IEC 62443 표준기반 스마트 디바이스 보안

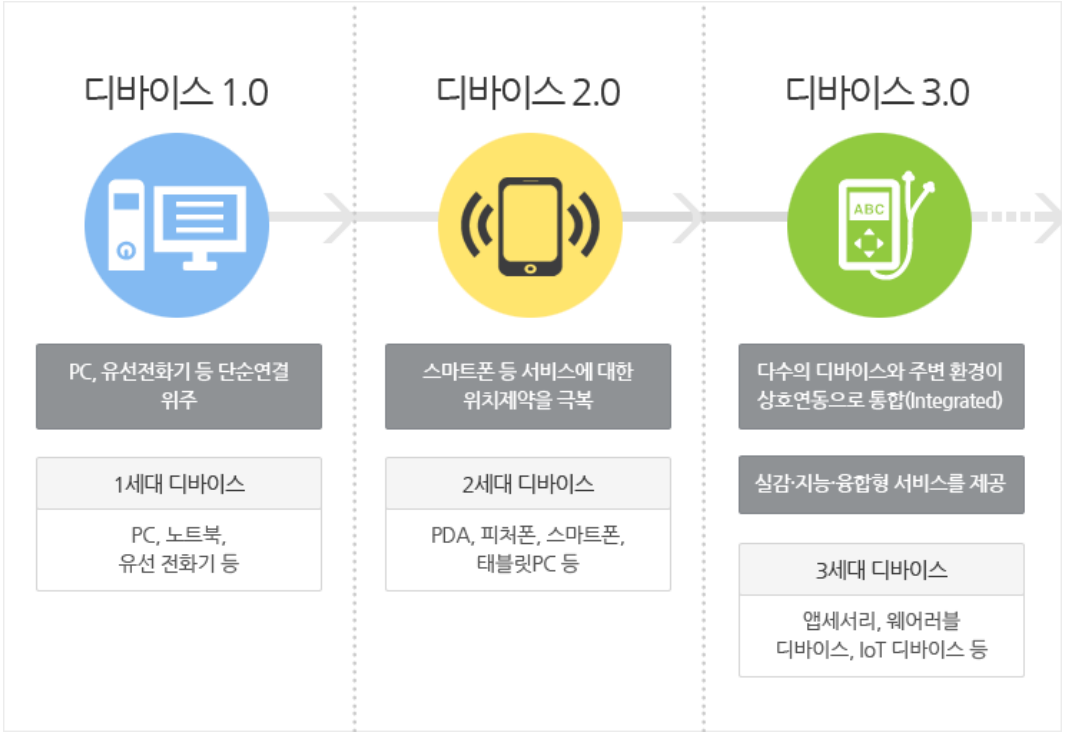
2020.7.

내용

- 스마트디바이스
- 스마트디바이스 보안위협
- IEC 62443 보안 표준
- 개발자 관점의 스마트디바이스 보안
- 사용자 관점의 스마트디바이스 보안
- 시험·평가자 관점의 스마트디바이스 보안
- 요약

스마트디바이스

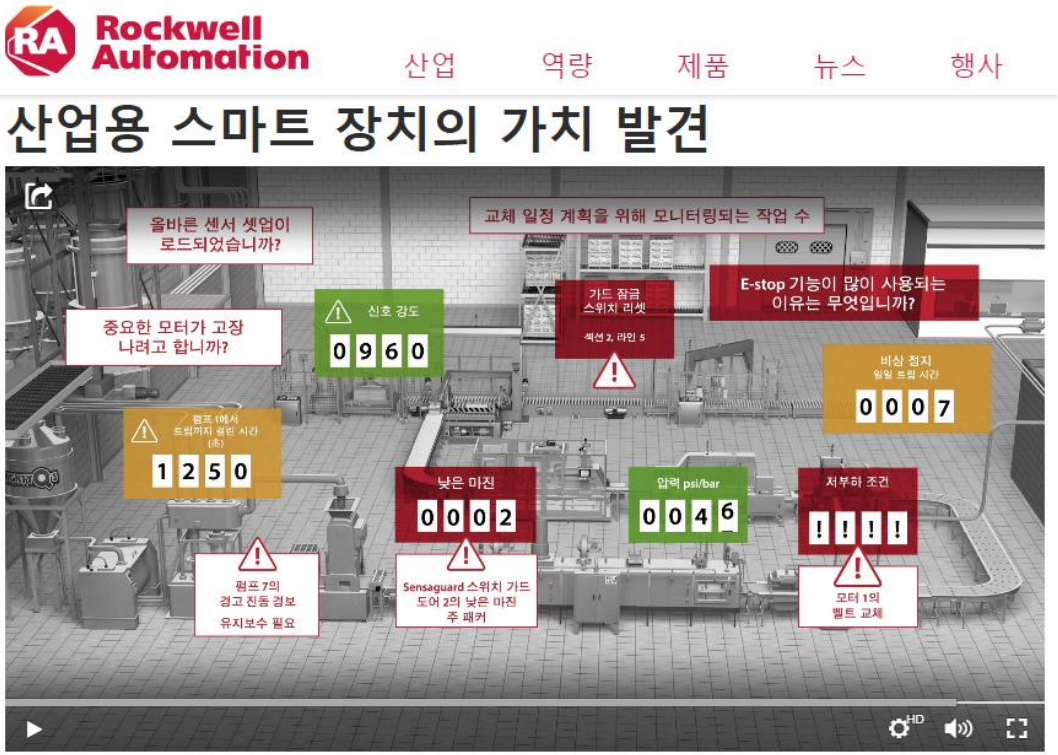
- 스마트디바이스
  - 각종 통신기술(WiFi, 블루투스, LTE 등)을 이용한 음향기기, 헬스케어, 영상기기, 구동기기(드론, RF 자동차·헬기 등) 같은 다양한 단말기기와 그 제어기기를 통칭하며, 웨어러블 기기, 스마트 가전, 디지털 사이니지, 증강현실기기(VR/MR) 등 다양한 형태의 제품들을 모두 포함(출처: 스마트기술진흥협회)



(출처: 스마트기술진흥협회)

스마트디바이스

- 스마트인프라
  - 4차 산업혁명으로 스마트화된 사회기반시설(도로/철도/항만/항공 교통, 에너지, 수자원, 제조 등)
- 산업용 스마트디바이스
  - 각종 통신기술(WiFi, 블루투스, LTE 등)을 이용한 센서, 구동기 같은 다양한 단말기기와 그 제어기기를 통칭



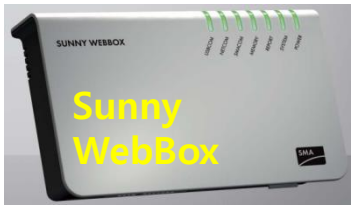
(출처: RA사 홈 페이지)

스마트디바이스 보안위협

- 스마트디바이스 보안취약점

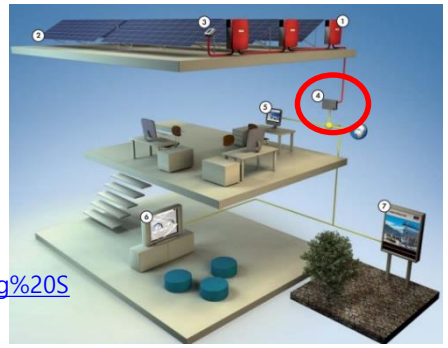
ICS Advisory (ICSA-14-247-01A)
Sensys Networks Traffic Sensor Vulnerabilities (Update A)
- 펌웨어 무단 업데이트, 평문 통신, 센서 위조 등의 취약점

이미지 출처 : VSN240 Sensor Installation and User Manual, Sensys Networks
(https://fccid.io/TDBVSN240/User-Manual/Users-Manual-616607)

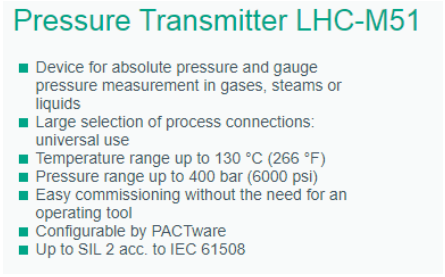


ICS Advisory (ICSA-19-281-01)
SMA Solar Technology AG Sunny WebBox
- CSRF 취약점

이미지 출처 : SUNNY WebBox
(http://www.suntechsolarsystem.com/datasheet/datasheet%20Remote%20Monitoring%20Systems/WebBox.pdf)



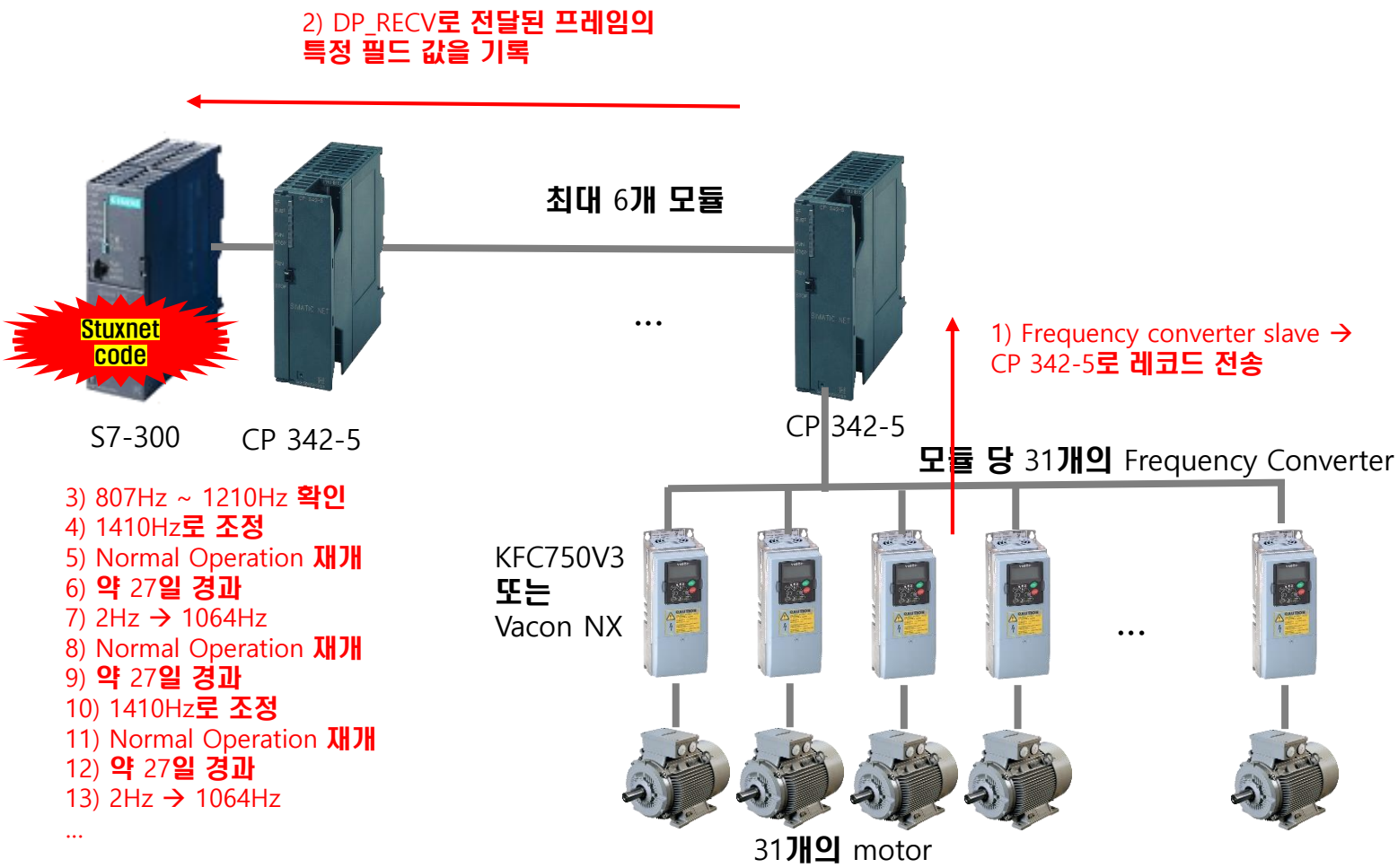
ICS Advisory (ICSA-15-036-02)
Pepperl+Fuchs Hart Device DTM Vulnerability
- 버퍼 오버플로우 유발



이미지 출처 : Pepperl-fuchs.com 한국어 홈페이지
(https://www.pepperl-fuchs.com/korea/ko/classid_491.htm?view=productdetails&prodid=58442)

스마트디바이스 보안위협

- 제어기기 대상 사이버공격 사례
  - Stuxnet (2010)



스마트디바이스 보안위협

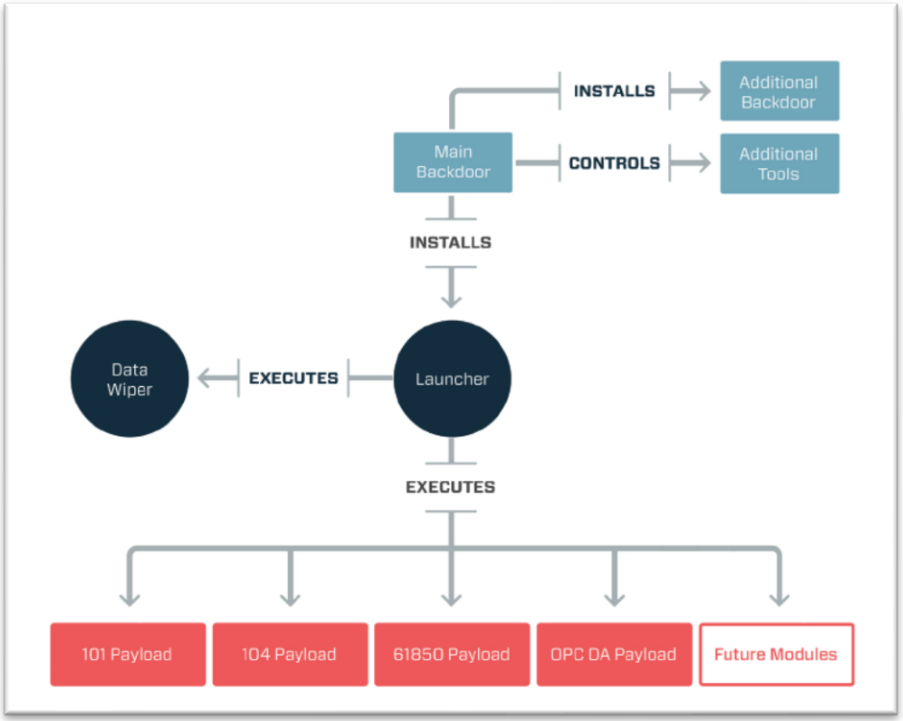
- 제어기기 대상 사이버공격 사례
  - Industroyer (2016)

Data Wiper
- ABB PCM600 **구성 파일 삭제**
- PCM600**은** IED **엔지니어링 도구**

File Extension	Usage
.pcmp	PCM600 Project (ABB)
.pcmi	PCM600 IEC File (ABB)
.pcmt	PCM600 Template IED File
.CIN	ABB MicroScada
.PL	Programmable Logic File
.paf	PLC Archive File
.SCL	Substation Configuration Language
.cid	Configured IED Description
.scd	Substation Configuration Description

SIPROTEC DoS

- Siemens SIPROTEC 4(IED), SIPROTEC Compact(IED) EN100 **이더넷 모듈 탑재 장비**
- 5000/UDP**로 임의의 패킷 전송시 원격에서** DoS **유발**
- (**피해**) SIPROTEC 4**대**



IEC 60870-5-101/104

- **유럽에서 사용하는 전력 송변전 SCADA용 제어프로토콜**
- **전력 차단 제어 명령을 전달** Off → On → Off
- (**피해**) 101 controller 8**대 이상**
- (**피해**) 104 **제어접점** 400**개 이상**

IEC 61850

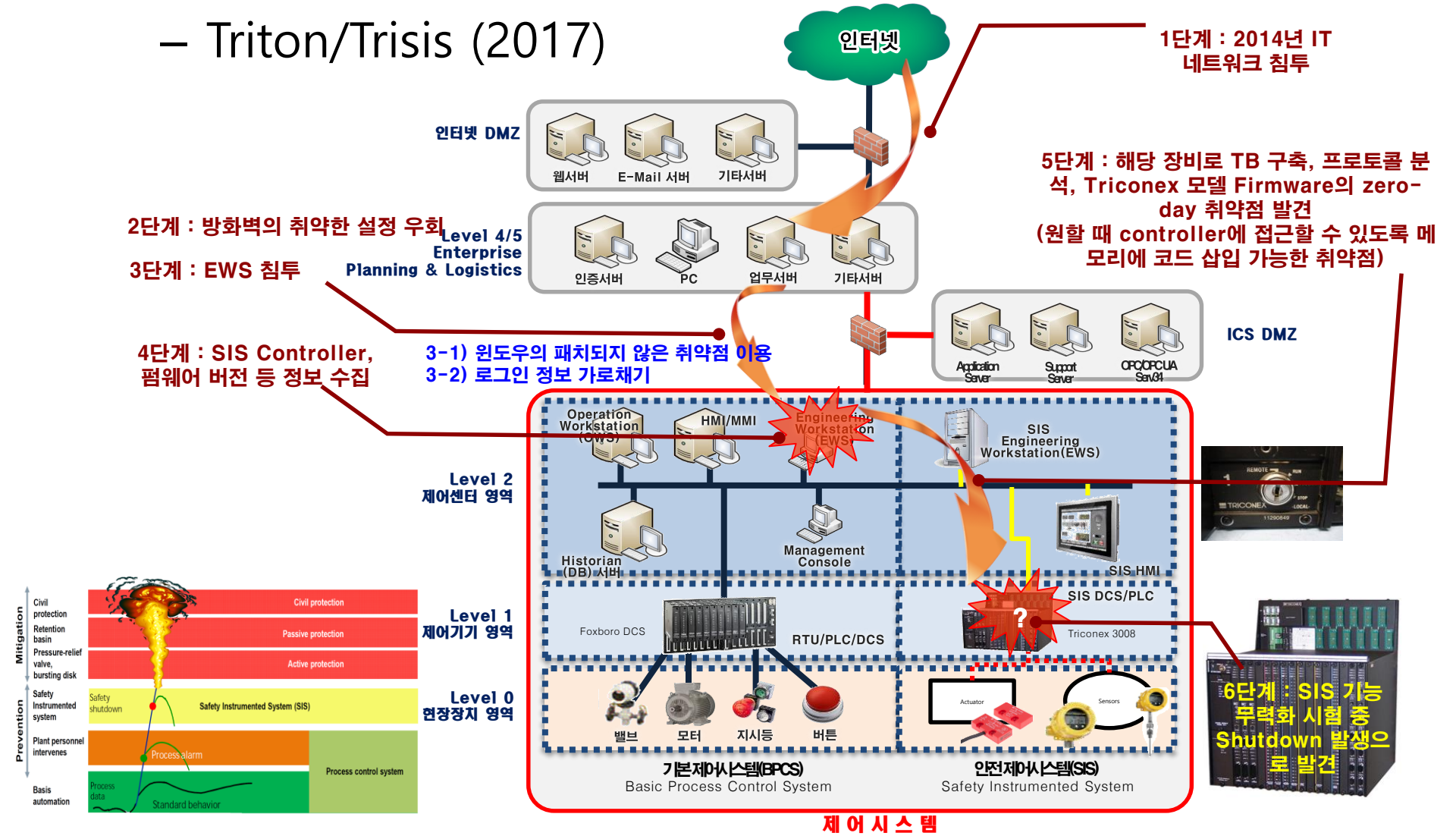
- **변전소/발전소 등에서 현장장치 보호를 위한** IED **설정/통신 프로토콜**
- IED**의 제어대상**(CSW)**의 동작 조작** SW OFF
- (**피해**) Subnet **내 전체** IED

OPC DA

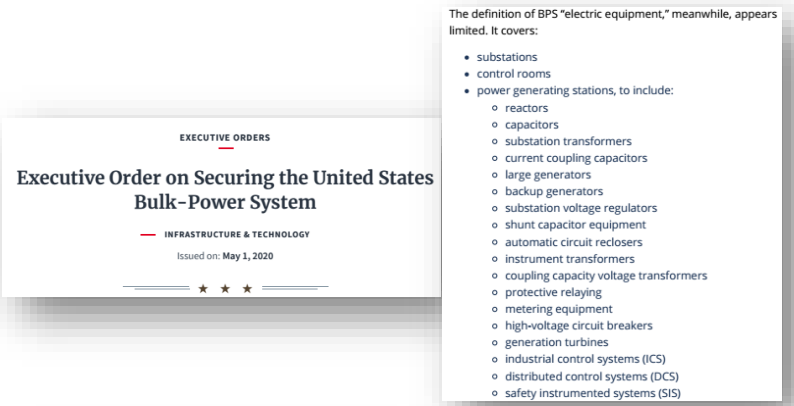
- OLE for Process Control Data Access **프로토콜**
- 0x01 **상태를 대상 시스템으로 전송** Primary Variable Out of Limits
- (**피해**) OPC **서버** 7**대 이상**

스마트디바이스 보안위협

- 제어기기 대상 사이버공격 사례
  - Triton/Trisis (2017)



스마트디바이스 보안대책


EXECUTIVE ORDERS

Executive Order on Securing the United States Bulk-Power System

INFRASTRUCTURE & TECHNOLOGY

Issued on: May 1, 2020

★ ★ ★

The definition of BPS "electric equipment," meanwhile, appears limited. It covers:

- substations
- control rooms
- power generating stations, to include:
  - reactors
  - capacitors
  - substation transformers
  - current coupling capacitors
  - large generators
  - backup generators
  - substation voltage regulators
  - shunt capacitor equipment
  - automatic circuit reclosers
  - instrument transformers
  - coupling capacity voltage transformers
  - protective relaying
  - metering equipment
  - high-voltage circuit breakers
  - generation turbines
  - industrial control systems (ICS)
  - distributed control systems (DCS)
  - safety instrumented systems (SIS)

트럼프, 대량 전력 시스템 보안에 대한 행정명령(2020.5.1)
- 적대국에서 제조한 전력망 장비나
  국가 안보에 위협이 되는 장비 구입 금지

* 기사 출처 : Trump Ban on Foreign Bulk Power Equipment Triggers New Uncertainty(2020.5.7., Power)


European Commission › Strategy › Shaping Europe's digital future › Policies ›

Shaping Europe's digital future

POLICY

The EU Cybersecurity Act

The EU Cybersecurity Act revamps and strengthens the EU Agency for cybersecurity (ENISA) and establishes an EU-wide cybersecurity certification framework for digital products, services and processes.

European Commission › Strategy › Shaping Europe's digital future › Policies ›

Shaping Europe's digital future

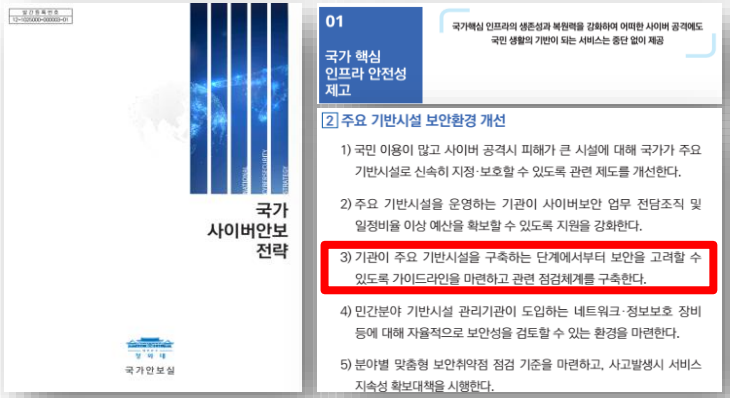
POLICY

The EU cybersecurity certification framework

The EU Cybersecurity Act establishes an EU certification framework for ICT digital products, services and processes. The European cybersecurity certification framework enables the creation of tailored and risk-based EU certification schemes.

Cybersecurity Act(EU 2019/881)
- 2019년부터 제품, 프로세스 및 서비스 제공을
  지원하는 유럽 사이보안 인증체계 준비

* 출처 : ENISA(http://ec.europa.eu/digital-sijngle -market/en/eu-cybersecurity-act/)


국가
사이버안보
전략

국가 안보실

01

국가 핵심 인프라 안전성 제고

국가핵심 인프라의 생존성과 복원력을 강화하여 어떠한 사이버 공격에도 국민 생활의 기반이 되는 서비스는 중단 없이 제공

2 주요 기반시설 보안환경 개선

1) 국민 이용이 많고 사이버 공격시 피해가 큰 시설에 대해 국가가 주요 기반시설로 신속히 지정·보호할 수 있도록 관련 제도를 개선한다.

2) 주요 기반시설을 운영하는 기관이 사이버보안 업무 전담조직 및 일정비율 이상 예산을 확보할 수 있도록 지원을 강화한다.

3) 기관이 주요 기반시설을 구축하는 단계에서부터 보안을 고려할 수 있도록 가이드라인을 마련하고 관련 점검체계를 구축한다.

4) 민간분야 기반시설 관리기관이 도입하는 네트워크·정보보호 장비 등에 대해 자율적으로 보안성을 검토할 수 있는 환경을 마련한다.

5) 분야별 맞춤형 보안취약점 점검 기준을 마련하고, 사고발생시 서비스 지속성 확보대책을 시행한다.

국가 사이버안보 전략(2019.4.)
- 기반시설 구축단계에서부터 보안을 고려

* 출처 : 국가 사이버안보 전략(청와대, 2019)

IEC 62443

2002~2007

2009

ISA99 committee

이미지 출처 : ISA 홈페이지
(http://isa.org/isa99/)

ANSI/ISA-99
ISA99

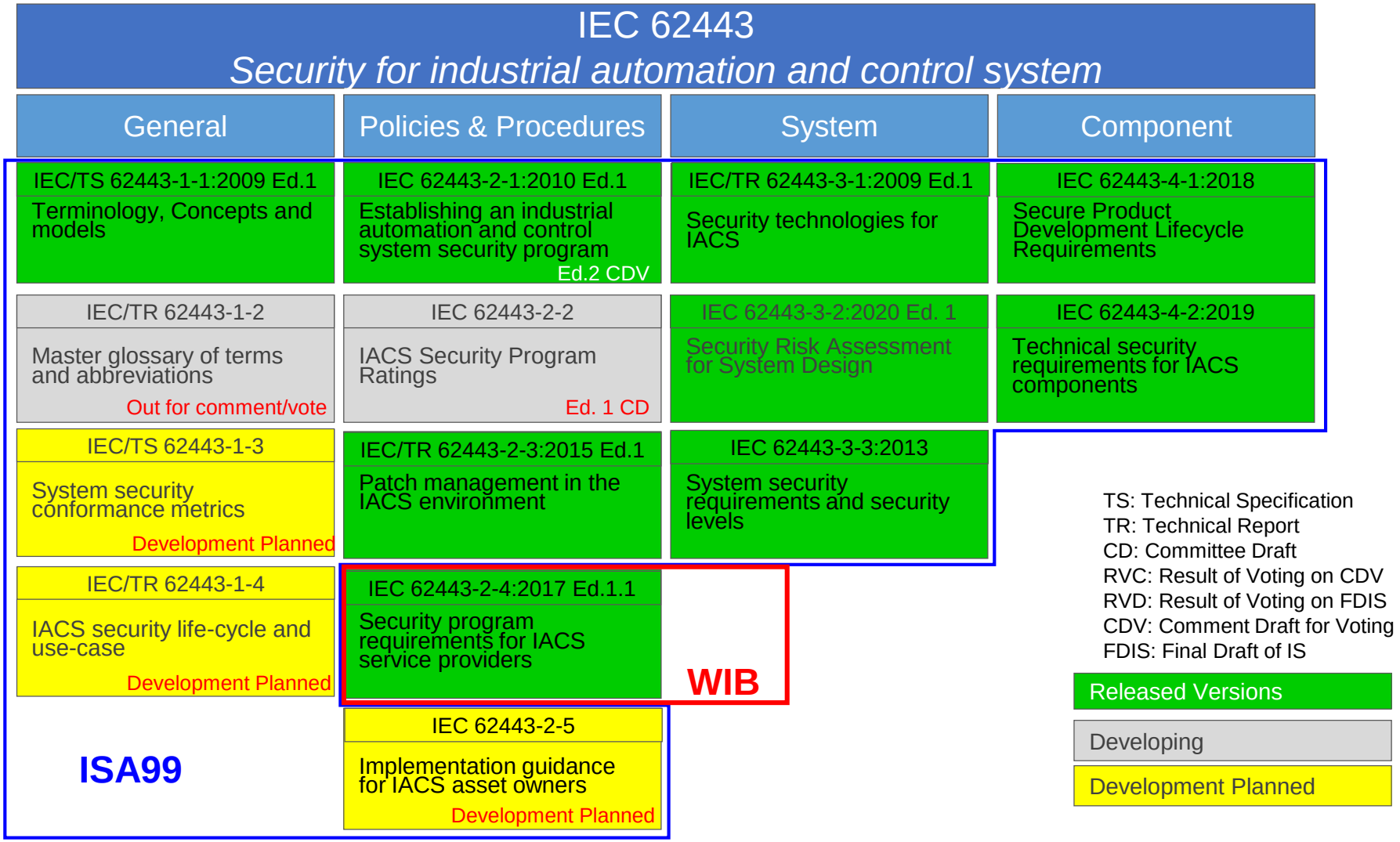
ANSI/ISA-
62443

TC65 WG10

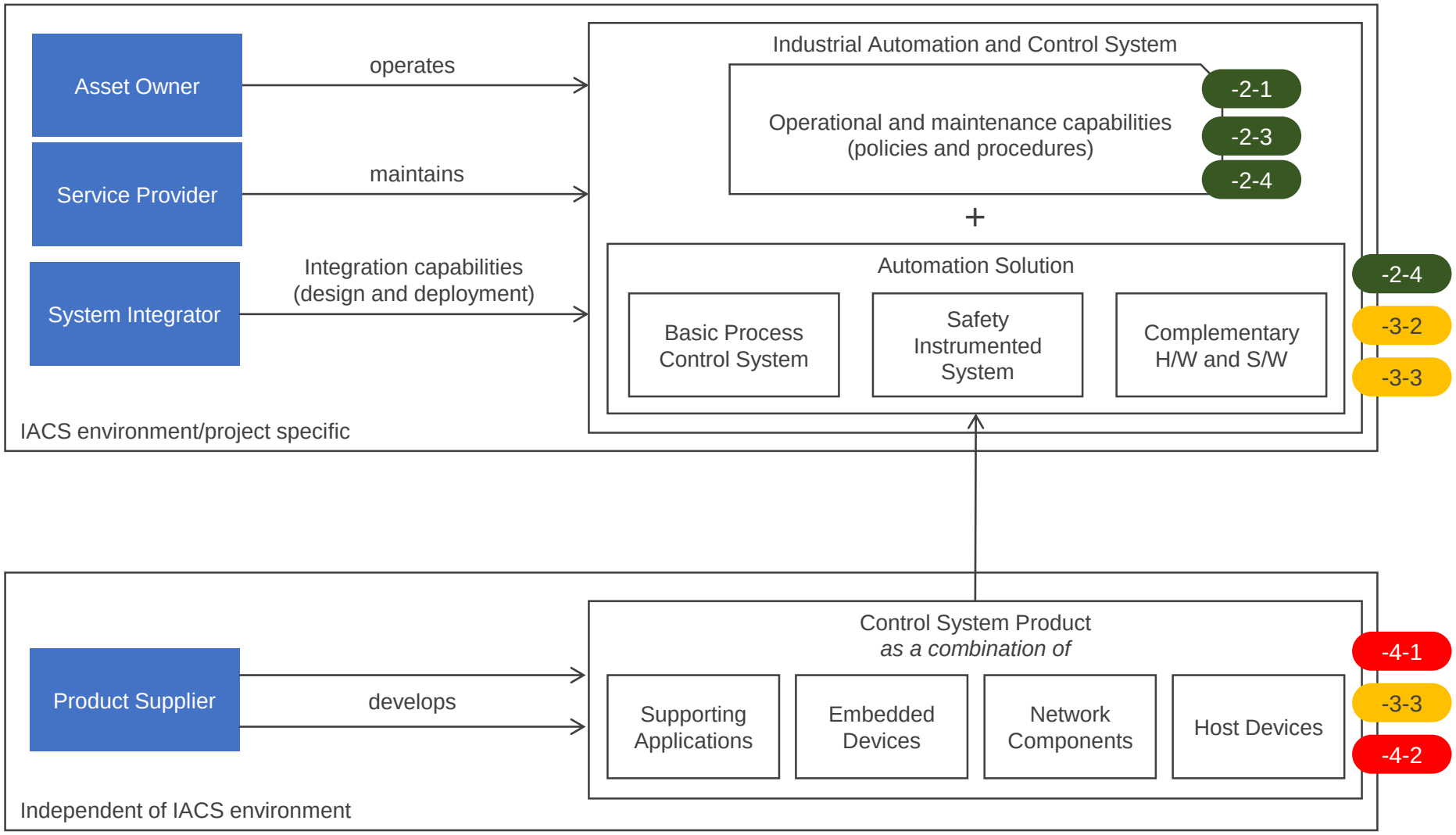
이미지 출처 : IEC 홈페이지
(http://iec.ch)

IEC-62443

IEC 62443

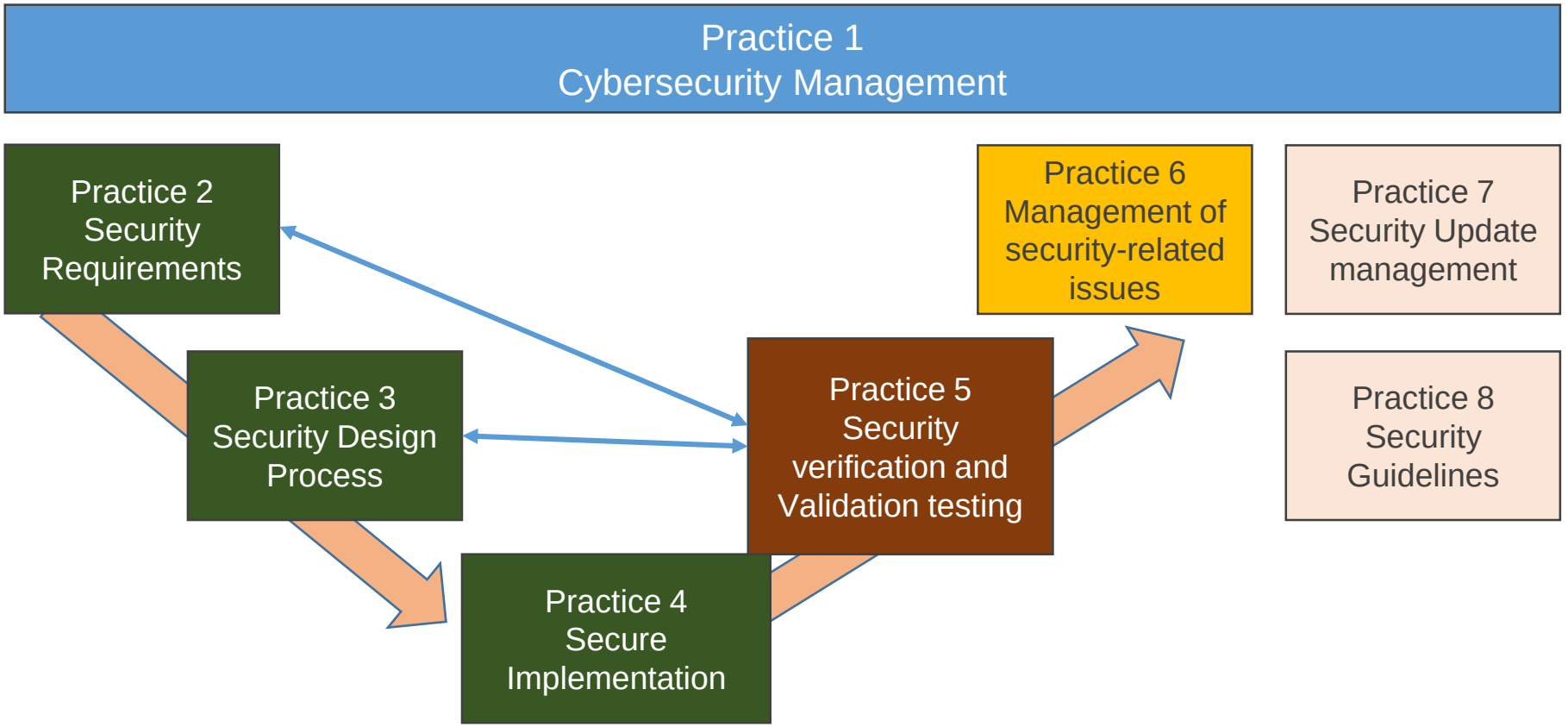

IEC 62443
Security for industrial automation and control system
General
Policies & Procedures
System
Component
IEC/TS 62443-1-1:2009 Ed.1
Terminology, Concepts and models
IEC 62443-2-1:2010 Ed.1
Establishing an industrial automation and control system security program
Ed.2 CDV
IEC/TR 62443-3-1:2009 Ed.1
Security technologies for IACS
IEC 62443-4-1:2018
Secure Product Development Lifecycle Requirements
IEC/TR 62443-1-2
Master glossary of terms and abbreviations
Out for comment/vote
IEC 62443-2-2
IACS Security Program Ratings
Ed. 1 CD
IEC 62443-3-2:2020 Ed. 1
Security Risk Assessment for System Design
IEC 62443-4-2:2019
Technical security requirements for IACS components
IEC/TS 62443-1-3
System security conformance metrics
Development Planned
IEC/TR 62443-2-3:2015 Ed.1
Patch management in the IACS environment
IEC 62443-3-3:2013
System security requirements and security levels
IEC/TR 62443-1-4
IACS security life-cycle and use-case
Development Planned
IEC 62443-2-4:2017 Ed.1.1
Security program requirements for IACS service providers
WIB
IEC 62443-2-5
Implementation guidance for IACS asset owners
Development Planned
ISA99
TS: Technical Specification
TR: Technical Report
CD: Committee Draft
RVC: Result of Voting on CDV
RVD: Result of Voting on FDIS
CDV: Comment Draft for Voting
FDIS: Final Draft of IS
Released Versions
Developing
Development Planned

IEC 62443


Asset Owner
operates
Service Provider
maintains
System Integrator
Integration capabilities
(design and deployment)
Industrial Automation and Control System
Operational and maintenance capabilities
(policies and procedures)
-2-1
-2-3
-2-4
+
Automation Solution
Basic Process
Control System
Safety
Instrumented
System
Complementary
H/W and S/W
-2-4
-3-2
-3-3
IACS environment/project specific
Product Supplier
develops
Control System Product
as a combination of
Supporting
Applications
Embedded
Devices
Network
Components
Host Devices
-4-1
-3-3
-4-2
Independent of IACS environment

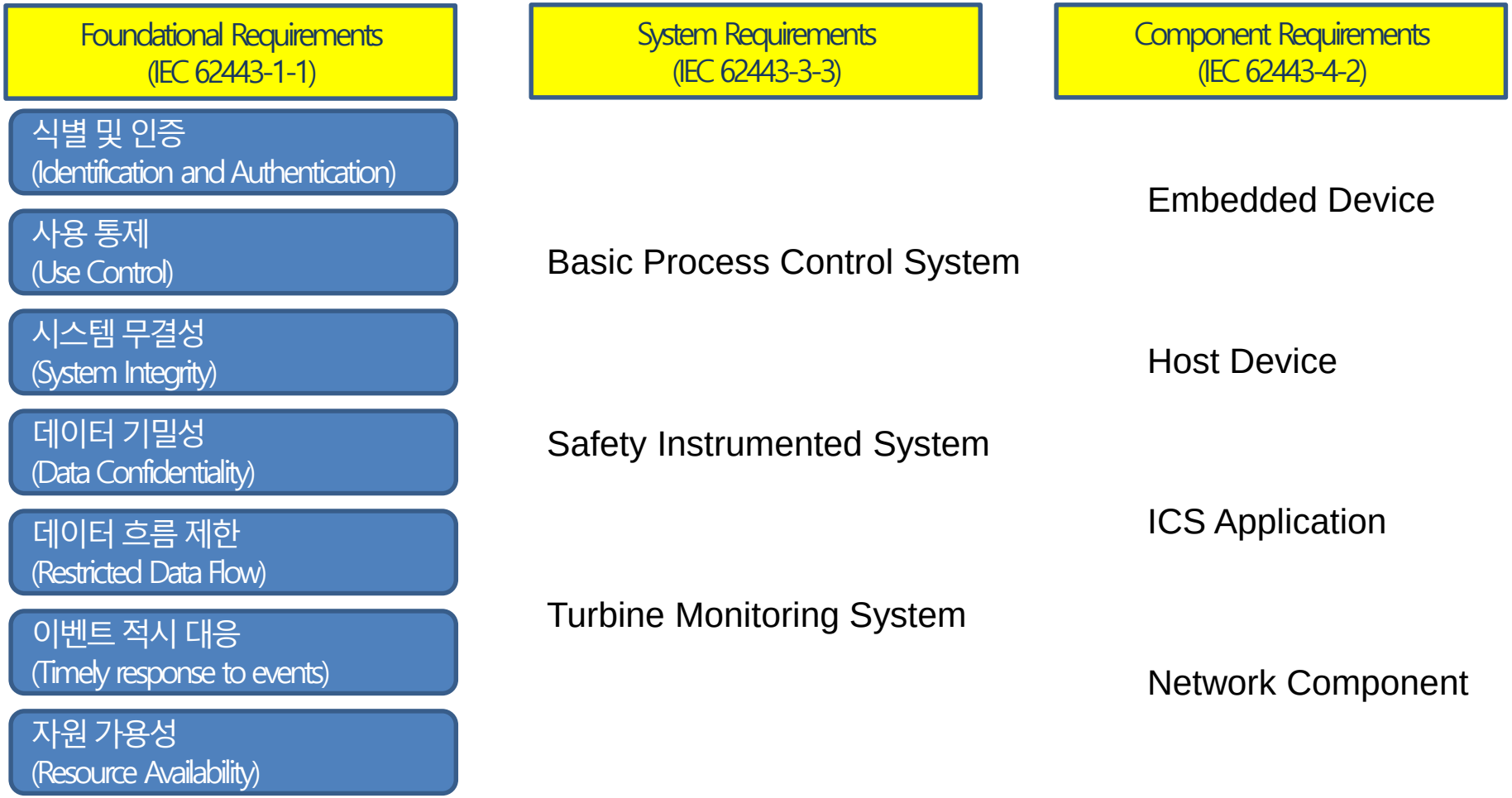
개발자 관점의 스마트디바이스 보안

- Secure Product Development Lifecycle
  - IEC 62443-4-1



개발자 관점의 스마트디바이스 보안

- 디바이스 보호를 위한 기술적 보안요구사항
  - IEC 62443-4-2



개발자 관점의 스마트디바이스 보안

- 디바이스 보호를 위한 기술적 보안요구사항
  - IEC 62443-4-2

Foundational Requirements	Component Requirements
식별 및 인증 (Identification and Authentication)	I&A, Account mgmt. Identifier mgmt., Authenticator mgmt. Wireless access mgmt. Strength password, PKI certificates, Authenticator feedback, Unsuccessful login attempts, System use notification, Access via untrusted networks
사용 통제 (Use Control)	Authorization enforcement, Wireless use control, portable & mobile media, mobile code, session lock, remote session termination, auditable events, audit storage cap.
시스템 무결성 (System Integrity)	Comm. Integrity, Malicious code protection, security function verification, Input validation, Error handling, Protection of audit information
데이터 기밀성 (Data Confidentiality)	Information confidentiality, Information persistence, Use of cryptography
데이터 흐름 제한 (Restricted Data Flow)	Network segmentation, Zone boundary protection, General purpose person-to-person communication restriction, Application partitioning
이벤트 적시 대응 (Timely response to events)	Audit log accessibility, Continuous monitoring
자원 가용성 (Resource Availability)	DoS protection, Resource mgmt., control system backup, Control system restore, emergency power, Network and security configuration settings, least functionality, Control system component inventory

개발자 관점의 스마트디바이스 보안

- 디바이스 보호를 위한 기술적 보안요구사항
  - IEC 62443-4-2 Embedded Device Requirements
    - 제약사항
      - 필수기능(essential function)에 영향을 미치지 않아야 한다.
        * IEC 62443: Health, Safety, Environment, Availability 유지에 필요한 기능/역량 (safety, control, view 등 산업 분야별로 다를 수 있음)
        * EDSA: control, view, command, alarm, 제조사가 정의한 기능
        - » 필수기능에 사용되는 계정 잠금 금지(임시 잠금 포함)
        - » 부인방지를 위해 운전원의 활동을 기록/검증시 응답시간 지연 금지
        - » 고가용성 시스템이 PKI 기능 제공시, CA 오류로 인한 필수기능 영향 금지
        - » 식별 및 인증 기능으로 인해 SIF 방해 금지
        - » 타임스탬프 오류가 포함된 감사 레코드의 필수기능 영향 금지
      - DoS로 인해 SIF 방해가 없어야 한다.
      - 직접적인 보안요구사항 제공이 어려운 경우 보완대책을 마련해야 한다.
      - 최소권한을 원칙으로 한다.
      - 안전한 개발 프로세스(IEC 62443-4-1)에 따라 개발되어야 한다.

개발자 관점의 스마트디바이스 보안

- 디바이스 보호를 위한 기술적 보안요구사항
  - IEC 62443-4-2 Embedded Device Requirements

기반 요구사항(FR)		요구 사항	EDR			
			SL 1	SL 2	SL 3	SL 4
FR 1	**식별 및 인증**(IAC) Identification and authentication control	24	8	13	19	20
FR 2	**사용 통제**(UC) Use control	23	7	15	19	22
FR 3	**시스템 무결성**(SI) System integrity	23	9	18	20	22
FR 4	**데이터 기밀성**(DC) Data confidentiality	5	2	3	5	5
FR 5	**데이터 흐름제한**(RDF) Restricted data flow	7	1	1	1	1
FR 6	**이벤트 적시 대응**(TRE) Timely response to events	3	1	2	3	3
FR 7	**자원 가용성**(RA) Resource availability	11	6	9	10	10
총계		96	34	61	77	83

구분		SL 1	SL 2	SL 3	SL 4
의도	Casual/ coincidental	O			
	Intentional		O	O	O
수단	Simple		O		
	Sophisticated			O	O
자원	Low		O		
	Moderate			O	
	High				O
기술	Generic		O		
	IACS specific			O	O
동기	Low		O		
	Moderate			O	
	High				O

사용자 관점의 스마트디바이스 보안

- 도입 시 보안요구사항을 만족하는 스마트디바이스 도입
  - RFP에 보안요구사항 명시
    - IEC 62443-4-2 컴포넌트 보안요구사항 참조
  - FAT 또는 SAT 시점에 보안요구사항 확인
- 운용 시 스마트디바이스에 대한 보안관리
  - 신규 취약점 발표 정보 모니터링 및 대책 수립
  - 패치 관리 대상으로 스마트디바이스도 고려
    - IEC62443-2-3 참조
  - 스마트디바이스가 제공하는 보안기능의 올바른 설정 적용 후 운용
- 유지보수 시 스마트디바이스 보안관리
  - 유지보수 시 서비스 제공자가 제공할 수 있는 보안수준을 계약서에 명시
    - IEC 62443-2-4 참조
    - 사용자는 IEC 62443-2-4 표준을 이용, 서비스 제공자가 제공할 수 있는 보안수준 결정

시험·평가자 관점의 스마트디바이스 보안

- 시험·평가의 필요성
  - (개발자) 보안요구사항에 적합하게 개발하였는지 확인
  - (사용자) 도입되는 스마트디바이스가 보안요구사항에 적합하도록 개발되었는지 확인
- 시험·평가 체계

ISASecure EDSA/CSA Certification
- 2010년 부터 실시, 최근 IEC 62443 표준 기반으로 전환

이미지 출처 : ISASecure 홈페이지
(https://isasecure.org/en-US/)

IEC 62443 Cyber Certification
- 제품, 개발 프로세스, 시스템, 인력에 대한 인증

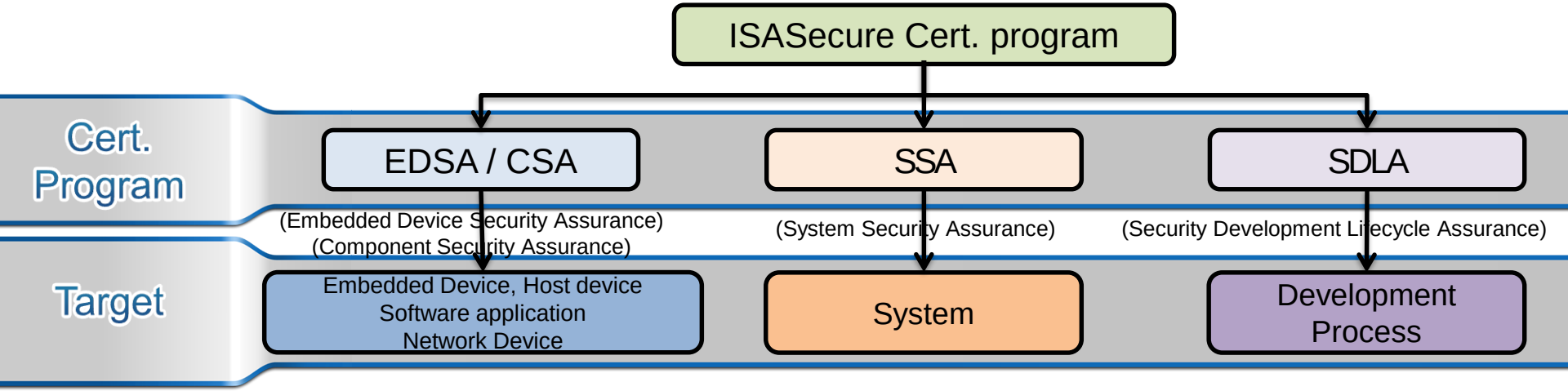
이미지 출처 : exida Certification 웹페이지
(https://www.exida.com/Certification/IEC62443-Cyber-Cert)

IECEE Cyber Security Certification Program
- 제품, 솔루션, 프로세스에 대한 인증

이미지 출처 : Flyer IECEE: International cyber security certification
(https://basecamp.iec.ch/download/flyer-iecee-international-cyber-security-certification-en/)
(UL, DEKRA, TUV NORD 이미지는 각 회사 홈 페이지에서 캡쳐)

시험·평가자 관점의 스마트디바이스 보안

- IEC 62443 표준 기반 시험·인증(예)



Type	개수
Safety Controller/Manager	14
DCS Controller (UOC)	15
Field/Fieldbus Controller	5
PLC	1
RTU	1
Wireless Gateway	1
기타 (Controller)	1
합계	38

#	Supplier	Type	Version	Level	Date
1	Emerson	DeltaV DCS and SIS	14.3	SSA 2 Level 1	2019
2	Honeywell	Experion PKS	R510.1	SSA 2 Level 1	2019

Picture	Supplier ▲	Type	Model	Version	Level	Certification Date
	Emerson Automation Solutions	System	DeltaV DCS and SIS	14.3	SSA 2.0.0 Level 1	3/7/2019
	Honeywell Process Solutions	System	Experion PKS	R510.1	SSA 2.0.0 Level 1	12/30/2019

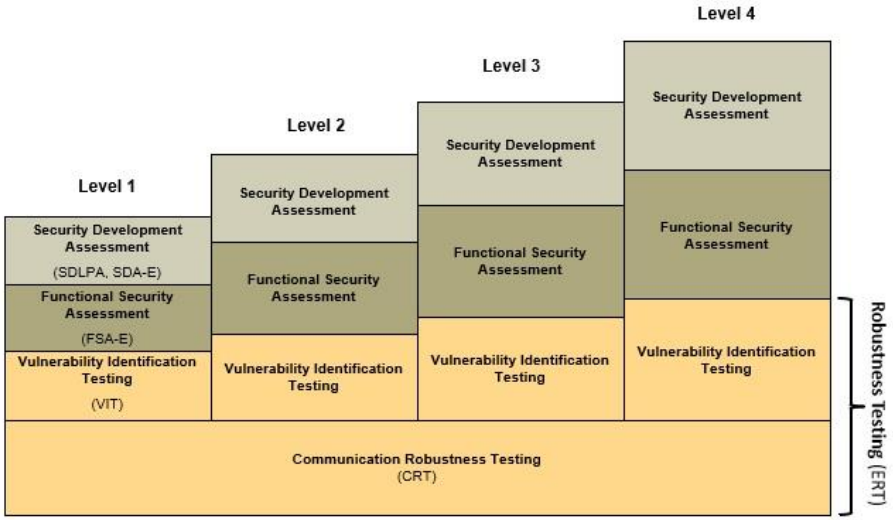
제조사	개수
ABB	1
AVEVA	3
Emerson	2
GE	1
Honeywell	1
Schneider Electric	5
Valmet	1
Yojogawa	1
합계	15

출처 :ISASecure Homepage
(https://isasecure.org/en-US/Certification)

시험·평가자 관점의 스마트디바이스 보안

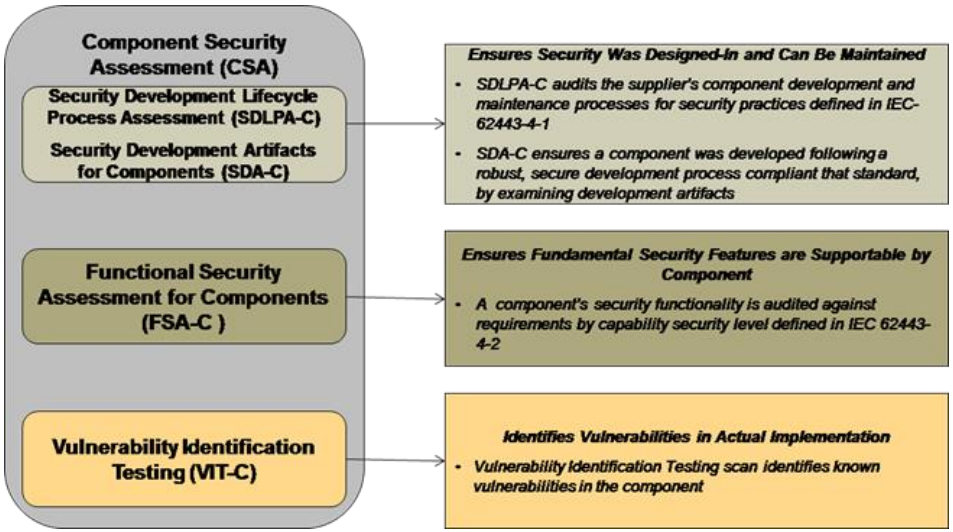
- IEC 62443 표준 기반 스마트디바이스 시험 기준

EDSA 3.0.0(2018.10.10. 이후)



출처 :ISASecure Homepage
(https://isasecure.org/en-US/Certification/IEC-62443-CSA-Certification#tab2)

CSA 1.0.0(2019.8.28. 이후)



출처 :ISASecure Homepage
(https://isasecure.org/en-US/Certification/IEC-62443-CSA-Certification#tab1)

시험·평가자 관점의 스마트디바이스 보안

- IEC 62443 표준 기반 스마트디바이스 시험 기준

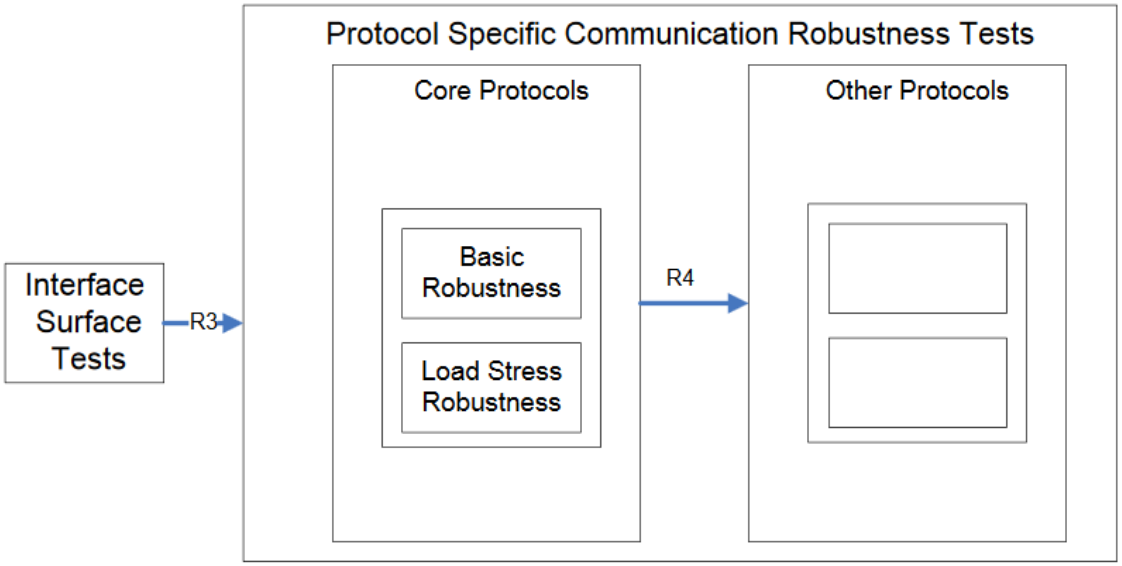
CSA-311 Component Security Assurance - Functional security assessment for components, Version 1.11

Software Application	Embedded Device	Host Device	Network Device	Section	Requirement ID and Reference Name	Capability Security Level
				CCSC - Common Component Security Constraints		
x	x	x	x		FSA-CCSC 1A Support of essential functions - account lock out	1, 2, 3, 4
x	x	x	x		FSA-CCSC 1B Support of essential functions - non-repudiation	1, 2, 3, 4
x	x	x	x		FSA-CCSC 1C Support of essential functions - failure of certificate authority	1, 2, 3, 4
	x				FSA-CCSC 1D Support of essential functions - I&A and SIF initiation	1, 2, 3, 4
	x				FSA-CCSC 1E Support of essential functions - authorization and SIF initiation	1, 2, 3, 4
x	x	x	x		FSA-CCSC 1F Support of essential functions - incorrect timestamps	1, 2, 3, 4
			x		FSA-CCSC 1G Support of essential functions - zone isolation	1, 2, 3, 4
	x				FSA-CCSC 1H Support of essential functions - DoS and SIF initiation	1, 2, 3, 4
x	x	x	x		FSA-CCSC 2 Compensating countermeasures	1, 2, 3
x	x	x	x		FSA-CCSC 3 Least privilege	1, 2, 3, 4
x	x	x	x		FSA-CCSC 4 Software development process	1, 2, 3, 4
				FR 1 - Identification & Authentication Control		
x	x	x	x		FSA-CR 1.1 Human user identification and authentication	1, 2, 3, 4
x	x	x	x		FSA-CR 1.1 RE(1) Unique identification and authentication	2, 3, 4
x	x	x	x		FSA-CR 1.1 RE(2) Multifactor authentication for all interfaces	3, 4
x	x	x	x		FSA-CR 1.2 Software process and device identification and authentication	2, 3, 4
x	x	x	x		FSA-CR 1.2 RE(1) Unique identification and authentication	3, 4
x	x	x	x		FSA-CR 1.3 Account management	1, 2, 3, 4
x	x	x	x		FSA-CR 1.4 Identifier management	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5A Authenticator management - initialize authenticator content	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5B Authenticator management - change default authenticators	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5C Authenticator management - change/refresh all authenticators periodically	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5D Authenticator management - protect authenticators	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5 RE(1) Hardware security for authenticators	3, 4
			x		FSA-NDR 1.6 Wireless access management	1, 2, 3, 4
			x		FSA-NDR 1.6 RE(1) Unique identification and authentication	2, 3, 4
x	x	x	x		FSA-CR 1.7 Strength of password-based authentication	1, 2, 3, 4
x	x	x	x		FSA-CR 1.7 RE(1) Password generation and lifetime restrictions for human users	3, 4
x	x	x	x		FSA-CR 1.7 RE(2) Password lifetime restrictions for all users (human, software process, or device)	4
x	x	x	x		FSA-CR 1.8 Public key infrastructure (PKI) certificates	2, 3, 4

출처 :ISASecure Homepage
(https:/https://isasecure.org/en-US/Documents/Authentication-Required-Specifications/CSA-1-0-0/CSA-311-Functional-security-assessment-for-compone)

시험·평가자 관점의 스마트디바이스 보안

- IEC 62443 표준 기반 스마트디바이스 시험 기준



Requirement ERT.R8 – Submission of essential functions

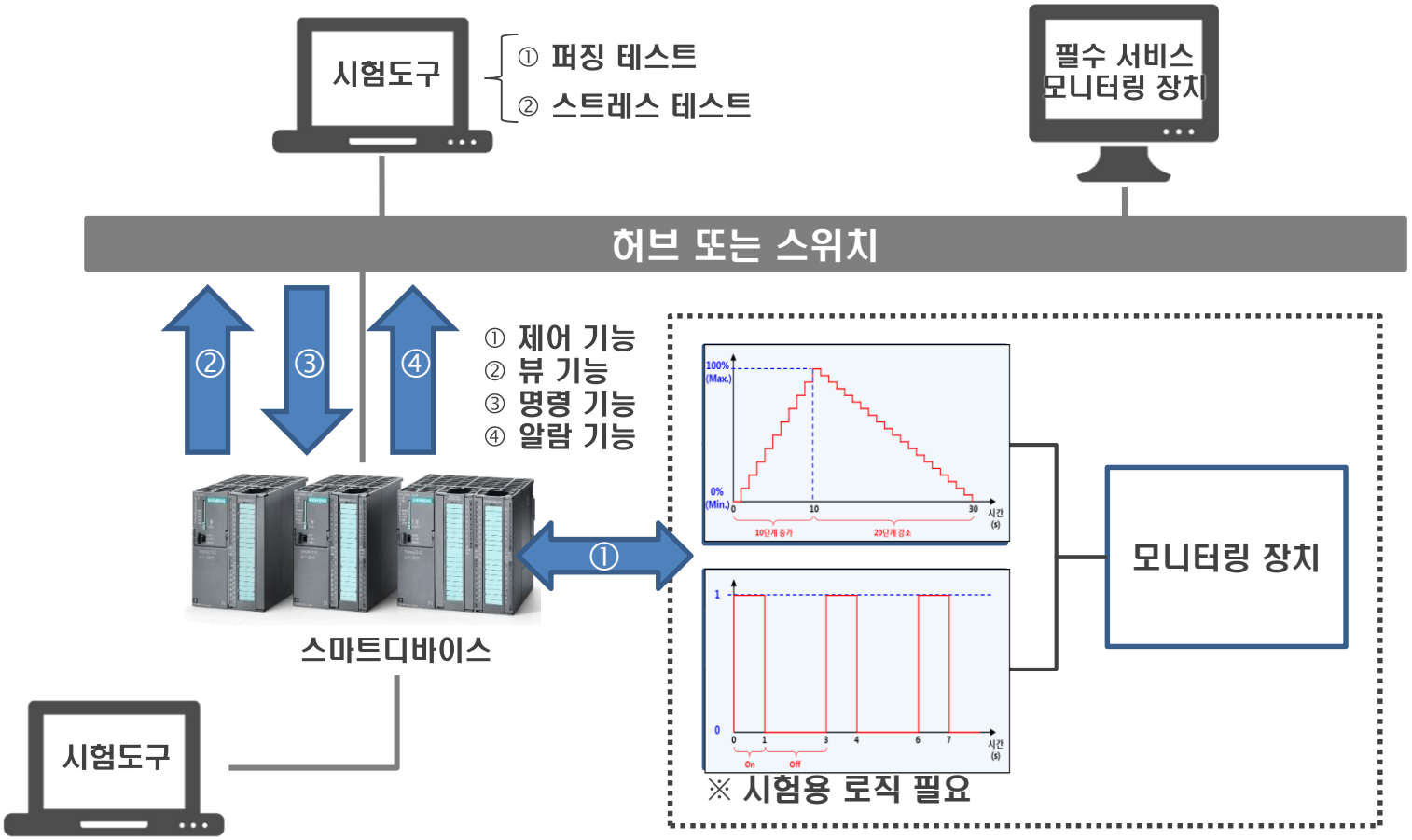
A certification applicant SHALL indicate which essential functions the embedded device has the capability of performing from the following list:

1. The control function
2. Process view
3. Process command
4. Process alarm
5. Peer-to-peer control communication
6. Process history

NOTE 1 For items 1 through 4, if the embedded device has the capability to perform these functions, then they must be included in the submittal. Items 5 and 6 may be submitted as essential functions by the certification applicant.

출처 :EDSA-310 Requirements for Embedded Device Robustness Testing
(https://isasecure.org/en-US/Certification/IEC-62443-CSA-Certification#tab2)

시험·평가자 관점의 스마트디바이스 보안



제어 기능	• 출력의 지연 여부 측정 • 제어 H/W의 지연 허용 시간/측정 오차 고려
명령 기능	• 제어 H/W에게 일정 시간 간격으로 명령어 전송 후, 모니터의 출력값 확인
뷰 기능	• HMI 스크린을 통해서 불연속 구간이 일정 시간 미만으로 발생하는지 확인
알람 기능	• HMI를 통해서 일정 시간 마다 알람 발생하도록 설정 후, 알람 발생 여부 확인

요약

- 산업용 스마트디바이스에 보안요구사항 반영
  - 개발자는 스마트디바이스에 대한 보안위협을 분석하고 보안기능을 반영하여 개발 ➔ 해외 수출
  - 사용자는 도입 시 스마트디바이스에 대한 보안요구사항을 제시하고 확인 ➔ 구축 단계부터 안전한 스마트인프라 구현
- 국내 스마트디바이스 보안 강화 방안
  - 산업용 스마트디바이스 개발사 대상 ICS 보안위협과 보안 강화 필요성 인식교육 및 국제 보안표준 기술 교육
  - 산업용 스마트디바이스 보안기능을 시험·평가할 수 있는 역량 확보
  - 보안기능이 내재된 산업용 스마트디바이스를 도입하는 사용자에게 인센티브 제공