2020 IT 21
Global Conference
Digital New Deal
Technology Essentials
디지털 뉴딜 기술 핵심

산업제어시스템 보안요구사항 – 기반시설을 중심으로 –

김신규 팀장 (ETRI 부설연구소)

[요약문]

우리나라는 국가적으로 중요한 기반시설을 '정보통신기반 보호법'을 통해 전자적 침해로부터 보호하기 위한 체계를 구축하고 운영하고 있다. 특히, 보호대상 기반시설 중 산업제어시스템의 경우 교통시설, 에너지·수자원 시설 등 국민의 생활과 밀접한 시설을 운영하는 데 활용되고 있어 중요성이 높다. 하지만, 이러한 시설의 취약점을 점검하는 기준인 '취약점 분석·평가 기준'이 지난 2013년 개정된 이후 변화가 없어, 최신 해킹 기법, 제어시스템 운용방식의 변화 등을 반영하지 못하고 있다. 좀 더 현실적이고, 좀 더 안전하게 산업제어시스템을 보호하기 위해서는 기준의 변경이 필요하다. 본 발표에서는 산업제어시스템에 대한 취약점 분석·평가 기준(보안요구사항)의 변화 방향에 대해 제안하고자 한다.

[발표자 약력]

2000년 연세대학교 기계전자공학부 학사
2002년 연세대학교 컴퓨터산업시스템공학과 공학석사
2014년 연세대학교 컴퓨터산업시스템공학과 공학박사
2003년~현재 국가보안기술연구소 팀장
관심분야 : 제어시스템 보안, 기반보호, CPS 보안, 취약점 분석, 보안위협 탐지 등

산업제어시스템 보안요구사항
- 기반시설 중심-

2020. 9.

ETRI부설연구소

목 차

1. 주요정보통신기반시설 산업제어시스템(1/3)

정보통신기반 보호법

[시행 2020. 6. 11] [법률 제16758호, 2019. 12. 10, 일부개정]

과학기술정보통신부(사이버침해대응과) 044-202-6465 ,6466

제1장 총칙

제1조(목적) 이 법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2007. 12. 21., 2020. 6. 9.>

1. "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어 관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 말한다.
2. "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.
3. "침해사고"란 전자적 침해행위로 인하여 발생한 사태를 말한다.

제3장 주요정보통신기반시설의 지정 및 취약점 분석

제8조(주요정보통신기반시설의 지정 등) ①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. <개정 2019. 12. 10., 2020. 6. 9.>

1. 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2. 제1호에 따른 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3. 다른 정보통신기반시설과의 상호연계성
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5. 침해사고의 발생가능성 또는 그 복구의 용이성

1. 주요정보통신기반시설 산업제어시스템(2/3)

제7조(주요정보통신기반시설의 보호지원) ①관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 과학기술정보통신부장관과 국가정보원장등 또는 필요한 경우 대통령령으로 정하는 전문기관의 장에게 다음 각 호의 업무에 대한 기술적 지원을 요청할 수 있다. <개정 2007. 12. 21., 2008. 2. 29., 2013. 3. 23., 2017. 7. 26., 2020. 6. 9.>

1. 주요정보통신기반시설보호대책의 수립
2. 주요정보통신기반시설의 침해사고 예방 및 복구
3. 제11조에 따른 보호조치 명령·권고의 이행

②국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. <개정 2007. 12. 21.>

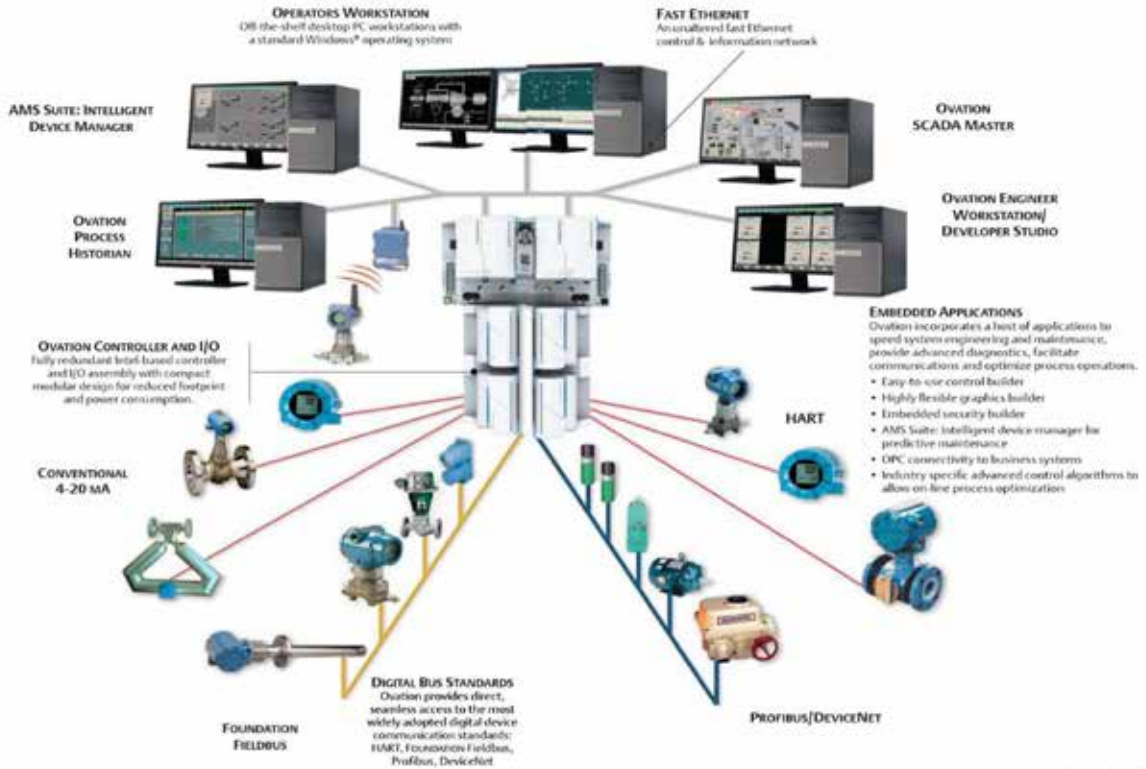
1. 도로·철도·지하철·공항·항만 등 주요 교통시설
2. 전력, 가스, 석유 등 에너지·수자원 시설
3. 방송중계·국가지도통신망 시설
4. 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설

③국가정보원장은 제1항 및 제2항에도 불구하고 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니된다. <개정 2007. 12. 21., 2020. 6. 9.>

1. 주요정보통신기반시설 산업제어시스템(3/3)

주요정보통신기반시설 지정 현황 (2019년 12월 기준, 2020 국가정보보호백서)
공공 265개 시설(141개 기관), 민간 149개 시설(91개 기관)

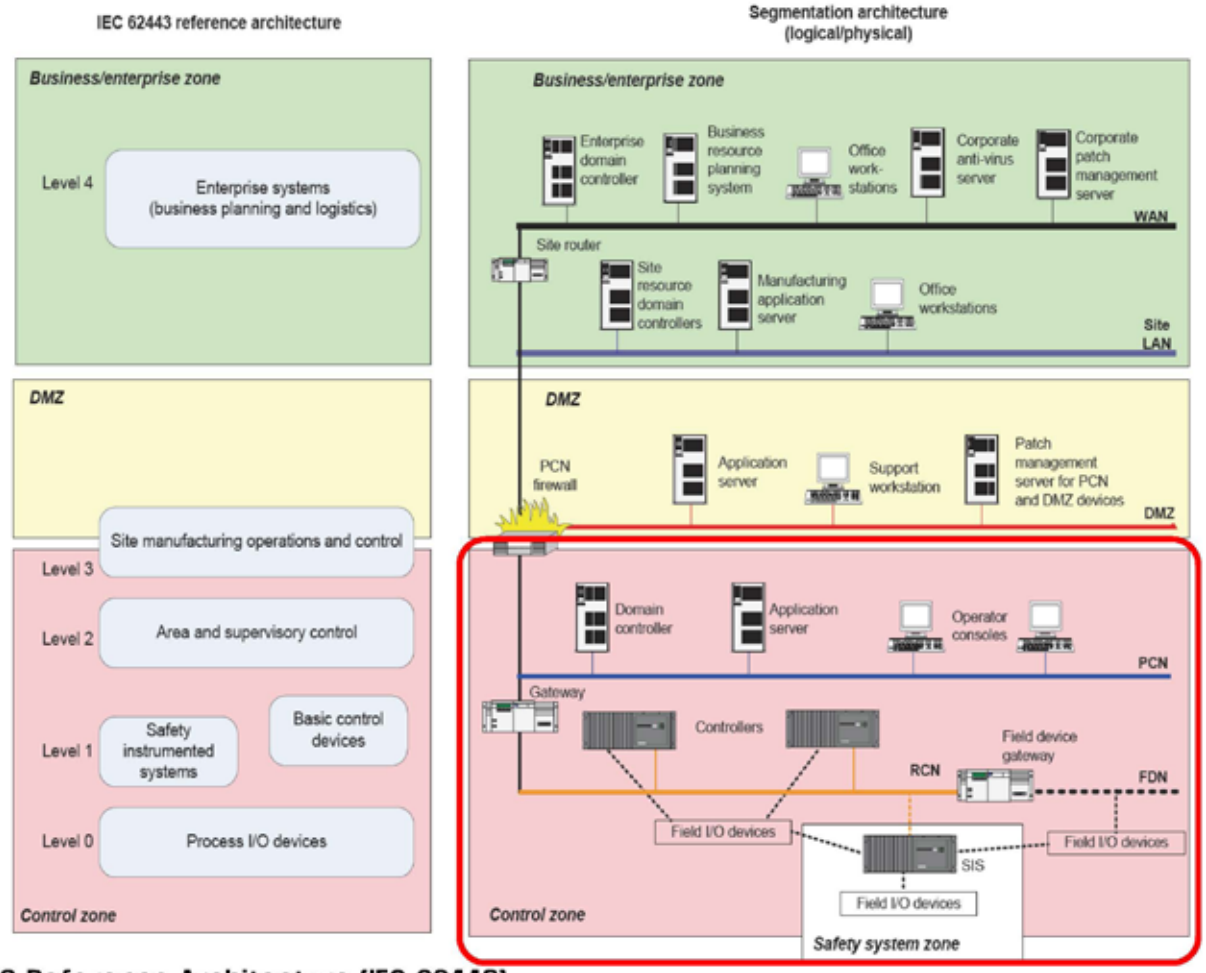
❑ 산업제어시스템 : ICS, SCADA, DCS, PLC



From Emerson Ovation

2. 배경 및 필요성

❑ 산업제어시스템



ICS Reference Architecture (IEC 62443)

IT System

General purpose O/S

Internet Protocol(TCP/IP)

Data Processing centric

ICS

RTOS based embedded system

Industrial Protocol

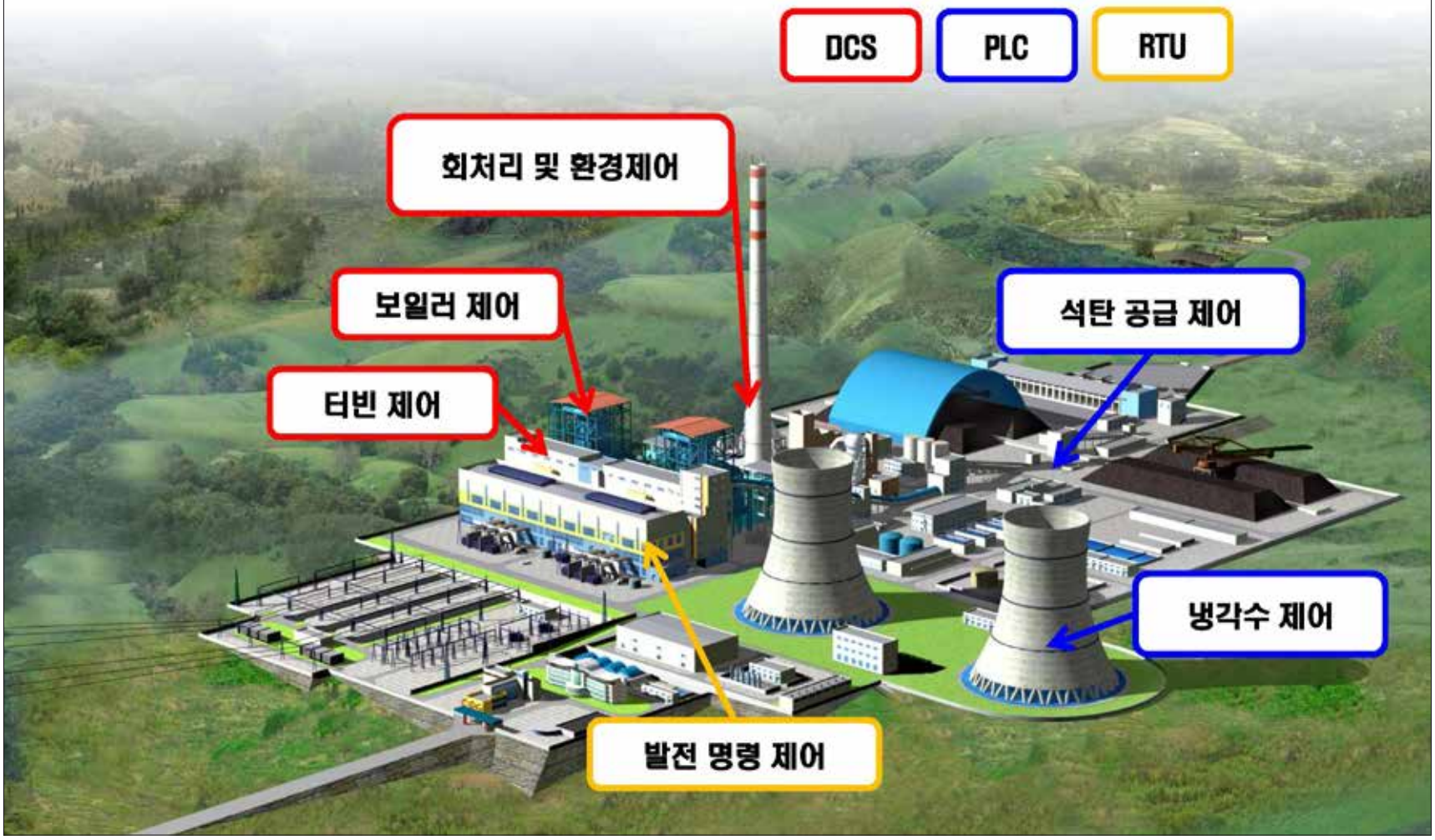
Industrial Process centric

- Monitor status
- Control physical devices

6

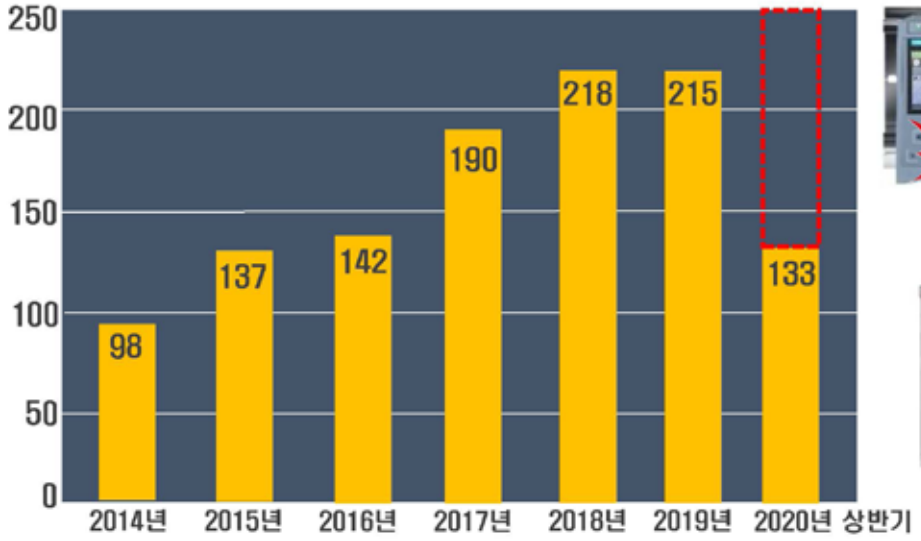
2. 배경 및 필요성

❑ 석탄화력발전소



2. 배경 및 필요성

❑ 산업제어시스템 취약점 지속 발견 및 인터넷 공개



ICS-CERT 발표 제어시스템 취약점 경고 건수
(CISA/ICS-CERT Advisories)

XXX社 PLC

조작된 패킷이 TCP 102번 포트로 전달되면 자동 재부팅
(ICSA-16-040-02)

YYY社 IED

IED 관리도구에 저장되는 패스워드 보호에 취약한 해쉬함수를 사용하여 패스워드가 쉽게 노출
(ICSA-16-152-02)

ZZZ社 IED

펌웨어의 패스워드를 추출하여 원격 접속 가능
(ICSA-17-117-01)

2. 배경 및 필요성

2010.7 — Stuxnet – 이란 나탄즈

- 제어시스템 최초의 악성코드 – 원전 시설의 PLC 감염
- Siemens PLC로 운전되는 원심분리기 1,000 여개 파괴

2015.12 — BlackEnergy 3 – 우크라이나 키예프

- 프리카파트야오블네르고, 키보블레네르고 社 운영의 30개 변전소 오프라인 발생으로 8만명에 영향
- HMI 시스템(PC) 이용 정전명령 실행 후 파괴, 프로토콜 컨버터 Firmware 감염, UPS 전원 차단

2016.12 — Industroyer/Crashoverride – 우크라이나 키예프

- 우크레네르고社 운영의 피브니치나(변전소) 전력망 중단
- ABB PCM600(IED) 삭제, Siemens SIPROTEC 4(IED) 서비스 거부 공격

2017.8 — TRISIS/TRITON 악성코드 – 사우디 석유공장

- 슈나이더사 안전계장시스템을 표적으로 한 제어기기 특화 악성코드 발견
- 공급망 공격(Supply Chain Attack)을 통해 제어시스템에 침투(추정)하여 제어로직 변경

슈나이더社 Triconex 안전계장시스템

2019.8 — LockerGoga 랜섬웨어 – 노르웨이

- 노르웨이 Norsk Hydro(알루미늄 제조회사)사의 생산 공정 중단
- 회사 내부 네트워크를 통해 확산하는 새로운 형태의 랜섬웨어로 시스템 내 파일 암호화

GE社 Proficy

Honeywell社 HMIWeb

2020.4 — EKANSE/SNAKE 랜섬웨어

- ICS를 타켓으로 하는 랜섬웨어 발견
- GE사 Proficy, Honeywell 사 HMIWeb 등의 서비스를 중단시키고 파일을 암호화

3. 취약점 분석 · 평가 항목 현황

✓ 주요정보통신기반시설 취약점 분석 · 평가 기준 (2013. 8. 8.)

✓ 기본항목 16개

마. 제어시스템

점검분류	번호	취약점 점검 항목	등급
계정 관리	C-1	제어시스템 운영, 관리를 위한 계정이 타 사용자와 공유되지 않음	상
	C-2	ID/PW, 접속경로, 인증서 등이 하드코딩되지 않음	상
	C-3	제어시스템 운영, 관리를 위한 계정의 로그인, 사용 기록 저장	상
패치 관리	C-4	제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 테스트 등의 절차 수립	상
접근 통제	C-5	제어시스템 운영자의 운영 권한은 제한된 범위 및 명령으로 제한	상
	C-6	제어시스템은 업무망, 인터넷 망과 물리적으로 분리	상
	C-7	제어 네트워크 외부와 자료인계시 물리적 일방향 환경을 구축하여 제어 네트워크로의 침입을 근본적으로 차단	상
	C-8	제어 네트워크에 무선인터넷, 테더링, 외부 유선망 인걸 등의 외부망 인걸을 제한하고 점검	상
	C-9	제어 네트워크에 비인가된 시스템에 대한 인걸 및 접속 차단	상
보안 관리	C-10	제어시스템 구성도, 운용 매뉴얼, 비상조치 절차서 등을 작성하고 최신으로 관리	상
	C-11	제어시스템에서의 USB 사용을 금지하고, 사용시 USB 등의 이동형 저장매체 사용 통제	상
	C-12	제어명령에 대한 위변조 방지 대책 적용	상
	C-13	제어명령 replay 공격에 대한 방지 대책 적용	상
	C-14	제어시스템 개발자, 운영자, 관리자에 대한 접근권한 분리	상
	C-15	제어시스템, 제어기기에 (vendor default) 은닉서비스 및 취약한서비스가 없도록 설정	상
	C-16	제어프로그램의 입력창에 비정상적인 특정값을 입력할 시 사전에 정의한 에러 메시지가 출력되도록 하여 시스템 중요정보가 노출되지 않도록 설정	상

✓ 선택항목 6개

마. 제어시스템

점검분류	번호	취약점 점검 항목	등급
보안 관리	CS-17	정보시스템에 대한 정책과 별도로 제어시스템에 대한 정보보안 정책, 지침이 수립되어 있는가?	중
	CS-18	비인가자 또는 인증과정이 없이 제어시스템, 제어기기에 대한 환경 설정이 가능하지 않도록 되어있는가?	중
	CS-19	제어시스템 및 운영시스템은 제어를 위한 목적으로만 사용되도록 다른 기능 및 서비스를 제거하였는가?	중
	CS-20	운영에 있어 사용가능한 제어명령 및 안전한 제어를 위한 파라미터의 범위를 제한하고 있는가?	중
	CS-21	제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축하였는가?	중
	CS-22	제어 네트워크는 각각의 세부망으로 세분화하고 제어시스템 운영에 필요한 네트워크, 시스템간으로 통신을 제한하고 있는가?	중

현황 반영 필요

적용사례 적음

취약점 분석·평가 어려움

최근 트렌드 복구대응!

가용성이 중요!

10

4. 산업제어시스템 보안요구사항 (1/12)

항목의 세분화

As-Is

점검 항목 (22개 항목)
계정관리
패치관리
접근통제
보안관리

To-Be

점검 항목 (50개 항목)
계정관리
패치관리
네트워크 접근통제
보안관리
서비스 관리
물리적 접근통제
보안위협 탐지
복구대응
교육훈련

4. 산업제어시스템 보안요구사항 (2/12)

용어 정리

- 제어시스템 : 원격 감시 및 제어를 수행하는 시스템 전체
- 제어 네트워크 : 제어시스템을 운용하기 위해 운영센터, 서버실, 현장 등에 구축된 데이터 통신 네트워크
- 제어관련기기 : 제어시스템 내 DCS, PLC, RTU, IED 등의 제어를 수행하는 기기와 통신 기능이 있는 센서, 엑추에이터
- 제어시스템 구성요소 : 제어시스템 구성하는 H/W, S/W, 네트워크 장비, 제어관련기기 등의 장비

4. 산업제어시스템 보안요구사항 (3/12)

❑ 계정관리 (6개)

분류	점검항목	중요도
계정 관리	제어시스템 운영, 관리를 위한 계정이 타 사용자와 공유되지 않음	상
	ID/PW, 접속경로, 인증서 등이 하드코딩되지 않음	상
	제어시스템 운영, 관리를 위한 계정의 로그인, 사용 기록 저장	상

분류	취약점 점검 항목	등급
계정 관리	계정기능이 있는 제어시스템 구성요소에 대해 계정을 설정하여 사용	상
	제어시스템 계정의 로그인/로그아웃, 사용명령 등 사용기록을 저장	상
	제어시스템 계정입력시 패스워드 마스킹 처리, 입력값 에러발생시 제공정보 제한 수행	상
	제어시스템 계정을 관리, 운영, 유지보수 등 용도에 따라 분리하고 운용	중
	제어시스템 계정에 대해 관리, 운영, 유지보수 등 용도에 맞는 최소 권한 부여	중
	제어시스템 운전원 별 유일 계정 부여 또는 시간별 사용자 기록 유지	중

4. 산업제어시스템 보안요구사항 (4/12)

❑ 패치관리 (5개)

분류	점검항목	중요도
패치 관리	제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 테스트 등의 절차 수립	상

분류	취약점 점검 항목	등급
패치 관리	제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 제조사 협력방안, 테스트 방안 등의 절차 수립	상
	외부 업체, 인터넷을 통한 다운로드 등의 경로로 반입된 각종 패치·업데이트 파일에 대해 무결성 검증 및 클린 PC를 통한 악성코드 존재 여부 검사 수행	상
	제어시스템 구성요소의 알려진 취약점에 대해 보안패치 적용 또는 상응하는 대응책 적용	상
	운영체제, 응용프로그램, 펌웨어 등에 대해 안정성이 확인된 최신 버전의 소프트웨어 사용 및 기술지원이 종료된 제품 미사용	중
	제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축	하

4. 산업제어시스템 보안요구사항 (5/12)

❑ 네트워크 접근통제

분류	점검항목	중요도
접근 통제	제어시스템 운영자의 운영 권한은 제한된 범위 및 명령으로 제한	상
	제어시스템은 업무망, 인터넷 망과 물리적으로 분리	상
	제어 네트워크 외부와 자료연계 시 물리적 일방향 환경을 구축하여 제어 네트워크로의 침입을 근본적으로 차단	상
	제어 네트워크에 무선인터넷, 테더링, 외부망등 연결 등의 외부망 연결을 제한하고 점검	상
	제어 네트워크에 비인가된 시스템에 대한 연결 및 접속 차단	상

4. 산업제어시스템 보안요구사항 (6/12)

❑ 네트워크 접근통제 (6개)

분류	취약점 점검 항목	등급
네트워크 접근통제	제어 네트워크는 업무망, 인터넷, CCTV망 등 외부망과 물리적으로 분리하여 사용	상
	제어 네트워크 외부로 자료전달 시 물리적 일방향 자료전달 환경을 구축하여 외부에서 제어 네트워크로의 침입을 차단	상
	제어 네트워크에 무선인터넷, 테더링, 외부 유선망 등의 외부망 연결을 제한하고 주기적으로 점검	상
	제어 네트워크에 비인가된 시스템/기기에 대한 연결 및 접속을 차단	상
	물리적 일방향 자료전달 환경의 올바른 동작 및 운용에 대한 주기적인 점검 수행	상
	제어 네트워크를 용도에 따라 세분화하고, 접근제어를 수행하여 제어시스템 운영에 필요한 네트워크, 시스템 간의 통신만 허용	중

4. 산업제어시스템 보안요구사항 (7/12)

❑ 보안관리

분류	점검항목	중요도
보안관리	제어시스템 구성도, 운용 매뉴얼, 비상조치 절차서 등을 작성하고 최신으로 관리	상
	제어시스템에서의 USB 사용을 금지하고, 사용시 USB 등의 이동형 저장매체 사용 통제	상
	제어명령에 대한 위변조 방지 대책 적용	상
	제어명령 replay 공격에 대한 방지 대책 적용	상
	제어시스템 개발자, 운영자, 관리자에 대한 접근권한 분리	상
	제어프로그램의 입력창에 비정상적인 특정값을 입력할 시 사전에 정의한 에러메시지가 출력되도록 하여 시스템 중요정보가 노출되지 않도록 설정	상
	정보시스템에 대한 정책과 별도로 제어시스템에 대한 정보보안 정책, 지침이 수립되어 있는가?	중
	제어시스템 및 운영 시스템은 제어를 위한 목적으로만 사용되도록 다른 기능 및 서비스를 제거하였는가?	중
	운영에 있어 사용가능한 제어명령 및 안전한 제어를 위한 파라미터의 범위를 제한하고 있는가?	중
	제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축하였는가?	중
	제어 네트워크는 각각의 세부망으로 세분화하고 제어시스템 운영에 필요한 네트워크, 시스템 간으로 통신을 제한하고 있는가?	중

4. 산업제어시스템 보안요구사항 (8/12)

❑ 보안관리 (7개)

분류	취약점 점검 항목	등급
보안 관리	제어시스템 구성요소에 대한 자산정보(담당자, 펌웨어 버전, 설치 SW 등)를 항상 최신으로 유지관리	상
	제어시스템 구성요소가 설치된 장소를 보호구역으로 설정	상
	제어시스템에서 USB 등 이동형 저장매체 사용해야 하는 경우, 사전정의된 정책에 따라 사용	상
	제어 네트워크에 연결되는 외부 정보통신기기 반·출입시 클린존 통과, 관리대장 작성 등 관리절차 마련	상
	제어시스템의 특성을 반영한 정보보안 정책, 지침을 수립	중
	제어시스템 운영업무에 대해 표준업무절차서를 작성하고 적용	중
	제어시스템 유지보수를 위한 전용 장비(노트북 등)를 마련하고 관련 정책을 시행	하

4. 산업제어시스템 보안요구사항 (9/12)

❑ 서비스 관리 (9개)

분류	점검항목	중요도
보안 관리	제어시스템, 제어기기에 (vendor default)은닉 서비스 및 취약한 서비스가 없도록 설정	상
	비인가자 또는 인증과정이 없는 제어시스템, 제어기기에 대한 환경 설정이 가능하지 않도록 되어 있는가?	중

분류	취약점 점검 항목	등급
서비스 관리	제어시스템 구성요소에 대한 시각 동기화 수행	상
	제어시스템에 불필요한 서비스 및 취약한 서비스 제거 또는 보완대책 수행	상
	제어시스템 구성요소에 대한 관리자 페이지 운영 시 이에 대한 접근통제(사전인가 접근만 허용) 수행	중
	제어시스템 내 파일/디렉토리 접근권한 및 신뢰관계를 적절히 부여	중
	제어시스템 내 제어와 직접적인 관련이 없는 불필요 프로그램 삭제	중
	제어시스템 운영 정보, 제어명령 등 중요정보에 대한 위변조 및 replay 공격 방지 대책 적용	중
	제어시스템 내 전달되는 제어명령 및 파라미터의 정상 범위를 식별하고 관리	하
	제어시스템 내 사용자 통신세션에 대해 세션타임아웃 적용	하
	GPS 스푸핑/재밍 공격 등 시각동기화 서비스를 교란하기 위한 공격에 대비한 보안조치 수행	하

4. 산업제어시스템 보안요구사항 (10/12)

❑ 물리적 접근통제 (2개)

분류	취약점 점검 항목	등급
물리적 접근 통제	제어시스템에 대해 네트워크 포트, USB 포트 등 외부 연결 접점에 대해 허가받은 사항을 제외하고 모두 물리적 또는 논리적으로 차단	상
	제어시스템 구성요소를 물리적으로 보호할 수 있는 조치 적용(잠금장치가 있는 함체, 랙, 수납책상 등)	중

❑ 보안위협탐지 (2개)

분류	취약점 점검 항목	등급
보안 위협 탐지	백신 프로그램 설치가 가능한 제어시스템 구성요소에 대해 악성코드 감염 및 차단을 위한 백신 프로그램 설치	상
	이상 트래픽 발생 탐지 등 제어시스템 내의 보안 관리를 위해 적합한 침입탐지시스템 등을 구축 및 운용하고, 구축된 보안 솔루션 및 보안장비에서 탐지한 보안 이벤트에 대해 모니터링 수행	하

4. 산업제어시스템 보안요구사항 (11/12)

❑ 복구대응 (12개)

분류	취약점 점검 항목	등급
복구 대응	제어시스템 대상 사이버 위기대응 매뉴얼을 수립	상
	제어시스템 대상 사이버 위기대응 훈련을 정기적으로 시행	상
	제어시스템 침해사고 대응을 위한 제어시스템 설정, 중요 데이터 등을 백업 및 관리	상
	제어시스템의 장애발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 수립	중
	제어시스템의 장애발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련을 정기적으로 시행	중
	제어시스템 조작불능에 대비하여 수작업 운전 매뉴얼 작성 및 교육훈련 시행	중
	제어시스템의 각종 이벤트에 대한 로그를 관리하기 위한 중앙집중식 로그 관리 수행	하
	제어시스템 구성요소의 기본 형상을 설정하고 변경 및 업데이트 시 형상관리 수행	하
	제어시스템 주요 장비 및 제어 네트워크 장비에 대해 이중화	하
	제어시스템 보호를 위한 화재탐지 설비 및 화재 진압설비를 구비	하
	제어시스템 보호를 위한 누수탐지 설비 및 침수 대응 장비 구비	하
	제어시스템에 대하여 정기적으로 사이버 위협 시나리오를 식별하고, 완화 방안 수립	하

4. 산업제어시스템 보안요구사항 (12/12)

❑ 교육훈련 (1개)

분류	취약점 점검 항목	등급
교육 훈련	제어시스템 운전원, 관리자, 유지보수인력, 보안인력에 대해 각 직무별 직무교육을 정기적으로실시	하

5. 제어관련기기 보안요구사항

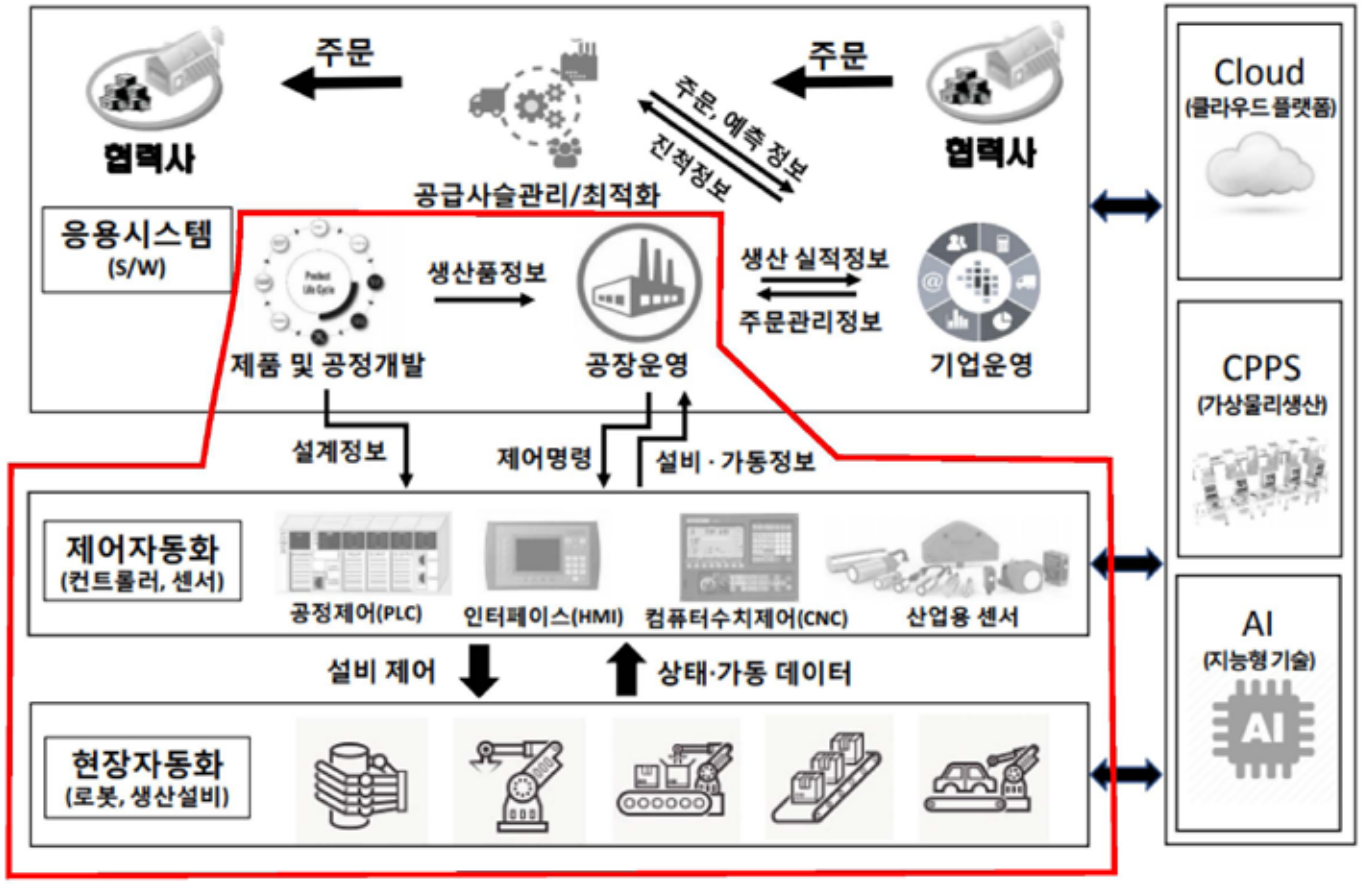
❑ KS X IEC 62443-4-2:2019

IEC 62443-4-2

- 식별 및 인증 (Identification and Authentication)
- 사용 통제 (Use Control)
- 시스템 무결성 (System Integrity)
- 데이터 기밀성 (Data Confidentiality)
- 데이터 흐름 제한 (Restricted data flow)
- 이벤트 적시 대응 (Timely response to events)
- 자원 가용성 (Resource Availability)

6. 스마트 공장 활용

❑ 스마트 공장 참조모델



From 스마트공장 추진단


Thank
You
Dank Je
Blagodaram
Ngiyabonga
Dziekuje
Juspaxar
நன்றி
Ua Tsaug Rau Koj
Děkuji
Suksama
Nuwun
Bedankt
Dakujem
Nirringrazzjak
Grazas
धन्यवाद
Hvala
Welalin
Ji Ou Mèsi
Maüruuru
Biyan
Chokrane
Arigato
Gracias
cảm ơn bạn
Kia Ora
Kop Khun Khap
Diolch i
Tack
Grazie
Mochchakkeram
Paldies
Tingki
Gratias Tibi
Obrigado
ありがとう
Djiere Dieuf