정 보 보 호 학 회 지
제29권 제2호, 2019. 4

산업 제어시스템 보안성 평가제도 동향

김 우 년*, 박 응 기*, 김 신 규*, 지 윤 석**

요 약

산업 제어시스템 보안 취약점 발견의 증가, 사이버보안 사고로 인한 정전과 같은 물리적 피해 발생, 4차 산업혁명으로 확산되는 스마트공장 및 스마트시트의 산업 제어시스템 네트워크 연계 증가 등으로 인해 산업 제어시스템에 대한 보안위협이 급증하고 있으며, 이에 대한 보안대책이 요구되고 있다. 본 논문에서는 산업 제어시스템 구성요소에 대한 보안 내재화를 유도하고, 산업 제어시스템의 도입, 운영, 유지보수 과정에서 사이버보안을 고려할 것을 요구하는 산업 제어시스템 보안성 평가제도의 동향에 대해서 설명한다. 구체적으로는 미국, 일본, 프랑스 등의 국가기관, ISA, IEC, UL 등과 같은 국제 표준화 기구, TÜV SÜD, exida와 같은 글로벌 시험기관, GE와 같은 제조사에서 실시하고 있는 산업 제어시스템 보안성 평가제도를 설명하고, 평가제도를 분류하여 특성을 파악할 수 있도록 제시하였다.

Ⅰ. 서 론

산업 제어시스템은 발전, 가스생산, 석유화학, 상수도 등의 에너지 생산 시설이나 전력 송변전 및 배전, 가스・석유・난방열 등의 공급 시설, 반도체, 자동차 등의 산업 생산 시설을 제어 및 모니터링 하는 시스템이다. NIST 800-82에 따르면 산업 제어시스템은 산업 설비의 변수가 사전 정의된 값을 달성하도록 가이드하고 다루는 시스템인 제어시스템의 여러 유형을 포괄하는 일반적인 용어로 정의하고 있으며, 유형에는 SCADA(Supervisory Control and Data Acquisition), DCS(Distributed Control Systems), PLC(Programmable Logic Controllers) 등이 포함된다. 이들 제어시스템은 제어기기(Controller)가 물리적 장치에 부착된 센서로부터 정보를 획득하여, 제어기기내의 제어로직에 따라 획득한 정보를 처리하고, 필요한 경우 물리적인 현장장치인 구동기(Actuator)를 동작시켜 산업 공정을 실행하며, 이러한 산업 공정은 HMI(Human-Machine Interface)를 통해 운전자에게 물리적 장치의 현황을 제공하고 필요시 운전자의 개입으로 산업 공정이 조정된다[1].

이와 같이 산업 제어시스템은 물리적인 장치를 직접 다루기 때문에 IT 시스템에 비해 더 높은 실시간성이 요구되고, 무중단 운영으로 시스템의 재시작이 어려운 경우가 있어 가용성이 기밀성 및 무결성보다 우선시 되며, 사람의 생명과 건강, 환경을 최우선으로 고려한다. 또한 한번 설치되면 10년~15년 이상 장기적으로 활용되며, 정해진 예방 점검 일정 계획에 따라 유지보수가 수행된다[1].

산업 제어시스템에 대한 보안취약점 발견의 증가, 산업 제어시스템 사이버보안 사고로 인한 정전과 같은 물리적 피해 발생, 4차 산업혁명을 계기로 확산되고 있는 스마트공장과 스마티시티의 산업 제어시스템이 네트워크에 연결되고 있으며, 이로 인해 보안위협이 증가하고 있어 산업 제어시스템에 대한 보안의 필요성이 증가하고 있다. 2003년부터 미국을 중심으로 산업 제어시스템에 대한 보안성 평가가 실시된 이래 일본, 프랑스 등의 국가기관이 주도하는 산업 제어시스템 보안성 평가제도 뿐만 아니라, 표준화 단체, 글로벌 시험기관, 제조사에서 실시하는 다양한 제도들이 운영 중이다. 따라서 본 논문에서는 산업 제어시스템 대상의 보안성 평가제도를 설명하고, 그 특징을 분석하고자 한다. 이를 통해 국내 산업 제어시스템 관련 제조사는 자사의 구성요소에 대한 보안성 평가기준을 설계에 반영하여 보안성이 향상된 제품을 개발하는데 활용하고, 국내 시험기관은 글로벌 시험기관과의 협력을 통해 관련 시험기술을 확보하

* ETRI 부설연구소 (wnkim@nsr.re.kr, ekpark@nsr.re.kr, skkim@nsr.re.kr)
** 숭실대학교 IT정책경영학과 박사과정 (youjun311@naver.com)

는데 활용하며, 국내 운영기관은 산업 제어시스템을 구축하는 단계에서부터 보안 요구사항을 반영하는데 활용할 수 있도록 하고자 한다.

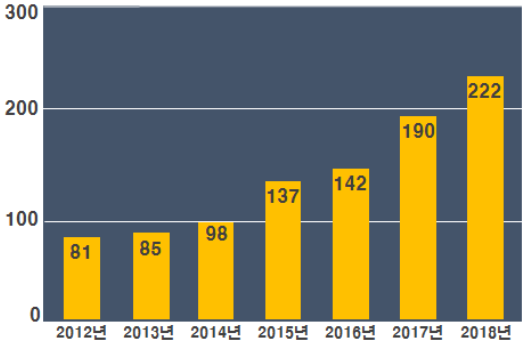
본 논문은 총 5장으로 구성되며, Ⅱ장에서는 산업 제어시스템에 대한 보안위협 설명을 통해 산업 제어시스템에 대한 보안성 평가제도의 필요성을 제시하고, Ⅲ장에서는 주요한 산업 제어시스템 보안성 평가제도를 상세하게 설명한다. Ⅳ장에서는 Ⅲ장에서 설명한 산업 제어시스템 보안성 평가제도를 여러 특징에 따라 분류하여 평가제도의 주요한 흐름을 살펴보고, 마지막 Ⅴ장에서 결론을 맺는다.

Ⅱ. 산업 제어시스템 보안성 평가의 필요성

산업 제어시스템에 대한 취약점은 사이버보안 및 기반시설 보안청(CISA, The Cybersecurity and Infrastructure Security Agency) 산하의 NCCIC(National Cybersecurity and Communications Integration Center)에서 발표하고 있으며, 2012년 81건에서 2018년 222건으로 지속적으로 증가추세에 있다. NCCIC에는 2017년까지 산업 제어시스템 보안 취약점을 발표하던 ICS-CERT(Industrial Control System - Cyber Emergency Response Team)가 통합되어 있다.

또한 산업 제어시스템에 대한 사이버 사고는 2000년 이래로 지속적으로 발생하고 있으며, 그 주요한 사고는 표 1과 같다.

이와 같이 증가하는 산업 제어시스템 보안위협에 대응하기 위해서는 산업 제어시스템 자체에 보안이 내재되어야 하고, 보안이 고려된 산업 제어시스템이 구축되어야 하며, 운영 및 유지보수 동안에도 산업 제어시스템 보안 프로그램에 의해 관리 되어야 한다. 이를 위해서 다양한 산업 제어시스템 보안관련 표준이 마련되고, 각 국가에서는 사이버보안 규제기준이 마련되고 있으며, 이를 기반으로 한 산업 제어시스템 보안성 평가제도가 실시되고 있다.



〔그림 1〕 CISA의 ICS-CERT Advisories 연도별 발표 건수

〔표 1〕 산업 제어시스템 사이버 사고 주요 현황

연도	사건 명칭	분야
2000.4	호주 Maroochy Shire 폐수 방류 사고	상하수도
2003.1	미국 Davis-Besse 원전 Slammer 웜 감염	원자력
2009.4	미국 전력망에서 중·러 악성코드 발견	전력
2010.6	이란, 우라늄재처리 공장 해킹으로 물리적 피해(Stuxnet)	원자력
2011.2	Night Dragon APT 공격	에너지시설 (업무망)
2011.11	일리노이 상수도 공급 제어시스템 해킹	상하수도
2014.1	몬주 원전, USB를 통한 악성코드 감염	원자력
2014	독일 제철소 제어시스템 해킹	제조시설
2015.12	우크라이나 배전제어시스템 해킹으로 정전 (BlackEnergy 3)	전력
2016.4	독일 그룬밍햄 원전 악성코드 감염	원자력
2016.12	우크라이나 배전제어시스템 해킹으로 정전 (Industroyer/CrashOverride)	전력
2017.11	안전계장시스템 악성코드 감염 (Triton/Trisis)	제조시설

Ⅲ. 산업 제어시스템 보안성 평가제도

본 장에서는 과거 추진되었거나 현재 시행중인 산업 제어시스템 대상의 보안성 평가제도에 대해서 설명한다.

3.1. 미국 에너지부의 NSTB 프로그램

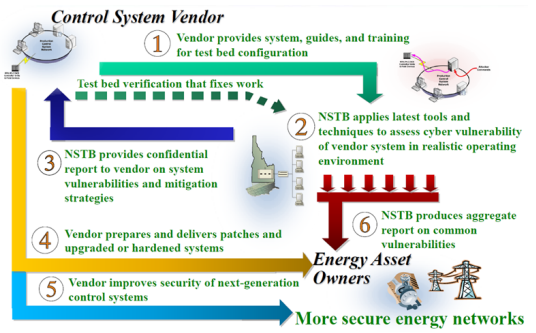
미국 에너지부는 2003년부터 아이다호 국립 연구소(INL)를 포함한 7개 국립 연구소에 SCADA 테스트베드를 구축하여, 미국의 에너지 기반시설이 직면한 보안 취약점과 보안위협을 발견하여 해소하기 위한 전문가 연구, 개발, 분석, 교육을 실시하는 국가 SCADA 테스트베드(NSTB, National SCADA Test Bed) 프로그램

〔표 2〕 NSTB 취약점 분석 평가 대상 중 일부[4]

연도	2009	2010
구성요소 (실험실 평가)	- ICCP Protocols - SCADA/EMS ICCP APIs(3) - Communications Authentication Devices - 3rd Party Products for SCADA/EMS	
시스템 (실험실 평가)	- ABB Network manager(4) - AREVA e-terra(3) - Siemens Spectrum Pwr3(1) - Siemens TG(1) - Telvent(2), -OSI(1)	- Siemens TG SCADA/EMS
현장평가	- Transmission Control Centers - Generation Control Centers - SCADA and DCS Installations - Substation Automation	- Oil Transmission System

을 추진하였다[2]. NSTB 프로그램 중 제어시스템에 대한 사이버 취약점 분석·평가는 아이다호 국립연구소에서 주로 수행하였으며, 2011년까지 제조사 구성요소 14개와 제조사 시스템 15개에 대한 실험실 평가, 그리고 8개 시설에 대한 현장평가 등 총 37개 제품 및 시설에 대한 사이버 취약점 평가를 실시하였으며, 일부는 표 2와 같다[3,4].

아이다호 국립연구소의 제어시스템 취약점 분석·평가 절차는 그림 2와 같이 진행되며, 분석 내용의 민감성으로 인해 비공개 협약을 체결하고, 제어시스템과 사이버보안 전문가의 상호 협력을 위해 R&D 협력 협약을 체결 후 진행된다[3]. 분석된 취약점은 제조사에 제공하여 취약점을 패치 할 수 있도록 하고, 운영기관에도 제공하여 발견된 취약점에 대한 보완대책을 수립하도록 하였다.



〔그림 2〕 INL의 제어시스템 취약점 분석·평가 절차[4]

3.2. 미국 국토안보부의 CSSP 프로그램 및 NCCIC 현장평가 프로그램

미국 국토안보부(DHS)는 2004년부터 제어시스템 보안 프로그램(CSSP, Control System Security Program)을 통해 국토안보관련 제어시스템에 대한 취약점 분석·평가를 수행하였으며, 2009년부터는 ICS-CERT에서 다양한 현장평가 프로그램을 운영하였다. ICS-CERT는 2017년 NCCIC에 통합되었고, 2018년부터는 NCCIC가 CISA에 포함되었다. 국토안보부에서 실시하는 사이버보안 평가 프로그램은 8개가 제시되어 있으며, 이중 제어시스템과 관련된 평가 프로그램은 CSET(Onsite Cyber Security Evaluation Tool) 평가, DAR(ICS-CERT Design Architecture Review) 평가, NAVV(ICS Network Architecture Verification and Validation) 평가가 있으며, 그 특징은 표 3과 같다[5].

CSET은 미국 국립표준연구소(NIST)의 제어시스템 보안 기준 800-82, 북미전기신뢰성위원회(NERC)의 CIP 기준, 원자력위원회의 규제기준, 교통보안국(TSA)의 파이프라인 보안 기준 등 다양한 기준 대비 제어시스템 운영기관의 준수 정도를 분석하고 평가하는 제도로써 8시간 정도 소요된다.

DAR은 ICS 네트워크 설계 및 자산 분석을 통해 산업 제어시스템과 네트워크의 사이버보안 설계를 지원하며 2일 정도의 시간이 소요된다.

NAVV는 산업 제어시스템 네트워크 트래픽을 수집하여, TCP 헤더 분석을 통해 산업 제어시스템 내 통신 흐름을 분석함으로써 네트워크에 대한 안전성을 검증하는 것으로 분석 양에 비례하여 소요 시간이 증가하며, Sophia 도구를 활용하여 분석을 자동화하였다.

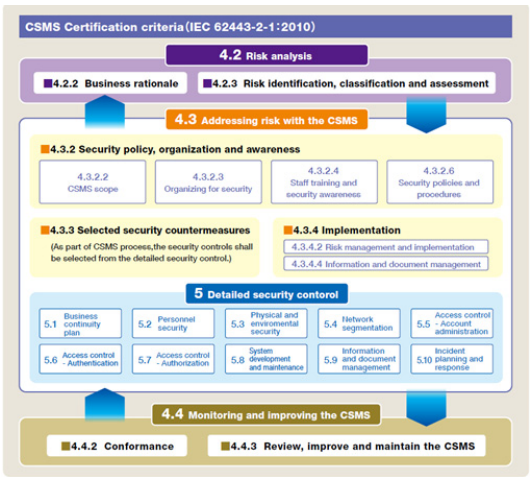
3.3. 일본 정보관리시스템인증센터의 CSMS 적합성 평가 제도

CSMS(Cyber Security Management System) 적합성 평가제도는 산업 제어시스템 사이버보안 관리 시스템을 대상으로 한 제3자 인증 제도이다[6]. CSMS는

〔표 3〕 미국 DHS의 제어시스템 사이버보안 평가 프로그램[5]

구분	CSET(Onsite Cyber Security Evaluation Tool) Assessment	ICS-CERT Design Architecture Review(DAR)	ICS Network Architecture Verification and Validation(NAVV)
평가 목적	산업 제어시스템 보안표준/기준 대비 조직의 제어시스템 사이버보안 수준을 평가	네트워크 설계 및 자산 분석을 통해 산업 제어시스템과 네트워크의 사이버보안 설계를 지원	TCP 헤더 데이터를 수동 수집하여, ICS 통신 흐름 분석을 통해, ICS 네트워크에 대한 안전성 검증
평가 범위	ICS	ICS, Network Architecture	ICS, Network Architecture, Network Traffic
소요 시간	8시간(1일)	2일	가변적
찾고자 하는 정보	ICS의 핵심 기능, 인프라, 정책 및 절차	네트워크 설계, 구성 설정, 상호 연계성	네트워크 트래픽 헤더 데이터 (Sophia 도구 활용)
현장평가 참석대상	ICS 운영자/엔지니어, IT 정책/관리 인력, 분야별 전문가	ICS 운영자/엔지니어, IT 인력, ICS 네트워크 및 구조 전문가	ICS 운영자/엔지니어, IT 인력, ICS 네트워크 및 구조 전문가
비고	NIST SP 800-82, NERC CIP, TSA Pipeline Security Guidelines 등 다양한 기준 적용 가능	ICS 네트워크 설계 및 자산 분석	ICS 프로토콜 분석, 네트워크 경계 점검 및 방어 기능 확인을 통해서 ICS 네트워크에 대한 V&V 수행

2014년에 일본정보경제사회추진협회(JIPDEC)에 의해 만들어진 이후 2018년 4월 공인기구로서의 독립성을 명확히 하고, 객관성 및 공정성 있는 인증 활동을 추진하기 위해 만든 사단법인 정보관리시스템인증센터(ISMS-Accreditation Center)에서 인정기구 역할을 하고 있으며, 인증기관은 일본 BSI(The British Standards Institution)와 재단법인 일본품질보증기구관리시스템(JQA)이 역할을 수행한다[6]. CSMS 인증은 IEC 62443-2-1:2010 표준을 기반으로 개발된 “CSMS 인증 기준”을 이용하며 그림 3과 같이 구성되어 있다[6]. CSMS에 의해 인증 받은 운영기관은 6개가 있으며 표 4에 열거되어 있다.



〔그림 3〕 CSMS 인증 기준[6]

〔표 4〕 CSMS 인증 현황

번호	기관명	인증부문	최초 인증일
1	미쯔비시 화학 엔지니어링	플랜트 프로세스 자동화 시스템	2014.4.25
2	도쿄 가스(주)	히타치 LNG 기지	2016.3.4
3	메타 워터(주)	DCS 패키지 S/W 개발	2016.9.26
4	MHPS 컨트롤 시스템	제조	2016.10.7
5	㈜ 히타치 시스템즈	SHIELD 보안센터	2018.2.16
6	JFE 엔지니어링	글로벌 원격 센터	2018.2.16

3.4. 프랑스 ANSSI의 CSPN 프로그램

CSPN 프로그램은 프랑스의 국가정보시스템보안청인 ANSSI(Agence nationale de la securite des systemes d’information)에서 2008년부터 IT 보안제품을 대상으로 실시하는 인증 프로그램이다[7]. CSPN은 CC인증에 비해 단기간에 저렴한 비용으로 프랑스 자국 내에서만 통용되도록 설계한 인증 제도로써 2016년부터는 PLC와 산업용 스위치 등의 산업 제어시스템 구성요소에 대한 보안 평가를 추가하여 수행하고 있다. PLC에 대해 시험을 승인받은 평가센터는 AMOSSYS, CEA-LETI, LEXFO, OPPIDA, SEREMA Technologies 등 5개가 있으며, 2019년 3월 기준으로 Siemens PLC 2종과 Schneider Electric PLC 1종 등

〔표 5〕 CSPN의 PLC 보안 요구사항[8]

대상	가용성	기밀성	무결성	진본성
Firmware			X	X
User program		(X)	X	X
Configuration		(X)	X	
Execution mode			X	
User authentication mechanism			X	X
User secrets		X	X	
Access control policy			X	
Local logging	X			
Remote logging	X			
Local logs			X	X
Remote logs			X	X

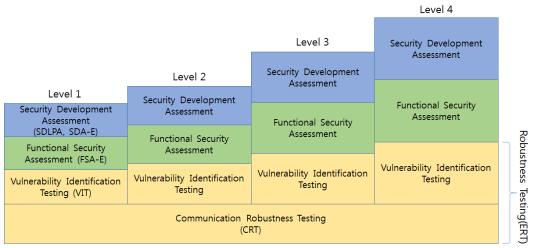
X : mandatory (X): optional

PLC 3개 제품과 Siemens의 Scalance 산업용 스위치 1개 제품이 인증을 받았다[7]. CSPN에서 PLC 인증에 사용되는 보안 요구사항은 표 5와 같다.

3.5. ISCI의 ISASecure 인증 프로그램

ISASecure 인증은 ISA 보안 준수기구인 ISCI(ISA Security Compliance Institute)에서 IEC 62443 표준 기반으로 인증하는 프로그램이다[9]. ISASecure 인증은 임베디드 장치에 대한 보안 인증을 수행하는 EDSA(Embedded Device Security Assurance), 제어시스템에 대한 보안 인증을 수행하는 SSA(System Security Assurance), 안전한 제어시스템 개발 보안 프로세스를 인증하는 SDLA(Security Development Lifecycle Assurance)의 세 종류가 있다[9].

EDSA 인증은 PLC, DCS Controller, SIS Controller, Field Sensor Device 등[10]의 임베디드 장치를 대상으로 하며, 4개 등급으로 보안수준을 판정한다. EDSA 평가는 그림 4와 같이 네트워크 견고성 시험과 취약점 식별 시험으로 구성된 임베디드 장치 견고성 시험과 보안기능 평가, 보안개발 평가로 구성된다. 네트워크 견고성 시험은 Ethernet, ARP, IPv4, ICMPv4, UDP, TCP 프로토콜 헤더에 대한 퍼징과 스트레스 시험을 수행하며, 모든 보안 등급에서 동일하다. 그러나 취약점 식별 시험, 보안기능 평가, 보안개발 평가는 보안등급이 높을수록 더 엄격한 요구사항이 요구된다. 또



〔그림 4〕 ISASecure EDSA 인증 평가 요소[9]

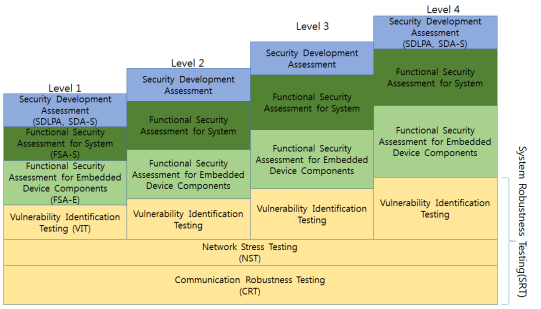
한 보안기능 평가는 IEC 62443-4-2 표준 기반의 요구사항을 적용하며, 보안개발 평가는 IEC 62443-4-1 표준을 기반으로 도출된 요구사항을 적용한다. 2019년 3월 현재 34개 제품이 인증을 받았으며, 6개 제품이 Level 2, 28개 제품이 Level 1 인증을 받았으며, Level 3과 Level 4 인증을 받은 제품은 없다.

SSA 인증은 시스템을 대상으로 하며, 여기서 시스템이란 전체 제어시스템을 구성하는 부분집합을 의미하며, 아래 4가지 중 하나로 볼 수 있다.

① 하나 이상의 구성요소로 이루어진 제어시스템
② 서로 다른 제조사의 H/W, S/W 구성요소로 구성된 제품으로 하나의 공급사가 공급하는 제어시스템
③ 하나의 존을 구성하는 고정된 장치들로 이루어진 제어시스템
④ 구성 관리(configuration control) 및 버전 관리하의 시스템 제품

SSA 평가는 그림 5와 같이 시스템 견고성 시험, 임베디드 장치 보안기능 평가, 시스템 보안기능 평가, 보안개발 평가로 구성된다. 시스템 견고성 시험은 네트워크 견고성 시험, 네트워크 스트레스 시험, 취약점 식별 시험의 세부 시험으로 구성된다. 임베디드 장치 보안기능 평가는 IEC 62443-4-2 표준의 요구사항, 시스템 보안기능 평가는 IEC 62443-3-3 표준의 요구사항, 보안개발 평가는 IEC 62443-4-1 표준의 요구사항을 기반으로 한다. 2018년 10월 10일 이후 3.0.0 버전의 기준이 적용되고 있다[9]. SSA 인증을 받은 제품은 2019년 3월 기준으로 1개 제품이 있으며, Level 1 인증을 받았다. SSA의 인증 수준은 IEC 62443-1-1에 정의된 4가지 보안 수준에 따른다.

SDLA 인증은 IEC 62443-4-1 표준을 기반으로 제조사의 제조 프로세스가 보안 요구사항을 만족하는지 확인하고, 제조 프로세스에서 생산된 제품 또는 결과물이 적합한지를 시험한다[9]. EDSA 및 SSA 인증을 받기



〔그림 5〕 ISASecure SSA 인증 평가 요소

위해서는 사전에 SDLA 인증을 받아야 하며, EDSA 및 SSA 인증과 함께 병렬로 SDLA 인증을 신청할 수도 있다.

ISASecure의 시험 인증기관은 미국의 exida, 일본의 CSSC-CL, 독일의 TÜV Rheinland가 있으며, 시험・인증 기관별 인증대상과 요구사항 버전은 다르다[9, 11]. exida는 EDSA 기준과 SSA 기준은 2.0.0, 2.1.0, 3.0.0의 세 가지 버전에 대해서 승인 받았으며, SDLA 기준은 2.0.0에 대해서 승인을 받았다. CSSC-CL은 EDSA 기준 2.1.0에 대해서만 시험 및 인증서 발행이 가능하며, 독일의 TÜV Rheinland는 EDSA 기준 2.0.0과 SDLA 기준 2.0.0에 대해서 시험을 수행하고 인증서를 발행할 수 있다.

3.6. IECEE의 산업 사이버보안 인증 프로그램

IECEE는 국제 전기기기 적합성 평가제도[12]로서, 2018년 2월 운영문서(OD) 2061 V1.1을 발표하고 IEC 62443 표준 기반의 산업 사이버보안 인증 프로그램을 시작하였다[13]. 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 인증서를 발급한다[13]. IEC 62443-2-4 표준을 이용하여 프로세스 역량평가, 제품 역량평가, 솔루션 적용 역량평가의 세 가지 인증서를 발급하고, IEC 62443-3-3 표준은 IEC 62443-4-1의 제품 역량 적용성 평가 인증과 함께 제품 역량평가 인증서를 발급한다. IEC 62443-4-1 표준을 이용해서는 프로세스 역량평가와 IEC 62443-3-3 또는 IEC 62443-4-2의 제품 역량평가 인증과 함께 제품 역량평가 인증서를 발급한다. IEC 62443-4-2 표준을 이용해서는 IEC 62443-4-1 표준을 이용한 제품 역량 적용성 평가 인증과 함께 제품 역량평가 인증서를 발급한다[13].

IECEE의 산업 사이버보안 인증은 각 NCB가 인증하고, NCB 소속 시험기관(CBTL: Certification Body Testing Laboratories)이 시험을 수행한다. IEC 62443-2-4:2015 표준의 발급 NCB는 12개, 인정 NCB는 1개, CBTL은 13개가 승인 받았으며, IEC 62443-3-3:2013 표준과 IEC 62443-4-1:2018 표준은 발급 NCB 5개, 인정 NCB 3개, CBTL 5개가 승인 받았다.

IECEE 산업 사이버보안 인증 프로그램에 참여하는 NCB 중에서 자체적으로 IEC 62443 관련 인증을 제공하고 있는 곳은 UL의 CAP for IEC 62443 인증[14], DEKRA의 Cyber Security Certification: IEC 62443[15], TÜV NORD의 Certification according to IEC 62443[16]이 있다. UL CAP for IEC 62443 서비스는 IEC 62443-2-4, IEC 62443-3-3, IEC 62443-4-1, IEC 62443-4-2 표준을 기반으로 시험・인증 서비스를 제공하며, 세부 시험 방법으로서 침투 테스트, 취약점 분석, 소스코드 분석, 퍼징 시험 등을 수행한다. IEC 62443-4-2 표준에 대한 시험은 현재 수행되고 있지 않다. DEKRA와 TÜV NORD의 IEC 62443 인증 관련 세부사항은 공개되어 있지 않다. 다만 TÜV NORD는 4차 산업시대의 보안 목표 달성을 위해서 산업 제어시스템에 대해서 IEC 62443 인증을 받고, 업무시스템에 대해서 ISO 27001 인증을 받음으로써, 4차 산업 준비도(Industry 4.0 readiness)를 달성하도록 권고하고 있다[16].

3.7. UL의 사이버보안 보증 프로그램

UL은 산업 제어시스템에 대한 사이버보안 보증 프로그램인 CAP(Cybersecurity Assurance Program) 서비스를 운영중이며, UL 2900-2-2 표준에 기반한 UL CAP for ICS와 IEC 62443 표준 기반의 UL CAP for IEC 62443 서비스를 제공하고 있다[17].

UL CAP for ICS는 UL 2900-2-2 표준을 기반으로 산업 제어시스템의 구성요소인 네트워크 게이트웨이, I/O 장치, 플랫폼, 대쉬보드 프로세서 등을 대상으로 한다. 해당 서비스에는 시험결과 보고서를 제공하는 시험

서비스와 전체 요구사항에 대한 시험 결과를 기반으로 인증서를 제공하는 인증 서비스가 있다[17]. UL CAP for ICS 인증을 받은 제품은 4개 제품이 있다[18].

UL CAP for IEC 62443 서비스는 UL이 IECEE의 산업 사이버보안 인증 프로그램에 국가인증기관으로 참여하여, 시험을 수행하고 인증서를 발행하는 것으로 [14], 3.6절에서 설명하였다.

3.8. exida의 사이버보안 인증 프로그램

미국의 시험기관인 exida는 ISASecure 인증과 자체 보안인증 서비스를 제공하고 있다[11]. exida의 ISASecure 인증은 3.5절에서 설명한 ISASecure 인증에 대한 시험·인증기관으로서 EDSA, SSA, SDLA 인증 기준에 의거 시험을 수행하고, 인증서를 발급하고 있다.

exida 자체 인증은 IEC 62443 제어시스템 보안 인증 프로그램이 있으며 엔지니어링 프로세스 사이버 보안 인증, 장치 및 애플리케이션 사이버보안 인증, 시스템 사이버보안 인증, 인력의 사이버보안 자격 인증의 4가지 인증 서비스를 제공한다[11].

엔지니어링 프로세스 사이버보안 인증에는 IEC 62443-4-1 표준을 이용하여 제조사를 대상으로 제공하는 exida Security Development Process 인증 프로그램과 IEC 62443-2-4 표준을 이용하여 시스템 통합사업자를 대상으로 제공하는 exida System Integrator Process 인증 프로그램이 있다. exida Security Development Process 인증 프로그램은 마이크로컴퓨터 기반의 장치 및 소프트웨어 애플리케이션을 설계하는 제조사의 프로세스가 인증 대상이며, exida System Integrator Process 인증 프로그램은 시스템 통합사업자의 시스템 설계 엔지니어링 프로세스가 인증 대상이다.

장치 및 애플리케이션 사이버보안 인증은 임베디드 제어 장치, 플랫폼 장치, 소프트웨어 애플리케이션에 대해서 IEC 62443-4-1 기반의 사이버보안 엔지니어링 프로세스를 시험하고, IEC 62443-4-2 기반의 사이버보안 방어 기술이 포함되었는지를 시험하여 4등급으로 인증한다.

시스템 사이버보안 인증은 제조사의 시스템(OEM System)에 대한 인증과 통합 시스템(Integrated System)에 대한 인증이 있다. exida System Security Certification은 IEC 62443-4-1 표준과 IEC 62443-4-2 표준을 기반으로 장치에 적용 가능한 사이버보안 요구사항을 시험하며, exida Integrated System Certification은 IEC 62443-2-4 표준과 IEC 62443-3-3 표준을 기반으로 시스템 통합 사업자에 의해 만들어진 시스템에 대하여 시험한다. 시스템 사이버보안 인증을 받은 제품중 일부는 ISASecure EDSA/SSA/SDLA 인증을 함께 받기도 한다.

인력에 대한 사이버보안 자격 인증은 IEC 62443-4-1과 4-2 표준을 기반으로 제조사 개발자를 대상으로 한 CACE(Certified Automation Cybersecurity Expert)/CACS(Certificed Automation Cybersecurity Specialist) 소프트웨어 프로그램, IEC 62443-2-4와 3-3 표준을 기반으로 시스템 설계자 대상의 CACE/CACS Designer 프로그램, 그리고 동일한 표준을 기반으로 시스템 통합 사업자 대상의 CACE/CACS Integrator 프로그램이 있다.

exida는 2019년 3월 22일 기준으로 24개 인증서를 발급하였으며, 엔지니어링 프로세스 5개와 제어기 19개를 포함하고 있다. 일부 제어기는 IEC 62443 인증과 ISASecure 인증을 함께 받은 것도 있다.

3.9. 독일 TÜV SÜD의 IEC 62443 인증

TÜV SÜD는 독일의 시험인증기관으로서 독일 인정기관인 DAkkS(German Accreditation Body)로부터 IEC 62443 표준에 따른 시험기관으로 인정받았으며 산업 자동화 제어시스템 사이버보안 인증 서비스를 제공한다. 인증은 IEC 62443-2-4와 IEC 62443-3-3 표준을 기반으로 시스템 통합 사업자를 인증하고, IEC 62443-4-1과 IEC 62443-3-3 표준을 기반으로 제조사의 안전한 개발 프로세스에 대해서 인증한다[19].

Siemens의 Simatic PCS7 프로세스 제어시스템이 IEC 62443-2-4와 IEC 62443-3-3 표준 기반 인증, Phoenix Contact과 COPA-DATA는 IEC 62443-4-1 표준 기반으로 인증을 받았다.

3.10. GE의 Achilles 인증

Achilles 인증은 GE사에서 제공하는 사이버보안 인증 프로그램으로 Achilles Communications Certifi-

cation(ACC), Achilles Practices Certification(APC), Achilles System Certification(ASC)이 있다[20].

ACC 인증은 임베디드 장치, 호스트 기반 장치, 제어 애플리케이션, 네트워크 컴포넌트를 대상으로 네트워크 견고성을 시험한다[20]. 시험기준은 대상 그룹별로 두 가지 보안수준(Level 1, Level 2)에 따라 Ethernet, ARP, ICMP, IP, UDP, TCP 및 제어 프로토콜에 대해서 프로토콜 퍼징 시험, 알려진 취약점 확인, 트래픽 부하 시험을 수행하여, 제어시스템에서 반드시 확보되어야 할 네트워크 가용성을 평가한다.

APC 인증은 IEC 62443-2-4 표준을 기반으로 산업 제어시스템 통합 사업자 또는 유지보수 서비스 제공자의 사이버보안 절차, 실무지침, 서비스 개발, 시험, 유지관리 등 생명주기 전반에 걸친 보안 요구사항을 평가하고 인증을 부여한다[22].

ASC 인증은 2016년부터 제공하는 인증 서비스로써, 임베디드 장치, 호스트 기반 장치, 제어 애플리케이션, 네트워크 컴포넌트를 통합하여 하나의 제품으로 판매하는 제어시스템에 대해서 IEC 62443-3-3 보안 요구사항 만족 여부를 확인하고, 보안수준 1 ~ 4까지의 수준에 따른 인증서를 제공한다[21]. 따라서 ASC 인증을 신청하는 대상자는 제어시스템 벤더사이며, 보안수준(SL1 ~ SL4), 기능요구사항 그룹(7개의 Foundational Requirement), 개별 요구사항 단위로 인증을 신청할 수 있다.

Ⅳ. 산업 제어시스템 보안성 평가제도 분석

본 장에서는 Ⅲ장에서 설명한 산업 제어시스템에 대한 보안성 평가제도의 특징을 분석한다. 산업 제어시스템 보안성 평가제도는 국가에서 도입 및 운영하는 제도, 국제 표준화 기구에서 도입한 제도, 시험기관이 독자적으로 도입한 제도, 제어시스템 제조사가 도입한 제도로 구분할 수 있으며, 표 6과 같다.

〔표 6〕 평가제도 도입 주체에 따른 분류

도입 주체	평가제도 명칭
국가	NSTB, CSET, DAR, NAVV, CSMS, CSPN
국제 표준화 기구	ISASecure EDSA/SSA/SDLA IECEE 산업 사이버보안 인증 UL CAP for ICS
시험기관	TÜV SÜD의 IEC 62443 인증 exida의 사이버보안 인증 프로그램
제조사	ACC, ASC, APC

산업 제어시스템 보안성 평가제도별로 제도가 적용되는 시기에 따라 분류하면 표 7과 같다.

〔표 7〕 평가 시기에 따른 분류

평가 시기	평가제도 명칭
제조 시점 (제어시스템 구성 제품, 시스템)	ISASecure EDSA/SSA/SDLA IECEE 산업 사이버보안 인증 CSPN, ACC, ASC, UL CAP for ICS TÜV SÜD의 IEC 62443 인증 exida의 사이버보안 인증 프로그램
구축 및 유지보수 시점 (시스템 통합 및 유지보수 사업자)	APC, IECEE 산업 사이버보안 인증 TÜV SÜD의 IEC 62443 인증 exida의 사이버보안 인증 프로그램
운용 시점 (제어시스템 운영자)	NSTB, CSET, DAR, NAVV, CSMS

산업 제어시스템 구성 제품 및 시스템에 적용되는 보안성 평가제도의 시험 및 인증 대상에 따라 분류하면 표 8과 같다.

〔표 8〕 평가 대상에 따른 분류

평가 대상	평가제도 명칭
임베디드 장치	ACC, ISASecure EDSA exida의 사이버보안 인증 프로그램 UL CAP for ICS, CSPN IECEE 산업 사이버보안 인증
호스트 장치	ISASecure EDSA exida의 사이버보안 인증 프로그램 UL CAP for ICS IECEE 산업 사이버보안 인증
제어 애플리케이션	ISASecure EDSA exida의 사이버보안 인증 프로그램 IECEE 산업 사이버보안 인증
네트워크 컴포넌트	ISASecure EDSA UL CAP for ICS IECEE 산업 사이버보안 인증, CSPN
제어시스템	ASC, ISASecure SSA exida의 사이버보안 인증 프로그램 IECEE 산업 사이버보안 인증

산업 제어시스템 보안성 평가를 위한 기준에 따라 분류하면 표 9와 같다. 현재 산업 제어시스템 보안성 평가에 사용되는 기준은 IEC 62443을 주로 하고 있으며, 그

〔표 9〕 평가 기준에 따른 분류

평가 기준	평가제도 명칭
IEC 62443	IECEE 산업 사이버보안 인증 exida의 사이버보안 인증 프로그램 ISASecure EDSA/SSA/SDLA CSMS, ASC TÜV SÜD의 IEC 62443 인증
UL 2900-2	UL CAP for ICS
NIST, NERC, TSA, DoD 표준 활용	CSET
자체 기준	NSTB, DAR, NAVV, CSPN, ACC, APC

외 UL 2900-2 표준과 자체 기준을 사용하고 있다.

Ⅴ. 결 론

본 논문은 산업 제어시스템 보안취약점 발견의 증가, 산업 제어시스템 사이버보안 사고로 인한 정전, 물리적 피해 발생, 4차 산업혁명을 계기로 확대되고 있는 산업 제어시스템의 네트워크 연결로 인한 보안위협 증가 등으로 인해 필요성이 증가하고 있는 산업 제어시스템 보안성 평가에 대해 설명하였다. 2003년부터 미국을 중심으로 산업 제어시스템에 대한 보안성 평가가 실시된 이래 일본, 프랑스 등의 국가기관이 주도하는 산업 제어시스템 보안성 평가제도 뿐만 아니라, 표준화 단체, 글로벌 시험기관, 제조사에서 실시하는 산업 제어시스템 보안성 평가제도 등 다양한 제도들이 운영중이며 이러한 세부사항은 Ⅲ장에서 제시하였다. 또한 Ⅳ장에서는 산업 제어시스템을 대상으로 한 보안성 평가제도를 제도 도입주체, 평가 시기, 평가 대상, 평가 기준에 따라 분류하였다. 이를 통해 산업 제어시스템 전 생명주기에 따라 평가를 수행할 수 있고, 임베디드 장치, 호스트 장치, 제어 애플리케이션, 네트워크 컴포넌트 및 이들의 결합으로 구성된 단일 제어시스템에 대한 평가도 가능함을 알 수 있었다. 또한 평가 기준 측면에서는 IEC 62443 표준이 주로 사용되고 있으나 일부 자체적인 기준을 사용하는 평가제도도 있었으며, 이는 국가에서 주도적으로 운영하는 제도인 경우가 많았다. 따라서 국내에서도 이에 대응할 수 있는 제도 마련이 필요할 것이다.

참 고 문 헌

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

[2] National SCADA Test Bed from https://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed/

[3] Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, Department of Energy, pp.11-16, 2011.

[4] David Kuipers, “Idaho National Laboratory National SCADA Test Bed,” Oct. 2010.

[5] Braford Willke and Sean McCloskey, “DHS Cyber Security & Resilience Resources: Cyber preparedness, Risk Mitigation & Incident Response,” Feb. 2015.

[6] 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.

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

[8] GTCSI, *Protection profile of an industrial programmable logic controller version 1.1*, July. 2015.

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

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

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

[12] IECEE CB Scheme from https://www.iecee.org/about/cb-scheme, 2019.

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

[14] UL, Accelerate your cyber readiness with IEC 62443 from https://industries.ul.com/wp-content/u

ploads/sites/2/2017/04/ ULCyber62443_133.01.0317.EN_.EPT_.pdf.

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

[16] 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/.

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

[20] Xie F., Peng Y., Zhao W., Gao Y. and Han X., “Evaluating Industrial Control Devices Security: Standards, Technologies and Challenges,” *IFIP International Conference on Computer Information Systems and Industrial Management*, LNCS, vol. 8838, pp. 624-635, 2015.

[21] GE Digital, Achilles System Certification(ASC) from GE Digital FAQ from https://www.ge.com/digital/asset/achilles-system-certification-frequently-ascked-questions

[22] 손경호, “산업제어시스템 보안성 평가・인증 동향 분석”, *정보보호학회지*, 24(5), 2014. 10.

〈저자소개〉

김 우 년 (Woonyon Kim)

정회원

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

박 응 기 (Eung-Ki Park)

정회원

1986년 2월 : 중앙대학교 전자계산학과 졸업
1988년 2월 : 중앙대학교 전자계산학과 석사
2005년 8월 : 아주대학교 컴퓨터공학과 공학박사
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

김 신 규 (Sin-Kyu Kim)

정회원

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

지 윤 석 (Yoon-Seok Jee)

정회원

1992년 2월 : 경원대학교 전자계산학과 졸업
1998년 8월 : 한양대학교 전자계산학 석사
2018년 3월 : 숭실대학교 IT정책경영학과 박사과정 재학 중
<관심분야> 기반시설보안, 사이버보안정책, 정보보안관리 실태평가