평가하기 위한 다양한 제도가 국제표준기구나 시험기관 등에서 이미 진행되고 있으나, 국내에서는 스마트공장 등에 적용할 수 있는 산업 제어시스템 대상의 보안성 평가 방안이 없는 실정이다. 본 논문에서 제안하는 보안성 평가 방안은 해외의 관련 제도를 비교·분석하고 국내 산업 제어시스템의 산업 환경을 고려하여 보안성 평가 분야와 대상 선정, 평가 기준의 설정, 평가 체계 마련 방안을 제안한다. 또한 국외의 산업 제어시스템 보안성 평가 방안과 제안하는 방안을 비교하여 국내 산업 환경에 적합함을 설명한다.

본 논문은 총 6장으로 구성되어 있다. Ⅱ장에는 산업 제어시스템 보안위협에 대해서 설명하고, Ⅲ장에서는 관련동향으로써 해외의 산업 제어시스템 보안성 평가·인증 제도 현황을 분석한다. Ⅳ장에서는 국내 산업 제어시스템 보안성 평가·인증과 유사한 제도 현황을 설명하고, Ⅴ장에서는 국내 스마트공장에 적용가능한 산업 제어시스템 보안성 평가 방안을 제시하며, Ⅵ장에서 본 논문의 결론과 향후 연구방향을 제시한다.

Ⅱ. 산업 제어시스템 보안위협

산업 제어시스템에 대한 보안 취약점은 2010년 Stuxnet 발견 이후 지속적으로 발견되고 있다.

Positive Technologies에서 2018년 발간한 ICS 보안 보고서[7]에는 그림 1과 같이 ICS 구성요소에서 2013년 158개에서 2017년 197개로 매년 100개 이상의 새로운 보안 취약점이 지속적으로 발견되고 있다. 이러한 취약점은 PLC와 같은 제어기기, 산업용 네트워크 장비, 산업 제어시스템용 소프트웨어, 감시 및 제어용 SCADA/HMI/DCS 등 산업 제어시스템을 구성하는 모든 요소에서 취약점이 발견되고 있다.

그러나 더욱 문제는 취약한 구성요소들이 보안패치가 적용되지 않은 채 운용이 된다는 사실이다. FireEye에서 2016년 8월 발표한 '2016 ICS 취약점 동향 보고서[8]'에 따르면 2010년부터 2016년 4월까지 약 1/3의 보안취약점이 패치가 발표되지 않은 상태에서 공개되었다고 밝혔다. FireEye는 패치가 되지 않는 이유를 4가지로 추정하였다.

① 취약점 발견자가 제조사에 취약점을 통보하지 않고 공개한 경우
② 제조사가 취약점을 통보받고도 적절히 대응하지 않은 경우
③ 패치 자체가 어려운 경우
④ 제조사가 더 이상 서비스를 지원하지 않는 제품의 취약점인 경우

보안패치가 되지 않은 4가지 이유 중 마지막 ③, ④는 앞으로도 보안패치가 불가능한 경우이고, ②의 경우도 제조사가 보안취약점을 파악하고도 미조치 상태라면 앞으로도 보안패치가 어려울 것으로 예상된다. ①의 경우도 패치를 할 수 있는 경우와, 패치가 불가능한 경우가 있을 수 있다. 따라서 발견된 보안취약점은 일부 패치가 이루어질 수 있으나 대부분은 패치가 되지 않은 채로 남아 있을 가능성이 높고, 이는 스마트공장의 보안위협이 된다.

운용 중인 산업 제어시스템에 대한 실제 사고사례를 살펴보면 2014년 독일 연방정부 보고서에서 공개된 철강회사 산업 제어시스템 해킹사고[6], 2015년 12월 우크라이나 키예프의 전력 시스템 해킹으로 인한 정전사고[9], 2016년 우크라이나 전력망 해킹에 의한 2차 정전사고[10] 등이 있다. 독일 철강회사 해킹은 산업 제어시스템이 인터넷 및 업무시스템과 연계된 채 운용되어 APT 공격으로 발생한 사고였으며, 우크라이나의 해킹에 의한 전력망 정전사고 역시 원격 접속 관리의 부실로 인해 발생한 사고였다.

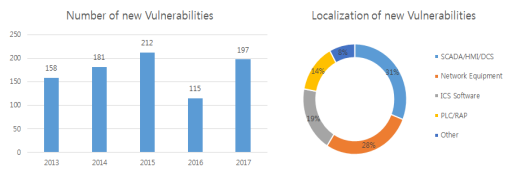

그림 1. 산업 제어시스템 신규 취약점 발견 수(좌) 및 구성요소별 비율(우)[7]
Fig. 1. Number of new Vulnerabilities(left) and Localization of new Vulnerabilities(right) in ICS

따라서 산업 제어시스템을 안전하게 운용하기 위해서는 산업 제어시스템 구성요소가 최소한의 보안 요구사항을 만족하도록 개발되었는지 평가하여 도입함으로써 제조사가 설계 및 개발 단계에서부터 보안을 고려하도록 유도해야 한다. 또한 보안성이 확인된 구성요소를 이용하여 산업 제어시스템을 구축했더라도, 안전한 운용원칙이 무시된 채 운용의 편의성만 우선시할 경우 보안이 문제가 될 수 있으므로, 구축된 산업 제어시스템에 대해서도 보안평가가 필요하다.

Ⅲ. 산업 제어시스템 보안성 평가 · 인증 제도 현황

산업 제어시스템에 대한 보안성을 평가하는 제도는 GE에서 운영하는 Achilles 인증[11], 산업 자동화 협회인 ISA 산하 ISCI(ISA Security Compliance Institute)의 ISASecure 인증[12], TÜV SÜD의 IEC 62443 인증[13], exida의 사이버보안 인증 제도[14], IECEE 산업 사이버보안 인증[15,16], UL 사이버보안 보증 제도[17,19], 프랑스의 CSPN 인증[20], 일본의 CSMS 인증[21] 등이 있다. 본 장에서는 각각의 산업 제어시스템 보안성 평가 · 인증 제도에 대해서 설명한다.

3.1 Achilles 인증

GE Wurldtech에서 제공하는 사이버보안 인증 제도로 네트워크 견고성을 인증하는 Achilles Communications Certification(ACC)과 제어시스템 구성요소 제조사나 시스템 통합 사업자의 보안정책, 절차 등의 보안 프로세스를 인증하는 Achilles Practices Certification(APC)이 있다[11].

ACC는 제어시스템에서 반드시 확보되어야 할 네트워크 가용성을 평가하는 시험 · 인증 제도로써, 대상은 PLC, DCS, RTU와 같은 임베디드 장치, EWS, 히스토리안, 도메인 컨트롤러와 같은 호스트 기반 장치, HMI S/W, Engineering S/W 등의 제어 애플리케이션, 라우터, 스위치 등의 네트워크 컴포넌트를 대상으로 한다. 시험 항목은 통신 계층별 프로토콜에 대해서 프로토콜 퍼징 시험, 알려진 취약점 확인, 트래픽 부하 시험을 수행[11]한다.

APC는 네덜란드 소재의 프로세스 자동화 사용자

협회(The Process Automation Users' Association)인 WIB가 2010년 11월에 발표한 산업 제어시스템 보안 요구사항 WIB V2.0을 기반으로 산업 제어시스템 구성요소 제조사의 사이버보안 절차, 실무지침, 개발·시험·유지관리 등 생명주기 전반에 걸친 모범사례에 대해 평가하고 인증을 부여하고 있다[22]. WIB 2.0 문서는 제조사를 위한 보안 요구사항으로서 산업 제어시스템 보안 분야 국제표준인 IEC 62443 표준의 한 부분(IEC 62443-2-4)으로 반영되었다.

3.2 ISASecure 인증

ISASecure 인증은 국제자동화협회인 ISA(International Society of Automation) 산하의 보안 준수기구인 ISCI(ISA Security Compliance Institute)에서 운영하는 보안성 평가·인증 제도로, IEC 62443 표준 적합성 인증서를 발행한다[12]. ISASecure 인증은 대상에 따라 3가지 인증 제도를 운영하고 있다. PLC, DCS Controller, SIS Controller, Field Sensor Device 등의 임베디드 장치의 보안기능을 인증하는 EDSA(Embedded Device Security Assurance) 인증[12, 25], 한 개 이상의 컴포넌트가 결합된 하나의 제품 형태인 시스템을 인증하는 SSA(System Security Assurance) 인증[12] 제도가 있다. 또한 제어시스템 구성요소 제조사의 안전한 개발 프로세스를 인증하는 SDLA(Security Development Lifecycle Assurance) 인증[12] 제도도 운영하고 있다.

EDSA 인증은 2019년 1월 현재 3.0.0 버전의 기준이 적용되고 있으며, 임베디드 장치 견고성 시험, 보안기능 평가, 개발 보안 평가를 수행한다. 임베디드 장치 견고성 시험은 장치의 취약점 식별 시험과 네트워크 견고성 시험으로 구성된다. 네트워크 견고성 시험은 Ethernet, ARP, IPv4, ICMPv4, UDP, TCP 프로토콜 헤더에 대한 퍼징과 스트레스 시험을 수행한다. 보안기능 평가는 IEC 62443-4-2 표준을 기반으로 장치의 보안기능을 시험하며, 개발 보안 평가는 IEC 62443-4-1 표준을 기반으로 보안개발 프로세스와 보안개발 결과물 평가를 수행한다.

SSA 인증은 2019년 1월 현재 3.0.0 버전의 기준이 적용되고 있으며, 시스템 견고성 시험, 임베디드 장치 보안기능 평가, 시스템 보안기능 평가, 개발 보안 평가를 수행한다. 시스템 견고성 시험은 시스템에 대한 취약점 식별 시험, 네트워크 견고성 시험, 네트워크 스트레스 시험을 수행하며, 임베디드 장치 및 시스템 보안기능 평가는 IEC 62443-3-3 표준, 개발 보안 평가는 IEC 62443-4-1 표준을 기반으로 한다.

EDSA와 SSA 인증을 신청하는 제조사는 미리 SDLA 인증을 받거나, EDSA 및 SSA 인증과 함께 병렬로 SDLA 인증을 신청해야 한다.

SDLA 인증은 2019년 1월 현재 2.0.0 버전의 기준이 적용되고 있으며, IEC 62443-4-1 표준을 기반으로 제조사의 제조 프로세스가 보안 요구사항을 만족하는지 확인한다.

ISASecure 인증 제도의 시험기관은 미국의 exida, 일본의 CSSC-CL, 독일의 TÜV Rheinland가 있으며, 시험기관별 시험 가능한 요구사항 버전은 표 1과 같다. exida는 EDSA, SSA, SDLA에 대해서 시험을 수행하고 인증서를 발급하며, CSSC-CL은 EDSA에 대해서만 시험 및 인증서 발행이 가능하다. 독일의 TÜV Rheinland는 EDSA와 SDLA에 대해서 시험을 수행하고 인증서를 발행할 수 있다.

표 1. 시험기관 별 ISASecure 요구사항 승인 현황
Table 1. ISASecure Requirements Version for Testing laboratories

Testing Lab.	EDSA (Approved Version)	SSA (Approved Version)	SDLA (Approved Version)
exida	O (2.0.0, 2.1.0, 3.0.0)	O (2.0.0, 2.1.0, 3.0.0)	O (2.0.0)
CSSC-CL	O (2.1.0)	-	-
TÜV Rheinland	O (2.0.0)	-	O (2.0.0)

3.3 IEC 62443 인증

독일의 시험 인증기관인 TÜV SÜD는 독일 인정기관인 DAkkS(German Accreditation Body)로부터 IEC 62443 표준에 따른 시험기관으로 인정받았으며, 산업 제어시스템 사이버보안 인증 서비스를 제공한다. 인증은 IEC 62443-2-4와 IEC 62443-3-3 표준을 기반으로 시스템 통합 사업자에 대한 보안을 인증하고, IEC 62443-4-1과 IEC 62443-3-3 표준을 기반으로 제조사를 인증한다[13]. Siemens의 Simatic PCS7 프로세스 제어시스템이 IEC 62443-4-1과 IEC 62443-3-3 표준 기반으로 인증을 받았으며, Phoenix Contact은 2018년에 IEC 62443-4-1:2018 Edition 1.0으로 인증을 받았다.

TÜV SÜD는 산업 제어시스템을 대상으로 IEC 62443 인증이외에도, 산업 IT 보안 시험소를 설립하여 산업 제어시스템 대상의 네트워크 견고성 시험 서

비스를 별도로 제공하고 있다.

3.4 exida 사이버보안 인증제도

exida는 미국의 시험기관으로서 ISASecure 인증과 exida 자체 인증 서비스를 제공하고 있다[14]. exida의 ISASecure 인증제도는 3.2절에서 설명한 ISASecure 인증에 대한 시험·인증기관으로서 EDSA, SSA, SDLA 기준에 의거 시험을 수행하고, 인증서를 발급한다. exida 자체 인증으로는 IEC 62443 사이버보안 인증 프로그램이 있으며 엔지니어링 프로세스 사이버보안 인증, 장치 및 애플리케이션 사이버보안 인증, 시스템 사이버보안 인증, 인력의 사이버보안 자격 인증의 4가지 인증 서비스를 제공한다[14]. 표 2는 IEC 62443 표준 기반의 exida 산업 제어시스템 사이버보안 인증제도 현황이다.

표 2. exida의 IEC 62443 인증제도[14]
Table 2. IEC 62443 based certifications scheme in exida

IEC Standards	Classification	Program Name	Applicable to
Category 1: Cybersecurity Engineering Process Certifications			
62443-4-1	Device Process Certification	exida Security Development Process	OEM New Product Development
62443-2-4	System Process Certification	exida System Integrator Process	System Integrator
Category 2: Cybersecurity Device and Application Certifications			
62443-4-1 62443-4-2	Device and Application Certification	exida Security Device Certification	OEM Product
Category 3: Cybersecurity System Certifications			
62443-4-1 62443-4-2	OEM System Certification	exida System Security Certification	OEM System
62443-2-4 62443-3-3	Integrated System Certification	exida Integrated System Certification	Integrated System
Category 4: Cybersecurity Personnel Certification			
62443-4-1 62443-4-2	Personnel Certification	CACE/CACS Software	OEM Developers
62443-2-4 62443-3-3	Personnel Certification	CACE/CACS Design	System Designer
62443-2-4 62443-3-3	Personnel Certification	CACE/CACS Integrator	System Integrator

3.5 UL 사이버보안 보증제도

미국에 본사를 둔 표준 개발, 인증, 감사, 시험, 검사 등의 서비스를 제공하는 글로벌 회사인 UL은 산업 제어시스템에 대한 사이버보안 보증제도인 CAP (Cybersecurity Assurance Program) 서비스를 제공하고 있다[17]. CAP 서비스는 UL 2900-2-2 표준 기반의 UL CAP for ICS와 IEC 62443 표준 기반의 UL CAP for IEC 62443이 있다. UL CAP for ICS는 UL 2900-2-2 Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems(Ed. 2) 표준을 기반으로 시험 서비스와 인증 서비스를 제공한다. 시험 서비스는 산업 제어시스템을 대상으로 퍼징 시험, 알려진 취약점 확인, 코드 및 바이너리 분석, 접근통제 및 인증, 암호, 원격 통신, 소프트웨어 업데이트, 침투 테스트 등의 시험을 수행하고 시험결과 보고서를 제공하며, 인증 서비스는 UL 표준 전체 요구사항에 대한 시험 결과를 토대로 인증서를 제공한다[17]. UL CAP for ICS 인증을 받은 제품은 네트워크 게이트웨이, I/O 장치, 플랫폼, 대시 보드 프로세서 등 4개 제품이 있다[18].

UL CAP for IEC 62443 서비스는 UL이 IECEE의 산업 사이버보안 인증제도에 국가인증기관(NCB, National Certification Body)으로 참여하여, 시험을 수행하고 인증서를 발행하는 제도이다[19]. UL은 IEC 62443-2-4, IEC 62443-3-3, IEC 62443-4-1, IEC 62443-4-2 표준을 기반으로 시험·인증 서비스를 제공하며, 시험의 세부 방법으로서 침투 테스트, 취약점 분석, 소스코드 분석, 퍼징 시험 등을 수행한다.

3.6 IECEE 산업 사이버보안 인증제도

IECEE는 국제 전기기기 적합성 평가제도로서, 사무실, 가정, 공장 등에서 사용하는 23개 품목의 전기기기에 대해 감전, 화재 위험 등으로부터 소비자를 보호할 수 있도록 안전(safety), 품질(quality), 효율(efficiency), 성능(performance)에 대한 시험을 IEC 규격에 따라 실시하고 국제적으로 통용될 수 있도록 인증을 부여하는 제도이다[15]. IECEE는 2016년 11월 28일 운영문서(OD) 2061 V1.0을 발표하면서 IEC 62443 표준 기반의 산업 사이버보안 인증 프로그램을 시작하였고, 2018년 2월 7일에는 업데이트된 OD-2061 V1.1을 발표하였다[16]. 운영문서에 따르면 IECEE에서 제공하는 산업 사이버보안 인증은 국가인증기관(NCB: National Certification Body)이 역량평가(capability assessment)와 역량 적용성 평가(application of capabilities assessment)의 두 가지 시나리오에 대해 평가하고 6가지 인증서를 발급한다[16]. 6가지 인증서 종류 중 Solution Capability Assessment와 Process Application of Capability Assessment의 2가지는 향후 고려할 예정이며, 나머지

표 3. 인증서 종류와 IEC 62443 표준의 적용[16]
Table 3. Certifications and IEC 62443 series of standards application

	IEC 62443-2-4	IEC 62443-3-3	IEC 62443-4-1	IEC 62443-4-2 (Future Consideration)
Process	Process Capability Assessment		Process Capability Assessment	
Product	Product Capability Assessment	Product Capability Assessment	Product Application of Capability Assessment	Product Capability Assessment
Solution	Solution Application of Capability Assessment			

4가지 인증서의 IEC 62443 표준별 적용 사례는 표 3과 같다.

IECEE 인증은 각 NCB가 인증하고, NCB에 속한 시험기관(CBTL: Certification Body Testing Laboratories)이 시험을 수행한다. NCB에는 인증서를 발급하고 다른 국가의 NCB가 발급한 인증서를 인정해줄 수 있는 발급(Issuing) 및 인정(Recognizing) NCB와 다른 국가의 NCB가 발급한 인증서를 인정만 해줄 수 있는 인정(Recognizing) NCB로 구분된다. 2019년 1월 기준 IECEE가 승인한 IEC 62443 표준별 NCB와 CBTL의 수는 표 4와 같다.

IECEE 산업 사이버보안 인증제도에 참여하는 NCB 중에서 자체적으로 IEC 62443 관련 인증을 소개하고 있는 곳은 UL의 CAP for IEC 62443 인증[19], DEKRA의 Cyber Security Certification: IEC 62443[23], TÜV NORD의 Certification according to IEC 62443[24]이 있다. UL CAP for IEC 62443은 IECEE 산업 사이버보안 인증제도에 UL이 참여하여 만든 인증으로서 3.5절에서 설명하였다. 현재는 IEC 62443-2-4:2015, IEC 62443-2-4:2015/AMD1:2017, IEC 62443-3-3:2013, IEC 62443-4-1:2018 표준에 대해 인증제도를 운영하고 있으며, 덴마크 UL이 NCB, UL Northboork이 CBTL로 IECEE로부터 승인받았다. DEKRA도 UL과 동일한 표준에 대해 DEKRA Certification B.V.가 NCB와 CBTL로써 IECEE로부터 승인받았다. DEKRA에서 실시하는 IECEE 사이버보안 인증제도 관련 세부사항은 공개되어 있지 않다. TÜV NORD도 UL, DEKRA와 동일한 표준에 대해 TÜV NORD CERT GmbH가 NCB와 CBTL로써 IECEE로부터 승인 받았다. TÜV NORD는 '안전을 위한 보안(Security4Safety)' 인증을 통해 4차 산업 준비도(Industry 4.0 readiness)를 달성하도록 권고하고 있다[24]. 이 제도는 제품, 컴포넌트, 프로세스에 대해서 위험평가를 수행하고, 조직의 IT 분야는 ISO 27001 인증을, 산업 제어시스템이 운영되는 OT(Operation Technology) 분야는 IEC 62443 인증을 받는 것으로 4차 산업 준비도를 달성할 수 있다고 제시하고 있으나, 세부사항은 공개하고 있지 않다.

표 4. IECEE의 IEC 62443 표준별 시험기관 현황
Table 4. IEC 62443 CBTL and CB in IECEE

Standards	IECEE Approved	# of CBTL	# of I&R NCB	# of R NCB
IEC 62443-2-4:2015	2017.7.25.	13	12	1
IEC 62443-2-4:2015 /AMD1:2017	2017.10.11.	12	11	2
IEC 62443-3-3:2013	2018.6.8.	5	5	2
IEC 62443-4-1:2018	2018.6.8.	5	5	2

* I&R NCB: Issuing and Recognizing NCB
* R NCB: Recognizing NCB

3.7 CSPN 인증제도

프랑스의 국가정보시스템보안청인 ANSSI(Agence nationale de la sécurité des systèmes d'information)에서 CC인증에 비해 단기간에 저렴한 비용으로 프랑스 자국내에서만 통용되도록 설계한 인증제도로써 2008년부터 IT보안제품을 대상으로 하고 있다[20]. 2016년부터는 PLC와 산업용 스위치에 대한 보안평가를 실시하고 있으며, 2019년 1월 기준으로 Siemens PLC 2종과 Schneider Electric PLC 1종 등 PLC 3개 제품과 Siemens의 Scalance 산업용 스위치 1개 제품이 인증을 받았다[20].

3.8 CSMS 인증제도

CSMS(Cyber Security Management System) 인증은 산업 제어시스템 사이버보안 관리 시스템을 대상으로 한 제3자 인증제도이다[21]. 사단법인 정보관리시스템인증센터가 인정기구 역할을 하고, 인증기관은 일본 BSI(The British Standards Institution)와 일본품질보증기구관리시스템(JQA)이 역할을 수행한다[21]. CSMS 인증은 IEC 62443-2-1:2010 표준을 기준으로 위험 분석, CSMS 위험 해소, 세부 보안 통제항목, CSMS 모니터링 및 개선 요구사항으로 정의되어 있다[21]. 따라서 CSMS 인증은 운영중인 제어시스템에 적용되는 보안관리 프로세스에 대해 평가하고 인증하는 체계이다.

Ⅳ. 국내 산업 제어시스템 보안성 평가 현황 분석

국내에는 산업 제어시스템에 대한 보안성만을 평가하는 제도는 없으나, 정보통신기반보호법에 의해 시행하는 주요정보통신기반시설 취약점 분석·평가제도에 산업 제어시스템 대상의 취약점 분석·평가 기준이 일부 반영되어 있으며, 사물인터넷 제품에 대한 보안성을 평가하는 IoT 보안인증서비스가 있다. 또한 관련 유사제도로는 보안적합성 검증제도와 정보보호제품 평가·인증제도가 있다.

4.1 주요정보통신기반시설 취약점 분석·평가제도

정보통신기반보호법은 도로, 철도, 지하철, 공항, 항만 등 주요 교통시설, 전력, 가스, 석유 등 에너지·수자원 시설 등의 국가안전보장에 중대한 영향을 미치는 산업 제어시스템을 주요정보통신기반시설로 지정하여 관리하도록 하고 있다[26]. 동법에 의해 주요정보통신기반시설로 지정된 시설은 고시된 기준에 의해 매년 취약점 분석·평가를 실시해야 한다[26]. 산업 제어시스템에 대한 평가는 취약점 분석·평가 기준의 기술적 분야의 제어시스템 세부 분야에 기본항목 16개, 선택항목 6개 등 총 22개 항목이 있다[27]. 실제 운용중인 산업 제어시스템에 대한 평가는 제어시스템 세부 분야의 22개 항목 이외에도 관리적·물리적 분야와 기술적 분야 중 산업 제어시스템 내 구성된 PC 및 서버의 운영체제, 네트워크 장비, 보안장비, 데이터베이스 등에 대해서도 평가를 수행할 수 있다. 그러나 취약점 분석·평가는 법에 의해 지정된 주요정보통신기반시설에 적용되므로, 산업 제어시스템 구성요소에 대한 보안성 평가와 신규 구축되었으나 주요정보통신기반시설로 지정되지 않은 산업 제어시스템에는 적용할 수 없다는 한계가 있다. 또한 취약점 분석·평가 기준의 제어시스템 분야 이외의 항목은 산업 제어시스템 적용을 고려하지 않고 개발되어 산업 제어시스템 적용 시 예기치 못한 상황이 발생할 수 있으므로 이를 고려하여 산업 제어시스템에 적합한 기준을 검토할 필요가 있다.

4.2 IoT 보안인증서비스

사물인터넷 제품 및 연동 모바일 앱에 대해 일정 수준의 보안을 갖추었는지 시험하여 기준 충족시 인증서를 발급해 주는 서비스로서, 인증대상은 IoT 기기 및 기기와 연동된 모바일 앱이다[28]. IoT 기기라 함은 계통적, 유기적으로 구성된 네트워크에 연결되어 감지, 제어, 중계, 촬영, 관리, 운행 등의 기능을 수행하는 기기를 총칭한다[28]. IoT 보안인증서비스의 시험·인증 기관은 한국인터넷진흥원에서 수행하며, 시험·인증 기준은 Standard와 Lite가 있다. Standard인 경우 인증(13개), 암호(3개), 데이터보호(8개), 플랫폼 보호(14개), 물리적보호(3개) 등 41개 보안 요구사항을 정의하고 있다[28]. IoT 보안인증서비스의 대상은 IoT 기기와 기기와 연동된 모바일 앱으로 한정하고 있어, 산업 제어시스템의 유선·무선 센서가 일부 포함이 될 수도 있으나, 산업 제어시스템의 임베디드 장치, 제어 애플리케이션 등은 고려되지 않는다. 따라서 산업 제어시스템 보안성 평가를 위해서 IoT 보안인증서비스를 이용하는 것은 적절하지 않을 것으로 판단된다.

4.3 보안적합성 검증제도

보안적합성 검증 제도는 국가정보통신망의 보안수준 제고를 목적으로 외부의 사이버 위협에 대응하기 위해 '전자정부법' 제56조 및 '공공기록물 관리에 관한 법률 시행령' 제5조에 의거 국가·공공기관에 도입되는 정보보호시스템에 대한 안전성을 검증하는 제도이다[33]. 침입차단시스템, 침입방지시스템 등 24종의 정보보호 제품에 대한 검증을 수행하고 있다. 산업 제어시스템 구성요소인 임베디드 장치, 제어 애플리케이션, 호스트 장치 등은 정보보호 제품이 아니고, IT 환경의 정보보호 제품과는 전혀 다른 특성으로 운영되는 OT 제품이라는 점을 고려할 때, 기존 보안적합성 검증 제도의 신규 검증 대상으로 반영하는 것은 적절하지 않다. 또한 보안적합성 검증제도는 국가·공공기관을 대상으로 하기 때문에 스마트공장과 같은 민간기관을 대상으로 적용하는 것은 적절하지 않다.

4.4 정보보호제품 평가·인증제도

정보보호제품 평가·인증제도는 '국가정보화 기본법' 제38조 및 동법 시행령 제35조에 의거 정보보호제품에 구현된 보안기능이 평가 신청한 평가보증등급 수준에 부합하는지 검증함으로써 사용자가 자신의 보안 욕구를 충족하는 IT 제품을 선택하는데 도움을 주기위한 제도이다[34]. 평가 대상은 보안기능이 있는 IT 제품으로써 정보보호 제품만을 대상으로 하고 있다. 따라서 산업 제어시스템 구성요소인 임베디드 장치, 제어 애플리케이션, 호스트 장치 등은 정보보호 제품이 아니고, IT 환경의 정보보호 제품과는 전혀 다른 특성으로 운영되는 OT 제품이라는 점을 고려할 때, 기존 정보보호제품 평가·인증제도의 신규 대상으로 반영하는 것은 적절하지 않다. 물론 프랑스의 CSPN 제도처럼 IT 보안제품 대상의 제도에 PLC를 추가한

사례도 있지만, 대부분의 산업 제어시스템 보안성 평가 제도는 OT 분야의 전문성을 고려하여 별도의 제도로 운영되고 있다.

Ⅴ. 국내 산업 제어시스템 보안성 평가 방안

본 장에서는 4차 산업혁명이 가속화되고 스마트공장 보급이 확대됨에 따라 공개 기술, 상용 기술, 무선 통신기술을 활용하여 다른 네트워크와 연결되는 스마트공장의 사이버 보안위협에 대응하기 위한 하나의 방안으로써, 산업 제어시스템의 보안성을 평가하는 방안을 제안한다. 산업 제어시스템은 산업설비의 가용성을 우선적으로 고려해야 하므로, 선 구축 후 보안기술 도입의 일반적인 IT 보안전략과는 다르게 접근해야 한다. 산업 제어시스템의 구성요소를 설계 및 개발하는 단계부터 가용성과 보안성을 고려하고, 산업 제어시스템의 운용 이전에 충분한 가용성을 확보하면서도 보안관리가 가능한 수준으로 구축되었는지를 평가함으로써, 운용 단계에서 충분한 보안관리가 가능하도록 해야 한다. 이를 위해서 국내 산업 제어시스템 보안성 평가를 위해서 국내 기존 제도 활용 방안과 국외 기존 제도 활용 방안을 검토하고, 산업 제어시스템 보안성 평가를 위해 별도의 국내 제도 마련이 필요함을 설명한다.

5.1 국내 기존 제도 활용 방안

주요정보통신기반시설 취약점 분석·평가 제도는 공공·민간 영역의 주요정보통신기반시설에 적용되는 제도로써, 스마트공장과 같은 일반 산업시설에 제도적으로 적용할 수는 없다. 그러나 주요정보통신기반시설 취약점 분석·평가 기준을 신규 구축된 산업 제어시스템에 대한 보안성 평가의 기준으로 고려할 수는 있다. 하지만, PLC, DCS 컨트롤러, 제어 애플리케이션과 같은 OT 시스템에 대한 평가 기준이 매우 제한적이어서 활용에는 한계가 있다.

IoT 보안인증서비스는 산업 제어시스템의 유선·무선 센서의 인증에 활용할 수도 있으나, 산업 제어시스템의 임베디드 장치, 제어 애플리케이션 등 대다수의 구성요소와 제어시스템은 적용할 수 없다.

보안적합성 검증제도는 국가·공공기관에 도입되는 IT 환경의 정보보호 제품이 대상이므로, 스마트공장과같은 민간 산업시설의 OT 제품의 보안성 평가 제도로 활용하기에는 부적절하다.

정보보호제품 평가·인증제도는 공공·민간을 구분하지 않으나 IT 정보보호 제품만을 대상으로 하기 때문에 산업 제어시스템의 OT 제품에 대한 보안성 평가 제도로 활용하기에 부적절하다.

5.2 국외 기존 제도 활용 방안

국외 기존 제도의 활용 방안은 산업 제어시스템 구성요소에 대한 보안성 평가 방안으로써만 검토한다. 산업 제어시스템의 운용환경이 망분리, 보안체계 등으로 국내·외 차이가 있으며, 국내 중요 산업 제어시스템에 대한 정보 유출을 보호하기 위함이다.

구성요소에 대한 국외 제도로는 ACC, EDSA, SSA, eSDC, eSSC, CAP for ICS, IECEE PCA가 있다. ACC는 네트워크 견고성 시험만 수행하므로 기능에 대한 보안성 평가가 부족하지만, 나머지 제도의 인증 받은 제품은 국내에서 그대로 도입하여 활용이 가능하다. 그러나 이 경우 산업설비에 대한 외산제품 종속성에 더해 산업 제어시스템 보안 시험·평가에 있어서도 종속될 수 있으며, 우리나라 기업이 시험·평가를 해외에서 받아야 하는 문제와 시험·평가 비용을 고려할 때, 산업 제어시스템 구성요소에 대한 보안성 평가는 국외의 기존 제도와 호환성을 갖는 방향으로 국내 제도의 운영이 필요할 것으로 판단된다.

5.3 제안하는 산업 제어시스템 보안성 평가 방안

산업 제어시스템에 대한 보안성 평가는 1절과 2절에서 기존 제도 활용을 검토한 결과 국내 산업 제어시스템 보안 시험·평가 기술의 확보와 국내 기존 제도 중 활용할 수 있는 적절한 제도가 없다는 것이 분석되었다. 이에 따라 본 절에서는 국내 스마트공장에 적용할 수 있는 산업 제어시스템 보안성 평가 방안을 제시한다.

5.3.1 고려사항

국내 스마트공장 대상의 산업 제어시스템 보안성 평가 방안 마련을 위해서 고려해야 할 사항은 다음과 같다.

첫째, 대부분 글로벌 기업에 의존하고 있는 산업 제어시스템 구성요소 시장 환경을 고려하여야 한다. 표 5는 시장조사기관인 Markets&Markets에서 조사한 산업제어 및 공장자동화 분야[29], 프로세스 자동화 분야[30], IIoT 기기 분야[31]별 Top5 제조사이며, 기타 주도 기업은 해당 분야의 Top5 이후의 주요 기업을 열거하였다. 표 5와 같이 국내 제조사는 전무한 실정이며, 2017년 중소기업기술로드맵의 스마트공장 분야 기술동향 분석에서도 핵심요소 대부분을 독일, 일본, 미국으로부터 수입해야 한다[32]고 설명하고 있다.

표 5. 산업 제어시스템 분야별 Top5 제조사
Table 5. Top 5 Manufacturers in ICS Domain

Ranking	Industrial Control and Factory Automation (2015)[29]	Process Automation & Instrumentation (2014)[30]	Industrial IoT (2015)[31]
1	Siemens AG	ABB	GE
2	ABB	Emerson Electric Company	Cisco Systems
3	Emerson Electric Company	Honeywell International	Intel
4	Mitsubishi Electric Corp.	Siemens AG	ARM
5	Schneider Electric SE	Rockwell Automation	Rockwell Automation
Other Leading Companies	①GE, ②Mitsubishi Electric, ③Yokogawa Electric, ④Honeywell International	①Endless+Hauser AG, ②HollySys Automation Technologies, ③Mitsubishi Electric, ④Pepperl+Fuchs, ⑤R. STAHL AG, ⑥Schneider Electric, ⑦Yokogawa Electric	①ABB, ②Texas Instruments, ③Dassault Systèmes, ④Honeywell International, ⑤Huawei Technologies, ⑥IBM, ⑦Kuka AG, ⑧NEC, ⑨Robert Bosch, ⑩Siemens AG, ⑪ZIH Corp

둘째, 산업 제어시스템 보안성 평가를 위한 분야와 대상을 선정해야 한다. 보안성 평가 분야와 대상은 표 6과 같이 구분할 수 있으며, 모든 분야의 모든 대상에 대해서 평가할지, 일부 분야의 일부 대상에 대해서 평가할지를 국내 환경을 고려하여 결정해야 한다.

셋째, 산업 제어시스템 보안성 평가를 위한 기준을 선정해야 한다. 보안성 평가 기준은 Ⅲ장에서 설명한 것처럼 IEC 62443, UL 2900-2-2, 시험기관별 자체 기준 등이 있다. 보안성 평가 기준 선정 시 국내 산업 제어시스템 시장 환경과 글로벌 무역규제 환경 등을 검토해서 결정해야 한다.

넷째, 산업 제어시스템 보안성 평가를 운영하는 체계를 마련해야 한다. 운영 체계는 평가를 요구하는 주체, 평가를 신청하는 주체, 평가를 실시하는 주체가 식별되어야 한다. 그리고 산업 제어시스템 보안성 평가 체계를 마련하기 위한 제도 등 근거도 마련되어야 한다.

표 6. 보안성 평가 분야 및 대상
Table 6. Cybersecurity Assessment Types and Targets

Type / Target	Functional Security	Security Management Process
Manufacturer	Product System	Security Development Life Cycle
SI or Maintenance	Solution	Cyber security management System for SI or Maintenance
Asset Owner	-	Cyber security management System for Asset Owner

5.3.2 제안하는 산업 제어시스템 보안성 평가 방안

본 항은 가항의 고려사항을 반영한 국내 환경에 적합한 산업 제어시스템 보안성 평가 방안을 제안한다.

1) 평가 분야와 대상 선정

국내 산업 제어시스템은 표 5와 같이 해외 제조사의 구성요소를 수입하여 구축하고, 일부 구성요소는 국내 제조사의 것을 활용하는 환경이다. 즉, 구성요소 제조사 대부분이 글로벌 대기업이다. 따라서 제조사에 대한 평가는 제품 및 시스템에 대한 블랙박스 시험 중심의 보안기능 평가가 현실적이다. 글로벌 제조사의 개발 보안관리 프로세스를 평가하기 위해서는 관련 문서의 제출과 현장심사가 필요하지만, 영업비밀 등을 이유로 이에 대한 협조가 어려운 실정이므로 추후 검토가 필요하다.

국내 산업 제어시스템 통합구축(SI) 사업에도 이들 글로벌 대기업이 많이 참여 하고 있다. 따라서 SI 및 유지보수 회사를 대상으로 한 보안성 평가 역시 제조사 평가와 동일한 이유로 시스템 통합 사업의 결과로 구축된 산업 제어시스템 솔루션에 대한 블랙박스 시험 형태의 보안기능 평가를 우선 추진할 것을 제안한다.

운영기관에 대한 보안평가는 운용측면의 보안관리 프로세스에 대한 평가를 수행할 수 있다. 다만 신규 구축 산업 제어시스템에 대한 보안성 평가의 참여자 및 사업자는 반드시 비밀유지계약을 체결하여 운영기관의 산업 제어시스템 관련 정보가 노출되지 않도록 해야 한다.

요약하면, 우선적으로 제조사의 제품 및 시스템 평가, SI 및 유지보수 회사의 솔루션 평가, 운영기관의 운용 측면의 보안관리 프로세스 평가를 우선적으로 실시하고, 글로벌 제조사의 협조를 이끌어내어 나머지 부분에 대한 보안성 평가를 수행하는 방향으로 진행할 것을 제안한다.

2) 평가 기준 선정

산업 제어시스템 제품, 시스템, 솔루션에 대한 보안성을 평가하는 기준은 표 7과 같이 IEC 62443 표준, UL 2900-2-2 표준, 시험기관별 자체 기준으로 분류된다. 대부분 IEC 62443 표준을 적용하고, UL CAP

for ICS는 UL 표준, ACC 인증과 CSPN 인증은 자체 기준을 적용하고 있다. 표 7과 같이 산업 제어시스템 보안성 평가·인증의 기준은 IEC 62443 표준을 중심으로 추진되고 있고, 국내 산업 제어시스템 구성요소의 공급사가 주로 글로벌 제조사임을 고려하면 국제적인 평가 기준을 적용하는 것이 향후 무역기술장벽 논란도 피할 수 있을 것으로 예상된다. 또한 국내 제조사도 국제적인 평가 기준에 따라 제조함으로써 필요시 국제적인 산업 제어시스템 보안성 평가를 받아 수출하는 것이 용이하고 국제 경쟁력 강화에도 도움이 될 수 있다. 산업 제어시스템 구성요소에 대한 보안성 평가에는 가용성 시험을 반영하는 경우도 있다. ACC는 퍼징, 스트레스 시험 등의 네트워크 견고성 시험이 있으며, ISASecure EDSA, SSA 인증도 퍼징, 스트레스 시험, 취약점 식별 시험을 포함하고 있다. TÜV SÜD도 별도의 산업 IT 보안 시험소를 설립하여 Achilles Test Platform을 이용한 네트워크 견고성 시험을 수행하며, UL CAP for IEC 62443 인증도 퍼징, 침투 테스트, 취약점 분석, 소스코드 분석 등의 시험을 수행한다. 따라서 구성요소에 대한 보안성 평가 기준으로 국제표준인 IEC 62443을 이용하더라도 퍼징, 스트레스 시험, 취약점 분석, 침투 테스트 등의 추가적인 시험의 반영도 고려할 필요가 있다. 또한 국내 산업 제어시스템 환경과 관련 법·규정 등에서 요구하는 보안기능(에, 패스워드 사용규칙, 보안 알고리즘 적용, 원격 보안관리 제한 등)에 대한 시험의 반영도 고려할 수 있다.

다음으로 산업 제어시스템을 소유한 운영기관의 보안관리 프로세스에 대한 평가기준으로는 표 7에 제시된 정보관리시스템인증센터에서 운영하는 CSMS 프로그램의 IEC 62443-2-1 기준이 유일하다. 그러나 산업 제어시스템이 운영되는 환경은 각 국가가 처한 현실과 각 국가별 규제준수 사항 등이 차이가 있기 때문에, 운영기관의 보안관리 프로세스를 평가하기 위한 기준으로는 IEC 62443-2-1 기준, 주요정보통신기반시설 취약점 분석·평가 기준을 포함하여 국내 환경을 고려한 자체 기준을 마련하여 적용하는 것이 적절할 것으로 판단된다.

3) 평가 체계 마련

산업 제어시스템 보안성 평가 제도 중 CSPN 제도와 CSMS 제도만 국가에서 참여하고, 그 이외에는 민간에서 자율적으로 운영되고 있다. 민간기업인 GE, 민간 시험기관인 TÜV SÜD, exida, 표준화 기구인 ISA의 ISCI, UL, IEC의 IECEE에서 산업 제어시스템 보안성 평가·인증제도를 운영하고 있다. 따라서 국내에서도 민간 자생적으로 이러한 제도가 운영될 수 있는 체계를 마련하는 것이 필요하다. 시험기관은 한국인정기구로부터 IEC 62443 표준에 따른 시험기관 인정을 받아 산업 제어시스템 구성요소에 대한 인증제도를 운영(그림 2의 ①, ②, ③) 한다. 스마트공장 자산 소유자인 운영기관이 산업 제어시스템 구성요소 도입과 관련하여 보안성 평가를 요구(그림 2의 ④, ⑤)하고, 제조사는 이러한 요구에 부응하도록 제품을 개발하여 사전에 시험기관으로부터 평가를 받아서 납품(그림 2의 ②, ③, ⑥)하도록 한다. 이를 통해 보안성 평가 요구가 증가하고, 자연적으로 시험하는 기관들이 증가함으로써 시험기관의 시험기술이 향상되어 더욱 보안성이 강화된 산업 제어시스템이 구축되게 된다.

다음으로 산업 제어시스템을 소유한 운영기관의 보안관리 프로세스에 대한 평가체계이다. 산업 제어시스템은 가동 후에는 가용성에 대한 우려로 보안성을 평가하기 어려운 경우가 많다. 이는 보안성 평가가 구축된 산업 제어시스템에 어떠한 영향을 미치는지 확인이 되지 않았기 때문이다. 따라서 산업 제어시스템을 신규 구축하는 과정에서 공장인수시험이나 현장인수시험 등에서 기술적 보안성 평가를 수행(그림 2의 ⑧, ⑨) 하여 가용성에 미치는 영향을 분석하고 취약한 부분을 보강(그림 2의 ⑩)함으로써, 구축된 시스템 자체의 보안성을 강화하고, 시간의 경과에 따라 발생하는 취약 상황을 운용 중에도 보완할 수 있는 가용성을 확보해야 한다. 보안성 평가는 운영기관이 자체적으로 평가반을 구성하여 보안관리 상태를 평가하거나, 관련 분야에 전문성을 보유한 정보보호 전문 서비스기업을 활용하는 방안이 있다.

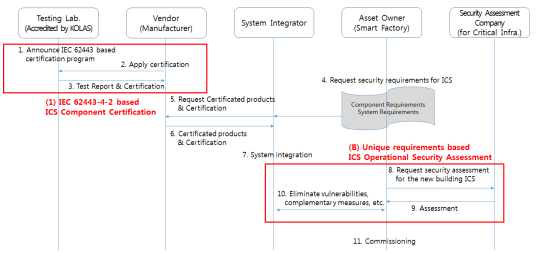

그림 2. 평가 절차
Fig. 2. Evaluation Procedure

표 7. 산업 제어시스템 보안성 인증 제도와 대상 및 기준 비교
Table 7. Comparison of ICS Cybersecurity Certification Programs, Targets, and Requirements

Certification \ Target			Manufacturer			SI/Maintenance Company		Asset Owner
			Security Development Life Cycle	Component[1]	System[2]	CSMS for SI/Maintenance Company	Solution[3]	CSMS for Asset Owner
GE Achilles	ACC			Proprietary Requirement				
	APC					IEC 62443-2-4 (WIB)		
ISCI	ISASecure EDSA			IEC 62443-4-1 62443-4-2				
	ISASecure SSA				IEC 62443-4-1 62443-3-3			
	ISASecure SDLA		IEC 62443-4-1					
TÜV SÜD	Certification for System Integrator					IEC 62443-2-4 62443-3-3		
	Certification for Manufacturer		IEC 62443-4-1 62443-3-3					
exida	Cybersecurity Engineering Process Certifications		IEC 62443-4-1			IEC 62443-2-4		
	Cybersecurity Device and Application Certifications			IEC 62443-4-1 62443-4-2				
	Cybersecurity System Certifications				IEC 62443-4-1 62443-4-2		IEC 62443-2-4 62443-3-3	
	Cybersecurity Personnel Certification							
UL	CAP for ICS			UL 2900-2-2				
IECEE	Industrial Cybersecurity Certifications	Product Capability Assessment		IEC 62443-4-2	IEC 62443-3-3		IEC 62443-2-4	
		Process Capability Assessment	IEC 62443-4-1			IEC 62443-2-4		
		Product Application of Capability Assessment	IEC 62443-4-1					
		Process Application of Capability Assessment				IEC 62443-2-4		
	UL	CAP for IEC 62443	Same as IECEE Industrial Cybersecurity Certifications					
	DEKRA	IEC 62443	Same as IECEE Industrial Cybersecurity Certifications					
	TÜV NORD	IEC 62443-2-4	Same as IECEE Industrial Cybersecurity Certifications					
France ANSSI	CSPN			Unique Requirement				
Japan ISMS-AC	CSMS							IEC 62443-2-1
Proposed Method				IEC 62443-4-2	IEC 62443-4-2		Proprietary Requirement	Proprietary Requirement

1) 컴포넌트는 단일 제어시스템 구성품
2) 시스템은 단일 제조사에서 2개 이상의 컴포넌트로 구성된 단일 제품(컴포넌트는 제조사가 다를 수 있음)
3) 솔루션은 Basic Process Control System, Safety Instrumented System과 같이 특정 프로세스를 제어하는 제어 솔루션(예: 터빈, 보일러 제어시스템 등)

Ⅵ. 결 론

4차 산업혁명으로 확산되고 있는 스마트공장의 현장 자동화 분야에 사용되는 산업 제어시스템은 전통적인 전용 운영체제, 비공개 통신기술, 폐쇄망 운영에서 상용 운영체제, 이더넷 및 무선 통신 기술의 활용, 다른 네트워크와 연결되는 구조로 변화하고 있다. 본 논문은 이러한 변화로 증가되고 있는 사이버 보안위협에 대응하기 위한 하나의 방안으로써 산업 제어시스템 보안성 평가 방안을 제안하였다.

국내 산업 제어시스템 시장 환경을 고려하여 설계자료나 소스코드 등을 검토해야 하는 개발 보안관리 프로세스나 SI 보안관리 프로세스에 대해서는 평가 우선순위를 미루었다. 제조된 제품 및 시스템에 대해 IEC 62443-4-2 국제표준을 기반으로 평가하고, 신규 구축된 솔루션과 운영기관의 보안관리 프로세스에 대해서는 국내 환경과 규제준수 사항 등을 고려한 자체 기준 기반의 보안성 평가를 제안하였다. 본 보안성 평가 방안은 국내 산업 제어시스템의 구축 및 운용환경, 보안성 평가의 국제 동향, 국내 보안 고려사항 등의 특성을 고려하여 가장 현실적이고 빠르게 적용할 수 있는 방안으로 제시하였다. 또한 산업 제어시스템이 가동 후에 발생하는 가용성 문제에 대응하기 위하여 신규 구축 후 가동전에 솔루션에 대해 평가할 것을 제안하였다. 이를 통해 제조사가 구성요소의 설계 및 개발 단계에서 보안을 고려하도록 하고, 운용단계에서 사이버보안 관련 대책을 적용할 수 있는 가용성을 사전에 확보할 수 있다.

향후 연구로는 산업 제어시스템 보안성 평가・제도의 상당수가 평가 항목으로 반영하고 있는 네트워크 견고성 시험 방안에 대한 연구 수행이 필요하다. 또한 신규 구축된 산업 제어시스템에 대한 운영기관의 보안관리 프로세스 평가에 필요한 자체 기준 연구도 필요하다.

References

[1] S. K. Cha, J. Y. Yoon, J. K. Hong, H. G. Kang, and H. C. Cho, "The system architecture and standardization of production IT convergence for smart factory," *J. Korean Soc. Precis. Eng.*, vol. 32, no. 1, pp. 17-24, Jan. 2015.

[2] S. Heo, G. Lee, D. Kim, and H. Kim, "Industrial control system security technologies for enhancing smart factory security," *Rev. KIISC*, vol. 27, no. 2, pp. 29-33, Apr. 2017.

[3] *Korea Smart Factory Foundation form*, https://www.smart-factory.kr/.

[4] D. H. Byun, "Trend of smart factory and model factory cases," *The e-Business Stud.*, vol. 17, no. 4, pp. 211-228, Aug. 2016.

[5] J. Cho, "The 4th Industrial Revolution and GE," *J. KSME*, vol. 58, no. 5, pp. 25-29, May 2018.

[6] K. Stouffer, J. Falco, and K. Scarfone, *Guide to industrial control systems (ICS) security*, NIST SP 800-82 Revision 2, May 2015.

[7] Positive Technologies, *ICS Security: 2017 In Review*, Jan. 2018 from https://www.ptsecurity.com/ww-en/analytics/ics-security-2017/.

[8] FireEye iSight Intelligence, *Overload Critical Lessons From 15 Years of ICS Vulnerabilities*, Aug. 2016. from https://www.fireeye.com/blog/threat-research/2016/08/overload-critical-lessons-from-15-years-of-ics-vulnerabilities.html.

[9] SANS ICS and E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, Mar. 2016 from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_t.pdf.

[10] Dragos, *CrashOverride: Analysis of the Threat to Electric Grid Operations*, Jun. 2017 from https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[11] F. Xie, Y. Peng, W. Zhao, Y. Gao, and X. Han, "Evaluating industrial control devices security: Standards, technologies and challenges," *IFIP Int. Conf. Comput. Inf. Syst. and Indu. Management, LNCS*, vol. 8838, pp. 624-635, 2015.

[12] *ISASecure* from https://www.isasecure.org/en-US.

[13] *TUV SUD Homepage* from https://www.tuev-sued-de/topics/information-technology-it/industrial-it-security.

[14] *exida for IEC 62443 Cyber Certification* from http://www.exida.com/Certification/ IEC62443-Cyber-Cert, 2019.

[15] *IECEE CB Scheme* from https://www.iecee.org

/about/cb-scheme, 2019.

[16] CMC TF Cyber Security, *OD-2061 IECEE System – Industrial Cyber Security Program*, Edition 1.1, Jun. 2018.

[17] UL, *Cybersecurity for Industrial Automation and Control Systems*(IACS) from https://industries.ul.com/industrial-systems-and-components/cybersecurity-for-industrial-control-systems-ics.

[18] UL, *Online Certifications Directory* from http://database.ul.com/cgi-bin/XYV/template/LISEXT/1FRAME/index.htm.

[19] UL, *Accelerate your cyber readiness with IEC 62443* from https://industries.ul.com/wp-content/uploads/sites/2/2017/04/ULCyber62443_133.01.0317.EN_.EPT_.pdf.

[20] ANSSI, *Certification CSPN* from https://www.ssi.gouv.fr/administration/produits-certifies/cspn/.

[21] JIPDEC, *Cyber Security Management System Conformity Assessment Scheme for the CSMS Certification Criteria*(IEC 62443-2-1:2010) from https://isms.jp/csms/doc/JIP-CSMS120E-10.pdf.

[22] K. H. Son, "Industrial control system security evaluation and certification trend analysis," *Rev. KIISC*, vol. 24, no. 5, Oct. 2014.

[23] DEKRA Homepage, Cyber Security Testing & Certification, from https://www.dekra-product-safety.com/en/programs./cyber-security.

[24] TUEV NORD Service GmbH Homepage, *Certification according to IEC 62443* from https://www.tuev-nord.de/en/company/certification/product-certification/functional-safety/certification-according-to-iec-62443/.

[25] ASCI, *EDSA-100 ISA Security Compliance Institute – Embedded Device Security Assurance – ISASecure certification scheme* Version 3.7, Oct. 2018.

[26] MSIT, *Information and Communication Infrastructure Protection Act* from https://www.law.go.kr/법령/정보통신기반보호법/.

[27] MSIT, *Critical Information and Communication Infrastructure Vulnerability Analysis and Assessment Criteria* from https://www.law.go.kr/행정규칙/주요정보통신기반시설취약점분석・평가기준/.

[28] KISA, *IoT Security Test and Certification Requirement*, Dec. 2017. from https://www.kisis.or.kr/kisis/ subIndex/307.do.

[29] MarketsAndMarkets, *Industrial Control And Factory Automation Market* – Global Forecast to 2022, Sep. 2016.

[30] MarketsAndMarkets, *Process Automation & Instrumentation Market* – Global Forecast to 2020, 2016.

[31] MarketsAndMarkets, *Industrial IOT Market* – Global Forecast to 2022, Feb. 2017.

[32] MSS, TIPA, NICE Information Service, "*SME Technology Roadmap 2018-2020 – Smart Factory*," pp. 32-37, 2017. from http://smroadmap.smtech.go.kr/download.2017_09.pdf.

[33] *Security Conformance Verification* from https://www.nis.go.kr

[33] *ITSCC* from http://itscc.kr/

김 우 년 (Woonyon Kim)

1996년 2월 : 안동대학교 컴퓨터공학과 졸업

1998년 2월 : 경북대학교 컴퓨터과학과 석사

2000년 2월 : 경북대학교 컴퓨터과학과 박사수료

2000년 3월~2003년 12월 : ㈜ 니츠 선임연구원

2003년 12월~현재 : ETRI 부설연구소 책임연구원

<관심분야> 기반시설보안, ICS/CPS/IIoT 보안, ICS 보안성/안전성 평가

[ORCID:0000-0002-3580-4231]

박 응 기 (Eung-Ki Park)
1986년 2월 : 중앙대학교 전자계산학과 졸업
1988년 2월 : 중앙대학교 전자계산학과 석사
2005년 8월 : 아주대학교 컴퓨터공학과 박사
1988년 2월~2000년 1월 : ETRI 선임연구원
2000년 1월~2000년 4월 : ETRI 부설연구소 책임연구원
2000년 4월~2002년 11월 : ㈜니츠 기술이사
2002년 11월~현재 : ETRI 부설연구소 책임연구원
<관심분야> 기반시설보안, ICS/CPS/IIoT 보안, ICS 보안성/안전성 평가, 사이버보안
[ORCID:0000-0003-1623-3012]

김 신 규 (Sin-Kyu Kim)
2000년 2월 : 연세대학교 기계전자공학부 졸업
2002년 2월 : 연세대학교 컴퓨터과학과 석사
2014년 2월 : 연세대학교 컴퓨터과학과 박사
2003년 12월~현재 : ETRI 부설연구소 선임연구원/팀장
<관심분야> 기반시설보안, 스마트그리드 보안, 취약점 분석, CPS 보안
[ORCID:0000-0002-7798-6344]