산업 기반 시설 보안 과정

보안프로젝트 조정원 대표
(ngnicky@naver.com)

강사 소개

現 보안프로젝트 대표, 중앙대학교 외래교수, 서울디지털대학교 외래교수

前 에이쓰리시큐리티, KT하이텔, KB증권

연구 분야: 취약점 분석, 오픈소스도구개발

강의 분야: 모의해킹 실무, 모바일 취약점 진단, MSF 침투시험, 개인정보

강의 경력 : 現 대기업, 공공기간 등 위탁교육 강의

現 IT보안 취업준비생 대상 보안교육 강의

보안프로젝트 IT보안 강의 총괄 및 강의

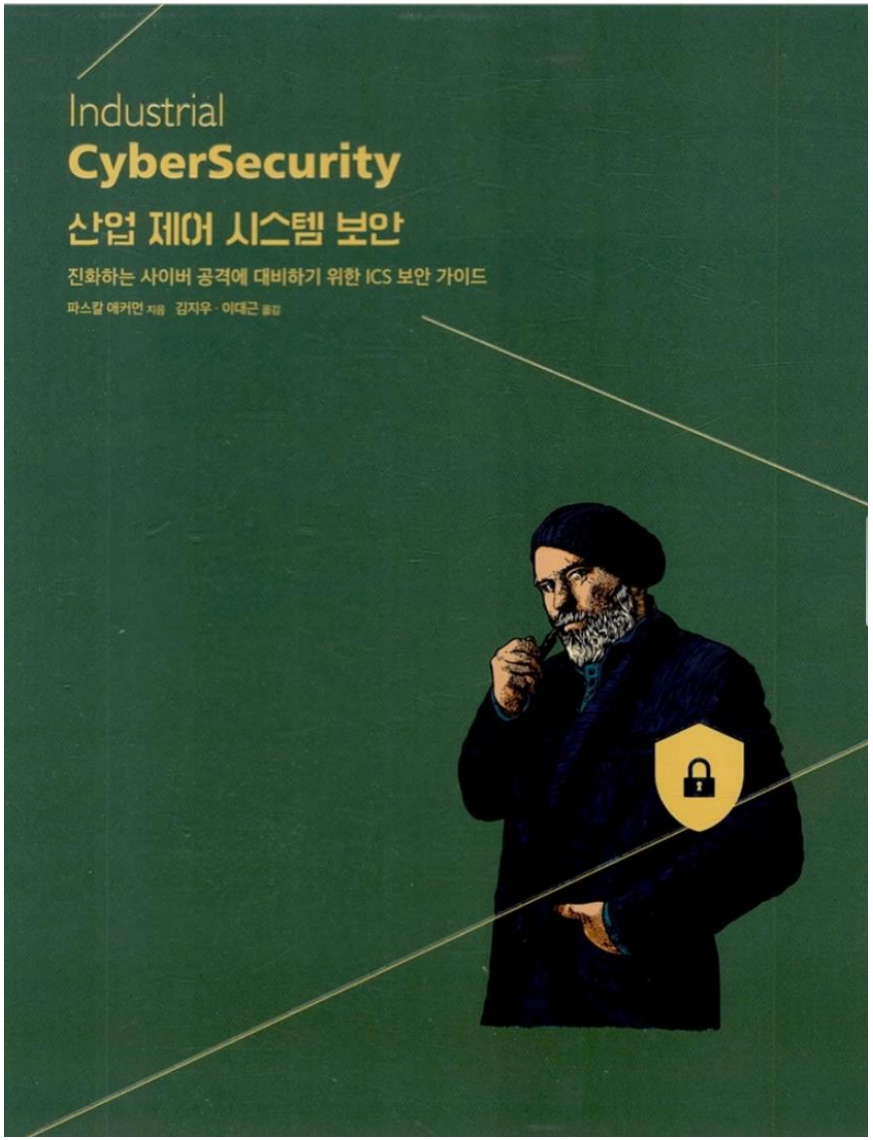
저서: (저) 모의해킹이란 무엇인가, (저) 실무자가 말하는 모의해킹

(공저) 칼리리눅스와 백트랙을 활용한 모의해킹, Nmap NSE를 활용한 취약점 진단, 비박스를 활용한 웹해킹 완벽 실습, 파이썬 오픈소스도구를 활용한 악성코드 분석 등 25여권 저술

이 강의에서 배우게 될 내용

- 산업 제어 시스템 인프라 구조와 프로토콜 이해
- 산업 제어 시스템 보안 위협 사례
- 산업 제어 시스템 가상 환경 구축
- 산업 제어 시스템 프로토콜 정보 수집 및 취약점 분석
- OSINT를 활용한 보안 위협 모니터링 구축
- IoT 환경 애뮬레이터를 통한 시리얼 통신 이해
- 내부 시스템 보안 위협과 대응 방안 제시
- 산업 제어 시스템 보안 위협 평가
- 모바일 앱 취약점 진단 (환경에 따라 결정)

교재 소개


Industrial
CyberSecurity
산업 제어 시스템 보안
진화하는 사이버 공격에 대비하기 위한 ICS 보안 가이드
파스칼 에커먼 지음 김지우 · 이대근 옮김

산업 제어 시스템 이해

산업 제어 시스템

산업 제어 시스템 구조

- **ICS**(Industry Control System): 다양한 자동화 시스템과 관련 장비에 사용되는 포괄적인 용어
  - **ICS는 '정보기술 (IT)'과 '운영기술 (OT)'로 나눌 수 있다**. IT 영역은 일반 사무실의 네트워크와 유사하다.
  - 실제로 해당 영역은 설비가 아닌 일반 사무적 용도를 위해 제공되는 네트워크 공간
  - OT는 주요 설비의 제어와 관련된 영역이다. 따라서 OT는 ICS에서 보안의 가장 중요 요소라고 할 수 있다. 프로그램 가능 로직 제어기 (PLC), 원결단말장치 (RTU) 등이 OT의 중요 요소이다. PLC는 설비의 제어를 담당하는 센서로 정의

https://www.sciencetimes.co.kr/?news=ics-%EB%B3%B4%EC%95%88%EC%9D%98-%EC%B6%9C%EB%B0%9C%EC%A0%90-ot-%EA%B4%80%EB%A6%AC

산업 제어 시스템 보안

IT vs OT

항목	IT 시스템	산업제어시스템
하드웨어 및 소프트웨어	짧은 교체 주기 (3 ~ 5년)	장기간의 교체 주기 (15 ~ 20년)
	다양한 애플리케이션 및 범용 프로토콜 사용	전용 애플리케이션 및 비공개 전용 프로토콜(제어 프로토콜) 사용
	패치 등 유지·보수가 용이	패치 등 유지·보수가 어려움
	범용 OS 사용 (윈도우, 리눅스 등)	전용 OS/ 실시간 OS 사용
네트워크 성능 요구사항	전체 성능(throughput)에 초점	견고성 및 실시간 요구사항 중시
	응답의 신뢰성이 중요하며 일부 통신 지연 허용	응답 시간이 중요하며 통신 지연 불허
위험관리 목표	데이터의 무결성 중요	인간의 안전 및 시스템 가용성 중요
	일부 고장 및 장애 허용	운전 정지가 허용되지 않음
사고 영향	사고 발생 시 업무 불편 및 지연 등 상대적으로 미미한 경제적 피해 발생	사고 발생 시 산업현장 운영 중단으로 인한 인명 피해 및 대규모 물리적·경제적 피해

IT는 CIA 우선순위
- Confidentiality (기밀성)
- Integrity (무결성)
- Availability (가용성)

OT는 AIC 우선순위
- Availability (가용성)
- Integrity (무결성)
- Confidentiality (기밀성)

https://www.eventservice.kr/2019/microfocus/00/file/0709_micofous_Security_Forum_04.pdf

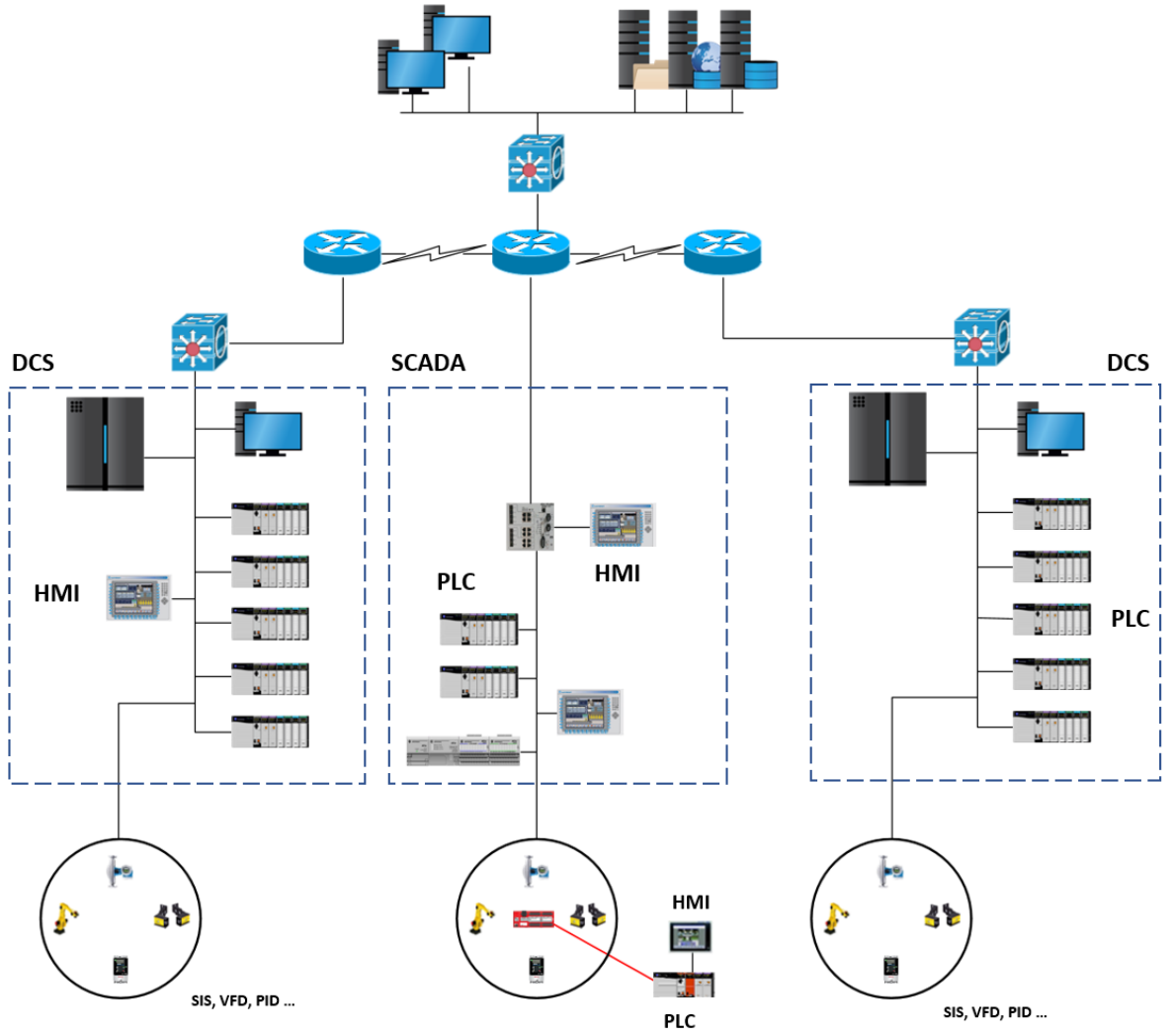
산업 제어 시스템

산업 제어 시스템 구조

- **프로그래머블 로직 컨트롤러: PLC**(Programmable Logic Control)
- **휴먼 머신 인터페이스: HMI**(Human Machine interface)
- **감시 제어 및 데이터 취득: SCADA**(Supervisory Control and Data Acquisiton)
- **시스템 분산 제어 시스템: DCS**(Distributed Control System)
- **안전 계측 시스템: SIS**(Safety Instrumented System)

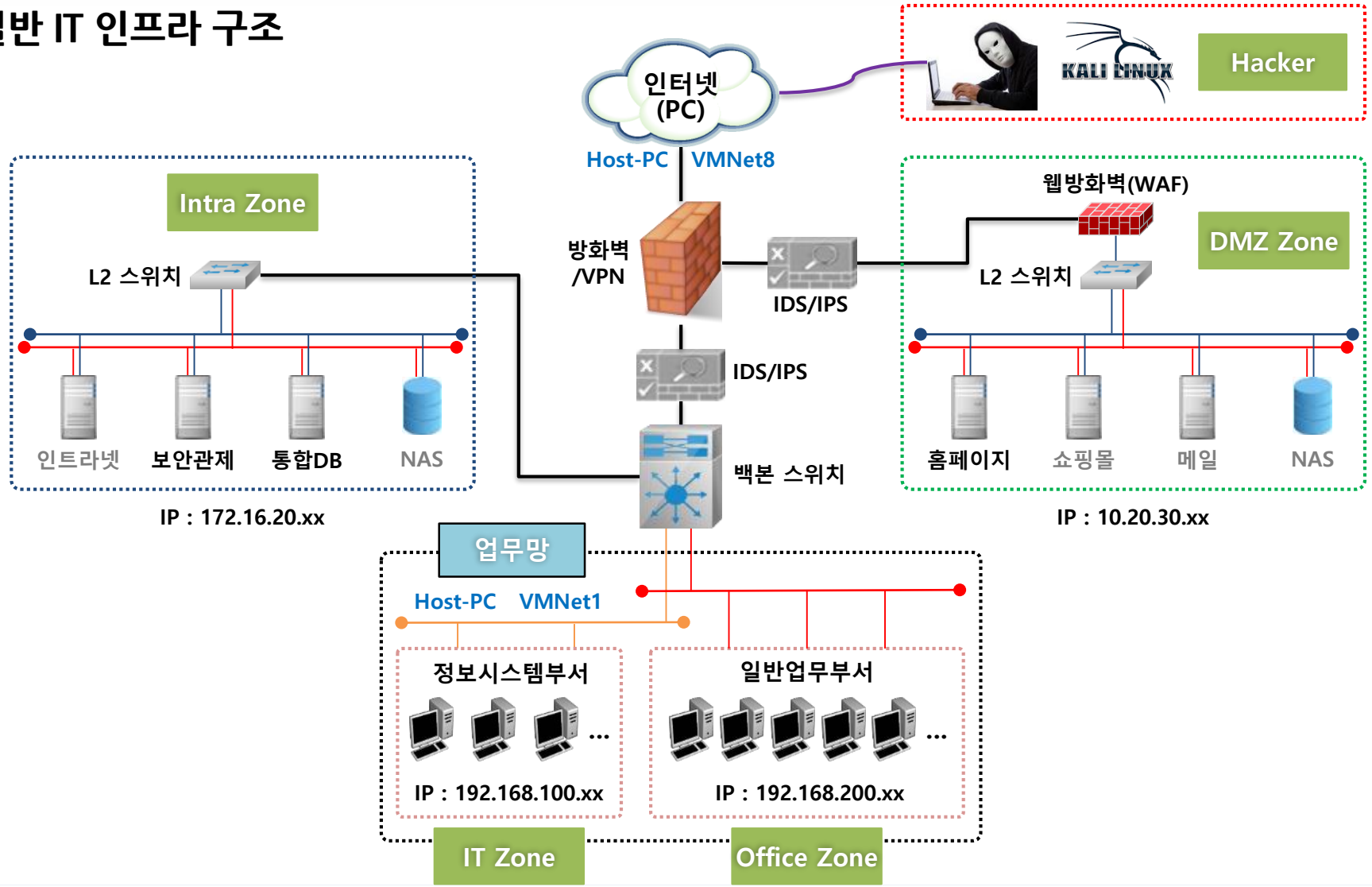
산업 제어 시스템

산업 제어 시스템 인프라 구조



산업 제어 시스템

일반 IT 인프라 구조



산업 제어 시스템

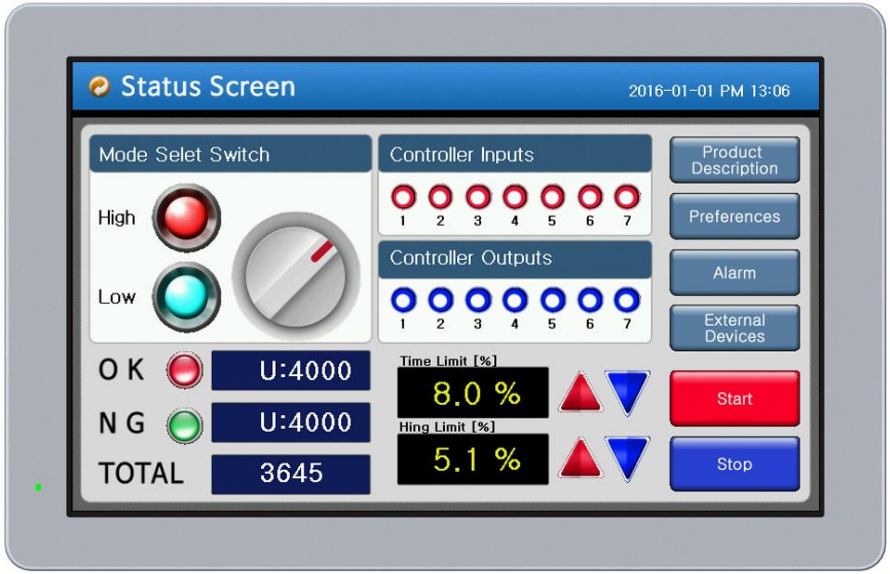
프로그래머블 로직 컨트롤러: PLC(Programmable Logic Control)

- 입력 채널을 통해 센서에서 데이터를 획득하고, 출력 채널을 통해 엑추에이터를 제어
- 인간의 두뇌와 같은 역할을 하는 마이크로컨트롤러와 입출력 채널의 배열로 구성
- 전용 USB, 장비의 시리얼 인터페이스, 애드온 카드로 제공되는 네트워크 통신 버스를 통해 수행

산업 제어 시스템

휴먼 머신 인터페이스: HMI(Human Machine interface)

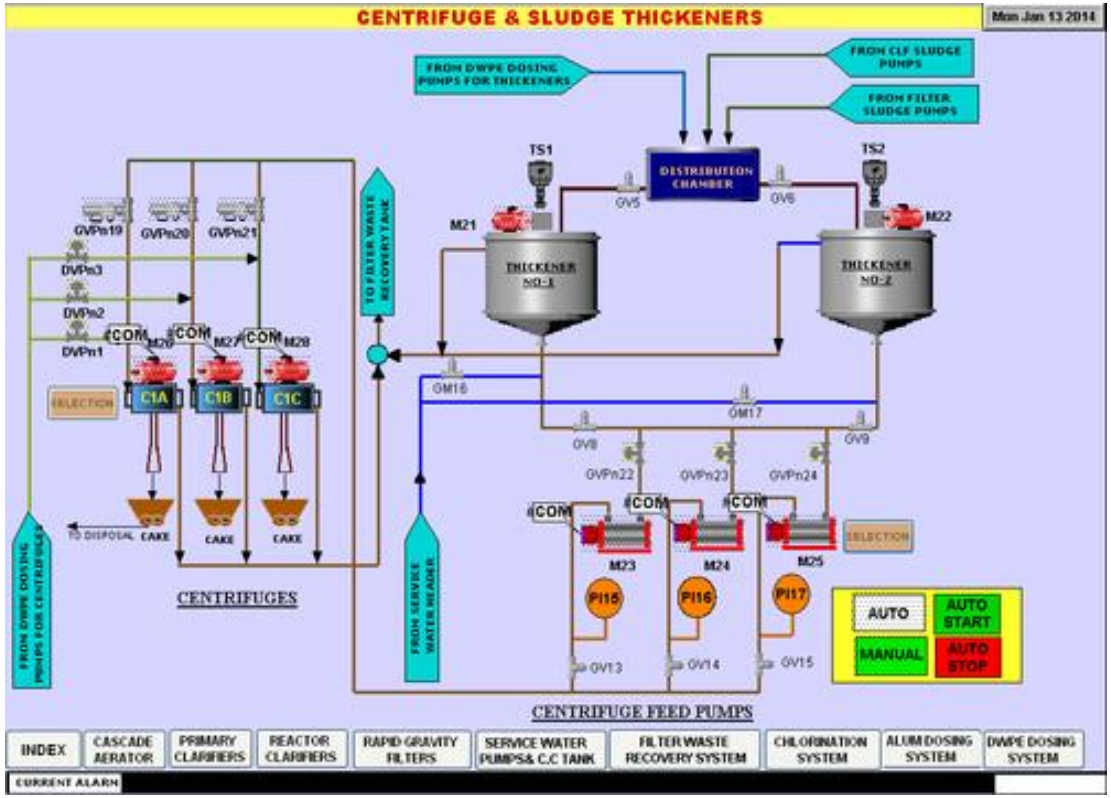
- 실행 중인 프로세스를 시각화해 프로세스 값의 검사와 조작, 경보 표시와 제어 설정 값의 현황 표시
- 시리얼 통신이나 이더넷 암호화 프로토콜을 통해 통신하는 터치 지원 독립형 장비



산업 제어 시스템

감시 제어 및 데이터 취득: SCADA(Supervisory Control and Data Acquisiton)

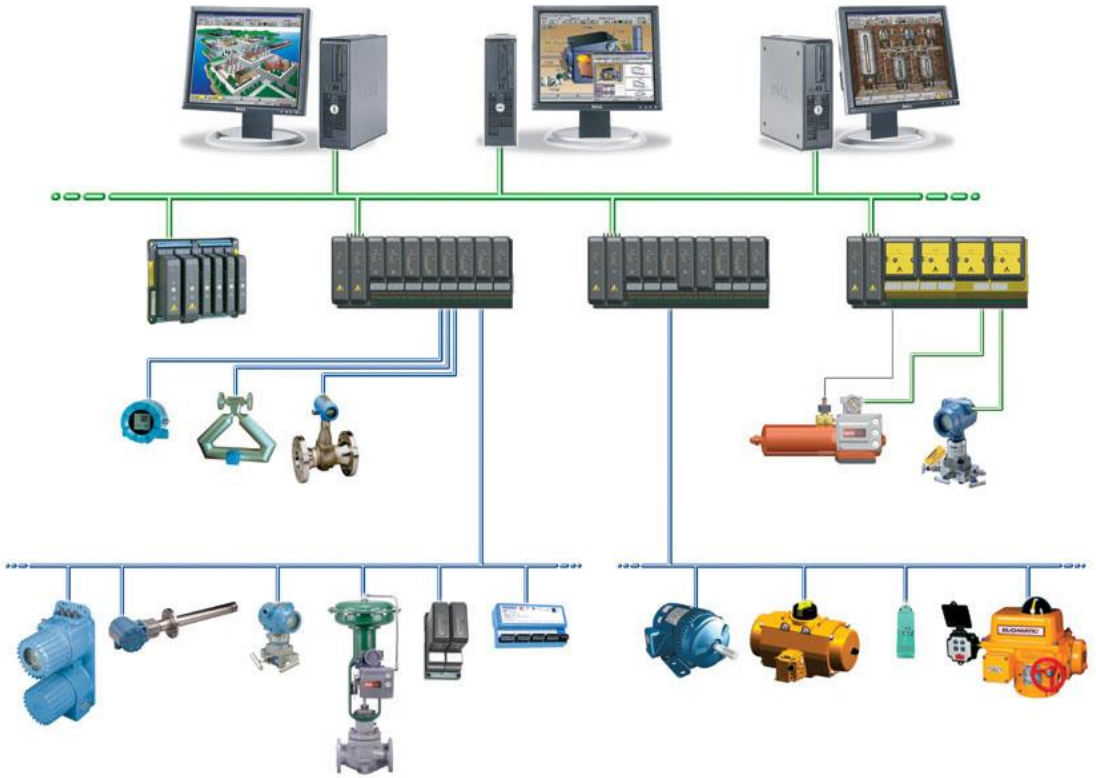
- ICS 유형 및 장비의 결합된 시스템을 의미함
- SCADA 시스템은 1960년대 **원격지의 시스템을 효과적으로 감시하고 제어하기 위하여 사용되기 시작**
- 장치마다 상호 또는 외부 기기와 연결하여 각각의 장치에 대한 원격 접근과 제어 가능
- 전력망, 수도 시설, 파이프 공정 라인과 원격 운영 스테이션을 사용하는 기타 제어 시스템에 적용



산업 제어 시스템

시스템 분산 제어 시스템: DCS(Distributed Control System)

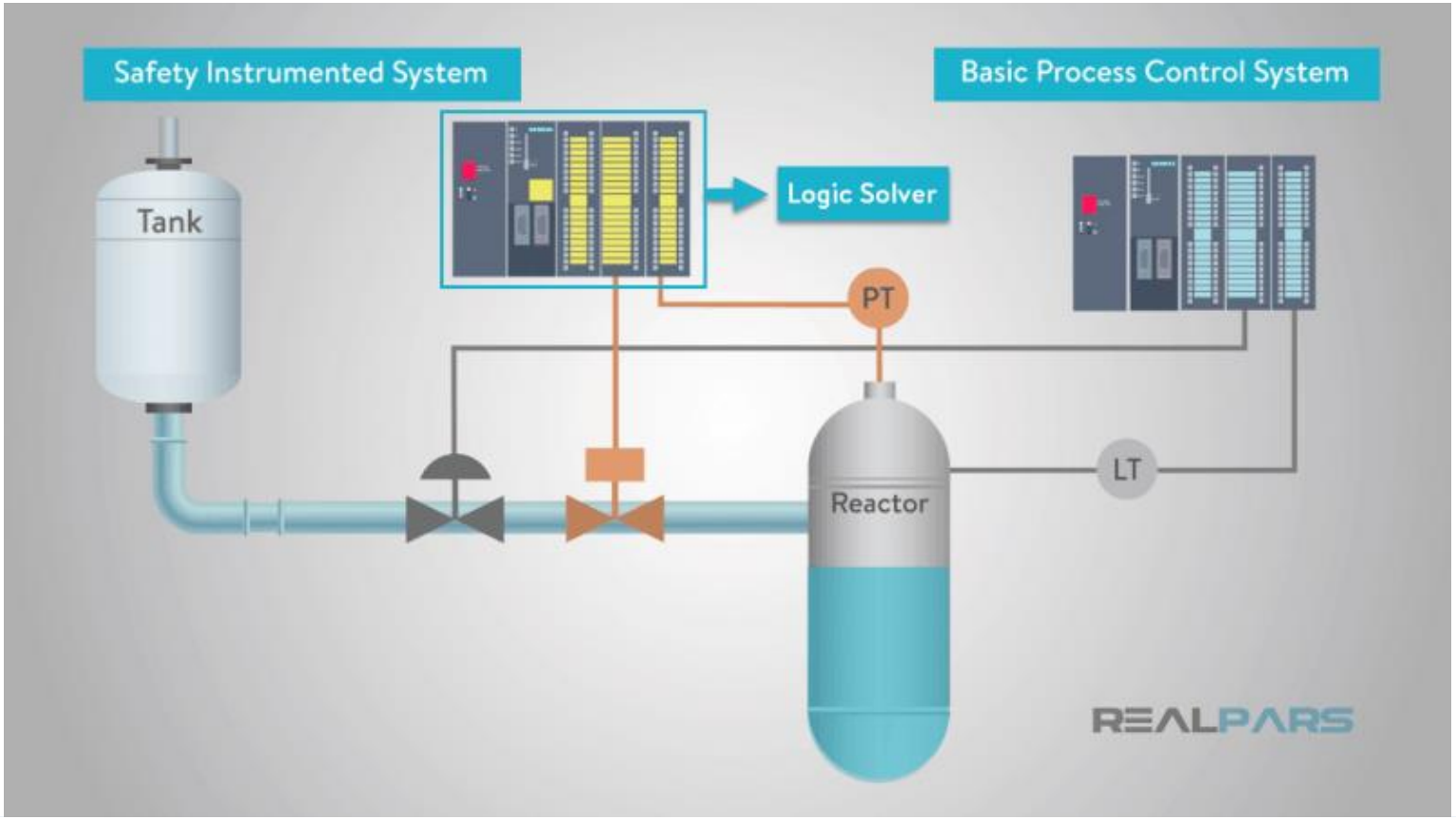
- 현재는 SCADA와 개념적으로 차이가 거의 없음
- SCADA 시스템은 큰 지리적 영역을 다루는 자동화 작업에 사용, DCS는 하나의 현장에서 이뤄지는 작업을 처리하는데 사용



산업 제어 시스템

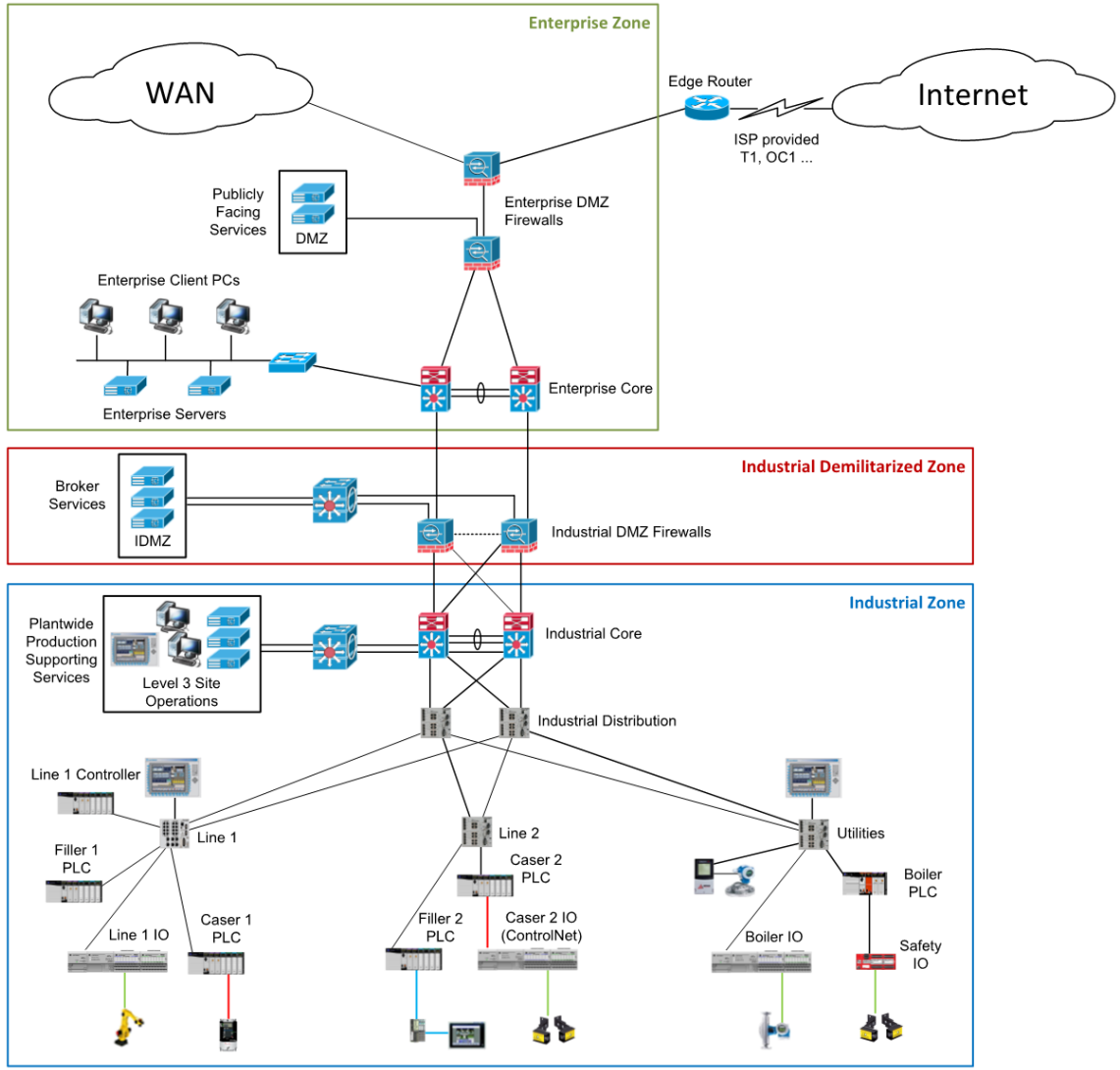
안전 계측 시스템: SIS(Safety Instrumented System)

- 안전 모니터링 전용 시스템
- 감시 대상 시스템의 전원을 정상적으로 다운 시키고, 하드웨어가 고장 난 경우 미리 정의된 안전 모드 상태로 시스템을 유지 시킴



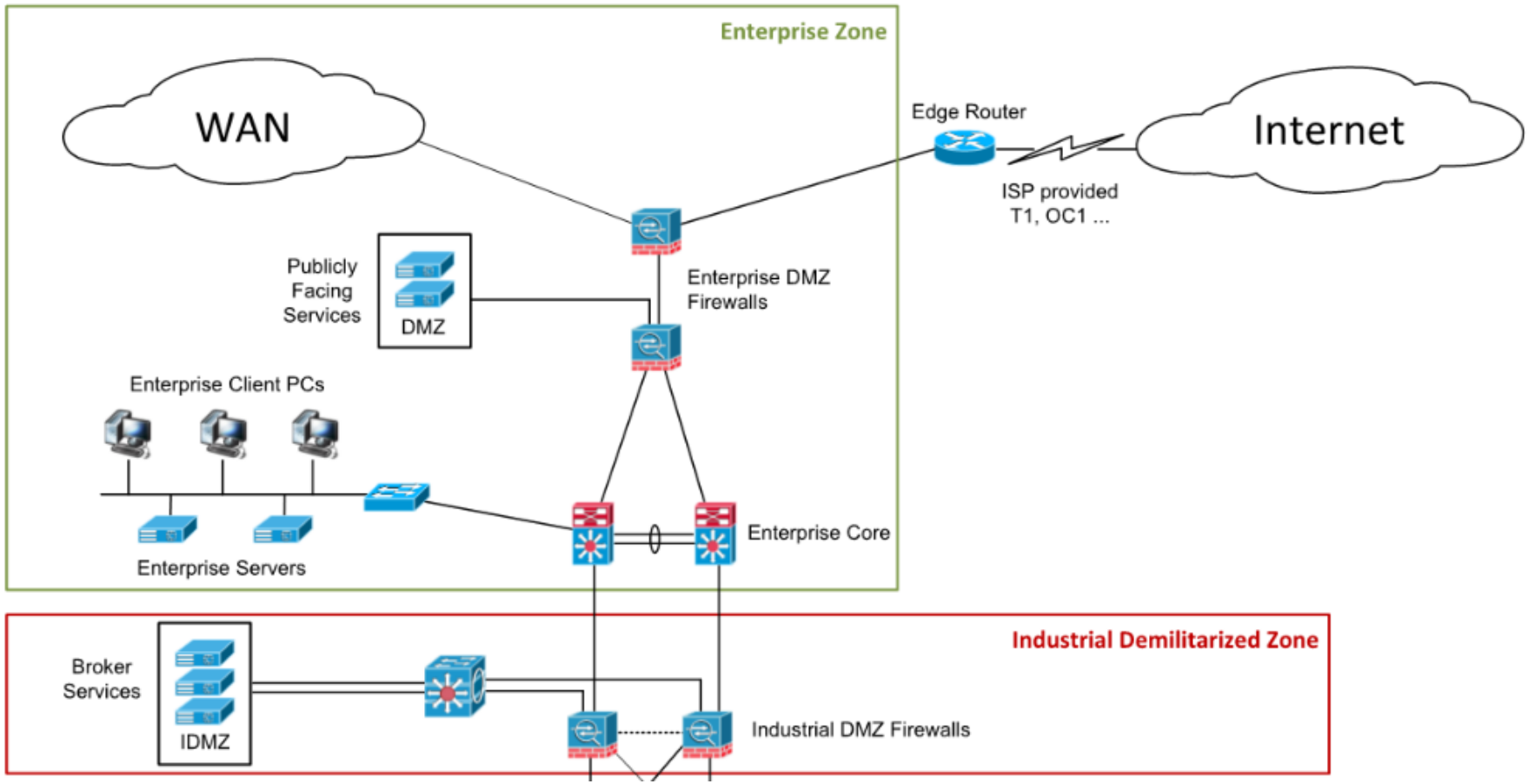
산업 제어 시스템 이해

인프라 이해



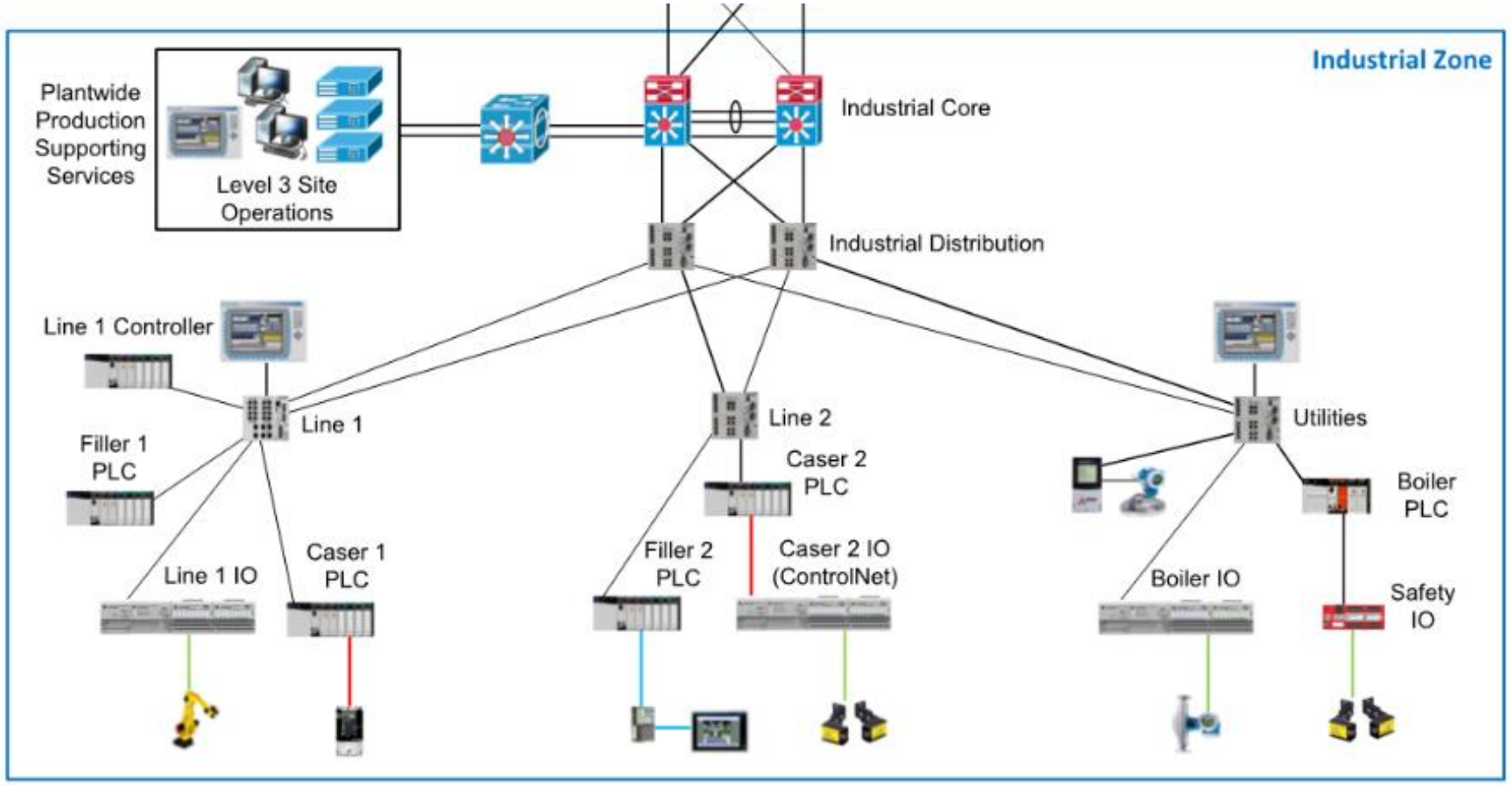
산업 제어 시스템 이해

인프라 이해



산업 제어 시스템 이해

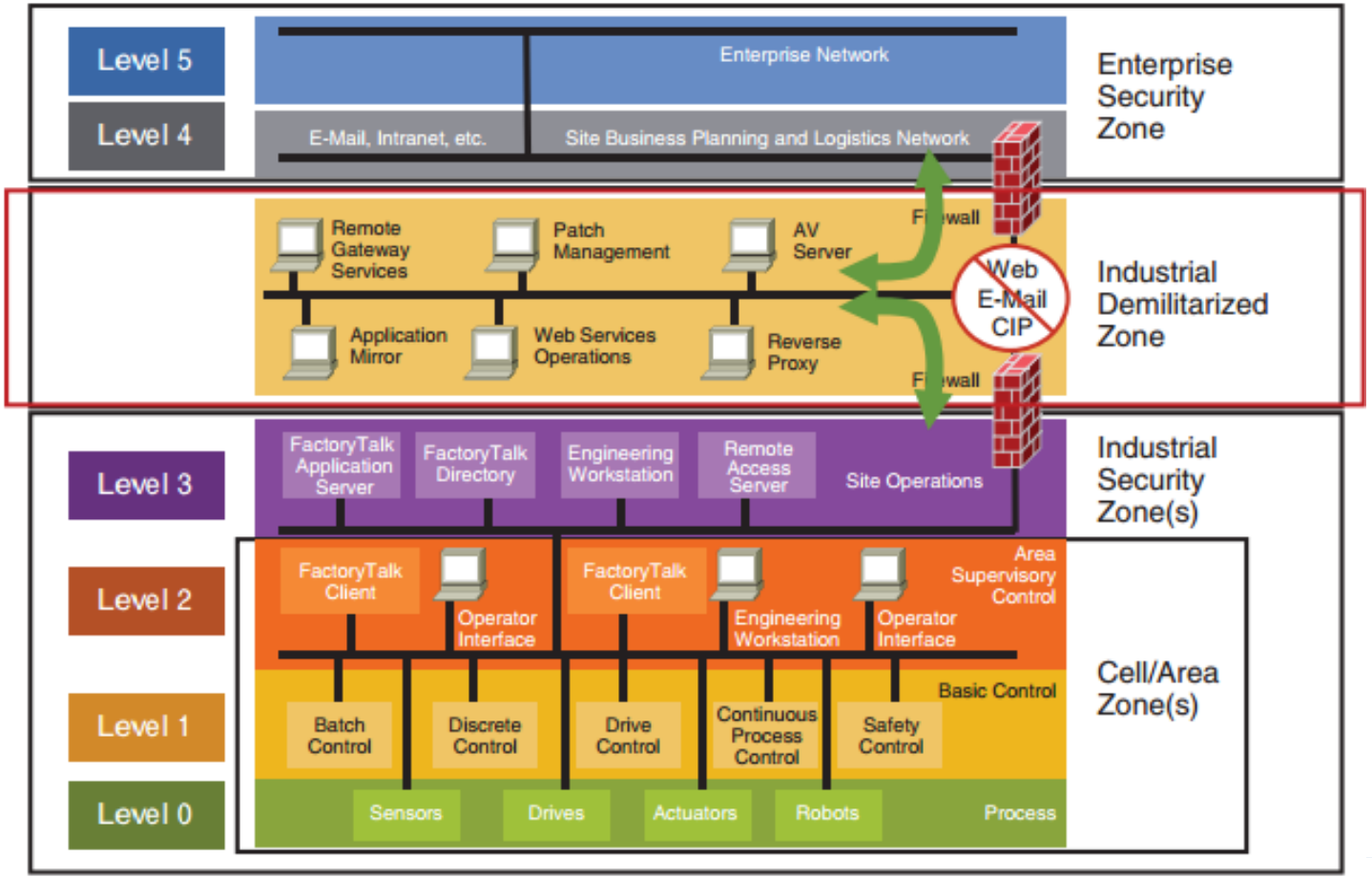
인프라 이해



산업 제어 시스템 이해

퍼듀 모델

- ISA-99의 PERA모델에서 채택된 ICS 네트워크 구조화를 보여주기 위한 개념 모델
- ICS의 모든 주요 구성 요소의 상호 연결과 의존성을 보여주는 산업 표준 참조 모델

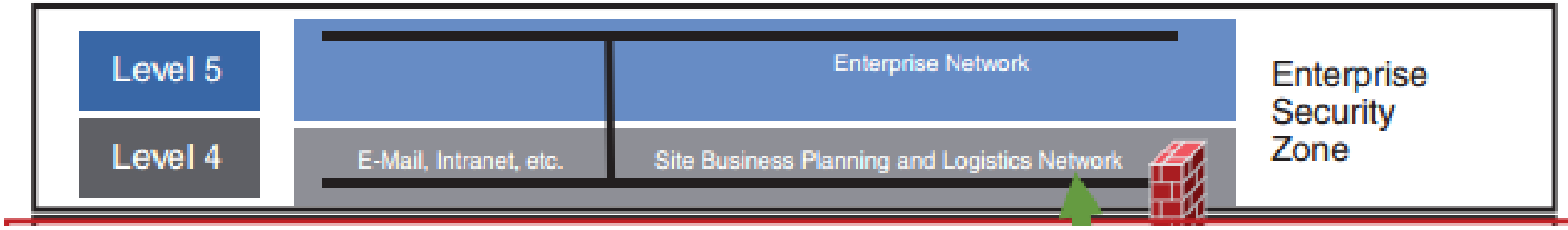


산업 제어 시스템 이해

퍼듀 모델 - 엔터프라이즈 영역(기업 레벨)

- 개별 공장의 서브시스템 데이터를 받아와 누적된 데이터를 기반으로 전반적인 공장 설비의 생산 상태, 재고 및 수요를 보고하는데 사용
- ICS 일부라고 하기보다는, **ICS 네트워크와의 연결을 기반으로 비지니스 결정을 내리는 데 필요한 데이터를 제공하는 역할**을 하는 구간

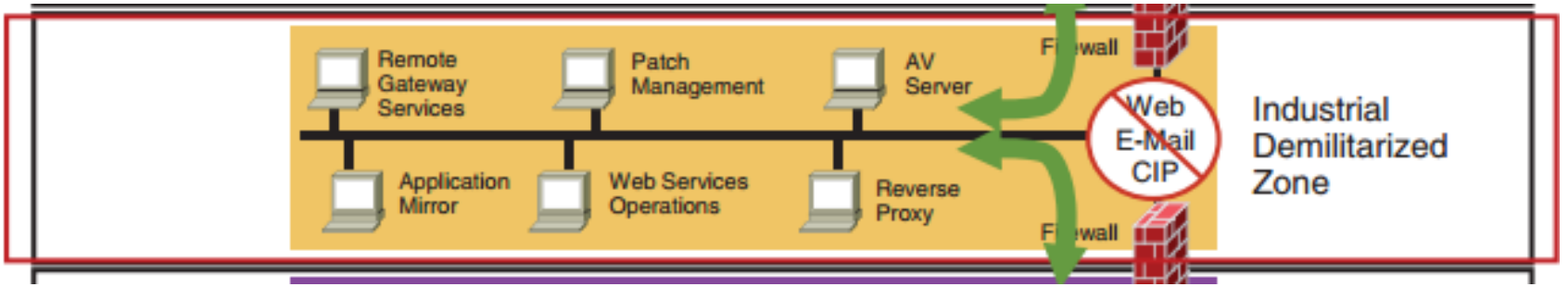
- 레벨4는 모든 정보 기술 시스템의 본거지로, **공장에서 생산하는 모든 프로세스를 지원**
- 구동 시간, 설비에서 생산된 개체 수와 같은 생산 정보 통계를 보고하고, 기업 시스템의 비지니스 데이터를 운영 기술이나 ICS 시스템에 분배되도록 지시
- 레벨4에는 일반적으로 데이터베이스 서버, 애플리케이션 서버, 파일 서버, 이메일 클라이언트, 감독자 데스크톱 등의 시스템이 위치



산업 제어 시스템 이해

퍼듀 모델 - 인터스트리얼 비무장 영역

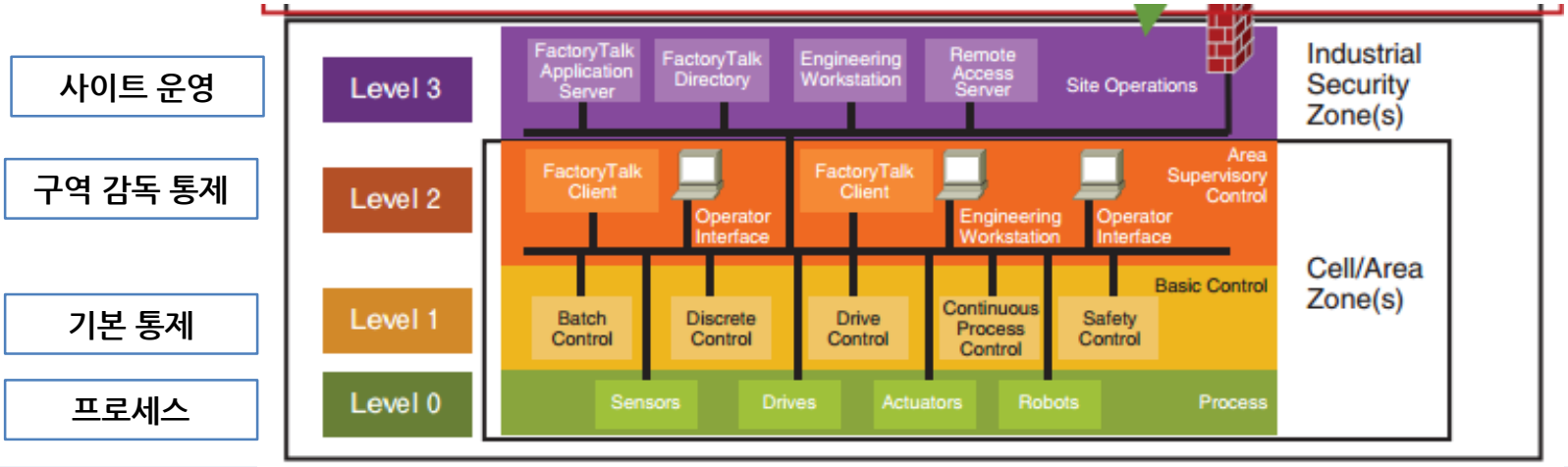
- OT 중심 구간이며, 전형적인 IT의 DMZ 영역처럼 여러 보안 요건이 갖추어서 네트워크를 안전하게 연결
- IDMZ는 수준 4와 5의 비즈니스 또는 IT 시스템과 수준 3 이하의 프로덕션 또는 OT 시스템 간의 정보 공유 계층
- IDMZ는 NIST 사이버 보안 프레임 워크 및 NERC CIP와 같은 보안 표준을 만들려는 결과임
- IT와 OT 시스템 간의 직접적인 통신을 방지하고 IDMZ의 중계 서비스를 통해 통신을 중계함으로써 별도의 분리 및 검사 계층이 전체 아키텍처에 추가됨
- IDMZ의 어느 시점에서 시스템이 손상 될 수있는 경우, IDMZ가 종료되고 절충안을 시행해 생산이 계속 될 수 있음



산업 제어 시스템 이해

퍼듀 모델 - 인터스트리얼 영역

- **레벨3 - 사이트 운영**
  - 공장 전반의 컨트롤 기능과 모니터링을 담당하는 시스템(HMI, 운영장비 등)이 위치함
  - 하위 수준의 시스템은이 수준의 프로덕션 데이터를 데이터 수집 및 집계 서버로 전송, 데이터를 더 높은 수준으로 보내거나 높은 수준의 시스템에서 쿼리를 수행
- **레벨2 - 구역 감독 통제**
  - 레벨 2의 많은 기능과 시스템은 레벨 3과 동일하지만, 전체 시스템의 더 작은 부분 또는 영역을 담당
  - 기계 또는 스키드를 시작 또는 중지하고, 기본 실행 값을 확인하고 기계 또는 스키드 별 임계 값 및 설정 등을 조작
- **레벨1 - 기본 통제**
  - 모든 제어 장비가 있는 곳, 밸브를 열고 액추에이터를 움직이고 모터를 시동하는 곳
  - PLC, 가변 주파수 드라이브 (VFD), 전용 비례 적분 파생 (PID) 컨트롤러 등이 위치함



산업 제어 시스템 보안

정보시스템 vs 스카다 시스템 차이

구분	정보시스템	스카다 시스템
성능 요구사항	비실시간 응답의 신로성 중요 지연 허용	실시간 응답시간 중요 지연 비허용
신뢰성 요구사항	계획된 작업 고장 및 장애 허용 베타 테스트만으로도 가능 적은 문서작업으로 변경 가능	연속작업 운정정지 및 허용되지 않음 철저한 QA 테스트 필요 공식적인 절차 필요
위험관리 목표	데이터 무결성 중요 데이터 손실이나 작업의 손실 재부팅으로 회복	인간의 안전 중요 환경, 인명, 장비, 제품의 손실 결함 허용이 필수
보안정책 우선순위	보안성 > 무결성 > 가용성	**무결성 > 가용성 > 보안성**
운영방식	중앙 집중적	분산
하드웨어	대부분 하나의 솔루션으로 충분 컴퓨터와 네트워크 짧은 생애주기 저렴	**프로토콜 차이로 다수 솔루션 필요** PLC, 컴퓨터, 네트워크, RTU 등 장기간(15년~20년) 생애주기 고가
소프트웨어	다양한 애플리케이션 소수의 프로토콜 패치가능 원격으로 펌웨어 수정 불가능	다수의 프로토콜(15개이상) 대부분의 비공개된 전용 프로토콜 패치 어려움(여러 인증 필요) 벤더가 원격(HMI를 통해)에서 펌웨어 수정 가능
위험영향	데이터 탈취, 파괴	데이터 및 시스템 파괴, 파국적 결과, 경제적 손실 큼
피해복구	용이함, 조사 및 재포멧	어려움, 벤더가 고침

IT는 CIA 우선순위
- Confidentiality (기밀성)
- Integrity (무결성)
- Availability (가용성)

OT는 AIC 우선순위
- Availability (가용성)
- Integrity (무결성)
- Confidentiality (기밀성)

https://crefunx.tistory.com/19

산업 제어 시스템 해킹 위협 사례

산업 제어 시스템 해킹 위협 사례

보안 사고 사례

발생시기	대상	공격 형태/피해
2007.08	미국 수자원	○전직 직원이 캘리포니아주의 TCCA 운하 제어시스템에 멀웨어 설치로 운하 운영 마비
2008.05	미국 전력	○회계감사원(GAO) 주관으로 미국 최대 국립전력회사인 TVA사 제어시스템을 모의해킹하여 인터넷 발전소 제어 시스템 침투
2008.08	터키 에너지	○석유 송유관 카메라 통신 소프트웨어 취약점을 이용해 네트워크로 침투하여 관리 네트워크 장애 발생 및 석유 압력 변조로 폭발 사고 유도
2010.07	이란 원자력	○스턱스넷 바이러스가 원자력발전소 제어시스템 침투하여, 이란 나탄즈 원자력 원심분리기 1000여 개가 복구 불능 상태가 됨
2011.08	다국적 석유회사	○SCADA 시스템에 대한 운영자료를 수집하여 유출
2011.11	미국 상수도	○일리노이주 상수도 시설 시스템에 침투하여 펌프 작동 시스템 파괴

출처: SK인포섹

산업 제어 시스템 해킹 위협 사례

보안 사고 사례

2012.10	독일 제철소	○제어시스템의 파괴로 인한 용광로의 제어 및 정상적인 Shutdown 불가로 큰 피해 발생
2014.06	유럽 스카다	○유럽 스카다(SCADA) 시스템 설치 프로그램에 포함된 하벡스(Havex) 멀웨어 발견
2015.12	우크라이나 전력	○멀웨어를 통해 발전소 제어시스템을 중단하여 정전을 유발 8만여 가구 정전 발생
2016.04	미국 전력	○랜섬웨어가 첨부된 이메일을 통한 스피어 피싱 공격이 발생. 내부 네트워크까지 감염이 확산되자 추가 피해 발생을 막기 위해, 회사 시스템을 일시 중단함
2017.06	일본 자동차	○혼다자동차 사야마 공장 워너크라이 랜섬웨어에 감염되어, 약 48시간 동안 엔진 생산과 조립 중단
2017.10	미국 달라스 비상사이렌	○무선통신망의 해킹으로 인해 달라스의 비상 사이렌이 15시간 동안 가동됨

출처: SK인포섹

산업 제어 시스템 해킹 위협 사례

사례 분석

- **한수원 해킹 사고 (보도 자료)**
  - http://large.stanford.edu/courses/2017/ph241/min1/docs/min_ref1.pdf
- **스턱스넷(Stuxnet) 분석 보고서**
  - https://www.owasp.org/images/9/9f/APAC13_Ihn-Hyuk._Song.pdf
- **미국 국립보건서비스 관련 랜섬웨어 피해 보고서**
  - http://img.innotium.com/newsletter/rans_20170514/rancert_wannacry_report_20170514.pdf

산업 제어 시스템 해킹 위협 사례

산업 제어 시스템 보안 위협에는 어떤 유형이 있을까

- 접근 제어 미흡에 의한 관리자/기계 제어 시스템 권한 탈취
- 벤더사 원격 제어 시스템의 악성코드 감염 위협
- 관리자 웹 애플리케이션 취약점 위협
- 랜섬웨어/파괴형 악성코드 배포
- 패치되지 않은 운영체제/시스템 위협
- 취약한 네트워크 프로토콜의 위협