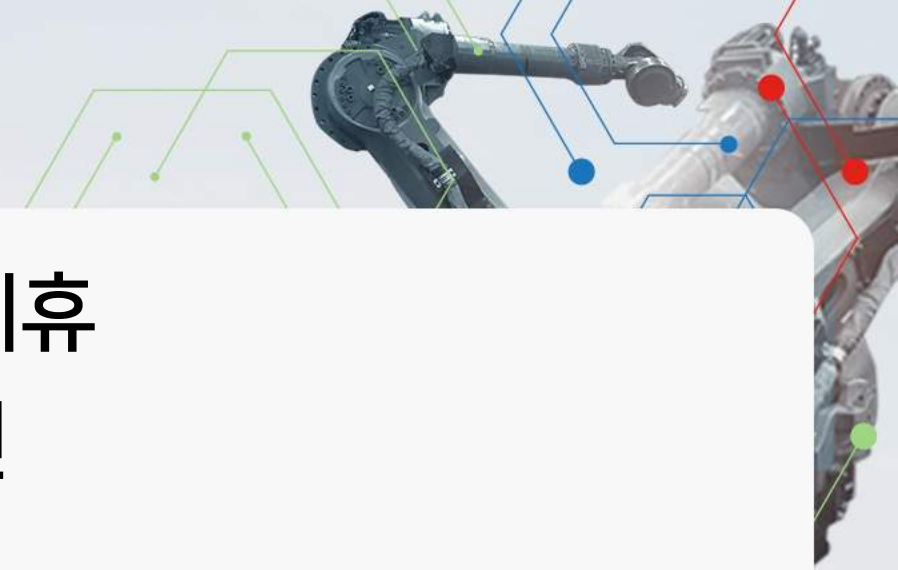
IT & OT 통합
플랜트 네트워크 표준화 방안

박병준 부장
로크웰 오토메이션 코리아

목차



- 로크웰 오토메이션과 시스코의 전략적 제휴
- CPwE를 활용한 컨버지드 아키텍처 구현
- CPwE 레퍼런스 아키텍처 오버뷰
- CPwE 아키텍처의 주요 원리
- Summary

참고: CPwE(Converged Plantwide Ethernet)

로크웰 오토메이션과 시스코의 전략적 제휴

시장 압력으로 산업 운영의 생산성과 수익성 위험

3경5천조원
2000 ~ 2016간
글로벌 GDP성장으로
빠른 세계화

노후화된
인프라

작년 제조 조직의
28% 가 보안 사고로
인한 수익 손실에 영향
을 받았다고 보고

산업용
IoT

빠른
세계화

제조의 87% 경영진은
노후화된 인프라가
플랜트 운영에 영향을
미친다고 보고

보안
리스크 및 위협

4 조
2020년까지 산업별
산업용 IoT 비즈니스
기기의 수

디지털
트랜스포메이션
을 통한 현대화
필요…

현대화는 복잡하며 수많은 문제점을 해결 필요

사일로 네트워크

노후화된 인프라는 네트워크의 복잡성을 증가하는 독점적인 네트워크로 구성

제한된 보안

기존 보안 접근 방식은 새로운 보안 위협을 해결할 수 없음

기술 격차

작업자가 최신 네트워크를 관리할 기술적 준비가 되어 있지 않음

데이터 관리

생성되는 데이터의 규모와 양이 저장 및 관리가 어려움

솔루션 복잡성

시장에서 사용 가능한 제품과 솔루션이 다양하고 복잡함

로크웰 오토메이션과 시스코가 함께 도와 드릴 수 있습니다

산업용으로 준비되고, 세계적 수준의 제어, 전력 및 정보 시스템, IT 네트워킹 및 보안 기술로 커넥티드 엔터프라이즈를 위한 디지털 혁신을 주도합니다.

CISCO

IT 네트워킹 및 보안 분야의 세계적인 리더

Rockwell Automation

산업 제어, 전력 및 정보 솔루션의 글로벌 리더

전략적 제휴를 통해 신뢰할 수 있는 도메인 전문가

미래 산업의 성공을 위한 열정

획기적인 솔루션 개발

기술, 네트워크, 문화 및 조직 융합

표준 및 공통 기술 관점:

개방형 표준 이더넷, IP 및 Wi-Fi 네트워킹 기술을 사용하는 확장 가능한 단일 아키텍처로 산업용 사물 인터넷(IIoT)이 경쟁 제조 환경에서 요구되는 유연성, 가시성 및 효율성을 달성하는 데 도움이 됩니다.

Converged Plantwide Ethernet (CPwE) 아키텍처:

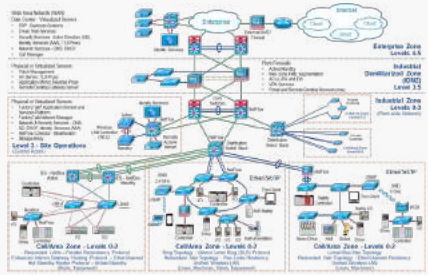
Cisco, Panduit 및 Rockwell Automation이 각 주제에 맞게 개발한 설계, 테스트 및 검증된 네트워크 디자인 모음입니다. CPwE의 내용은 운영 기술(OT) 및 정보 기술(IT) 분야 모두와 관련이 있습니다. CPwE는 문서화된 아키텍처, 모범 사례, 설계 지침 및 구성 설정으로 확장 가능하고 안정적이며, 미래에 대비할 수 있는 공장 전체 또는 현장 전체 산업 네트워크 인프라의 개발 및 배포를 통해 운영을 지원합니다.

공동 제품 협업:

최고의 로크웰 오토메이션과 시스코의 결합 – 산업용 이더넷 스위치 Stratix® 2500/Stratix 5000 제품군, 보안 기능을 보유한 Stratix® 5950 그리고 FactoryTalk® Network Manager™ 소프트웨어.

인력 개발- 인력 및 프로세스 최적화:

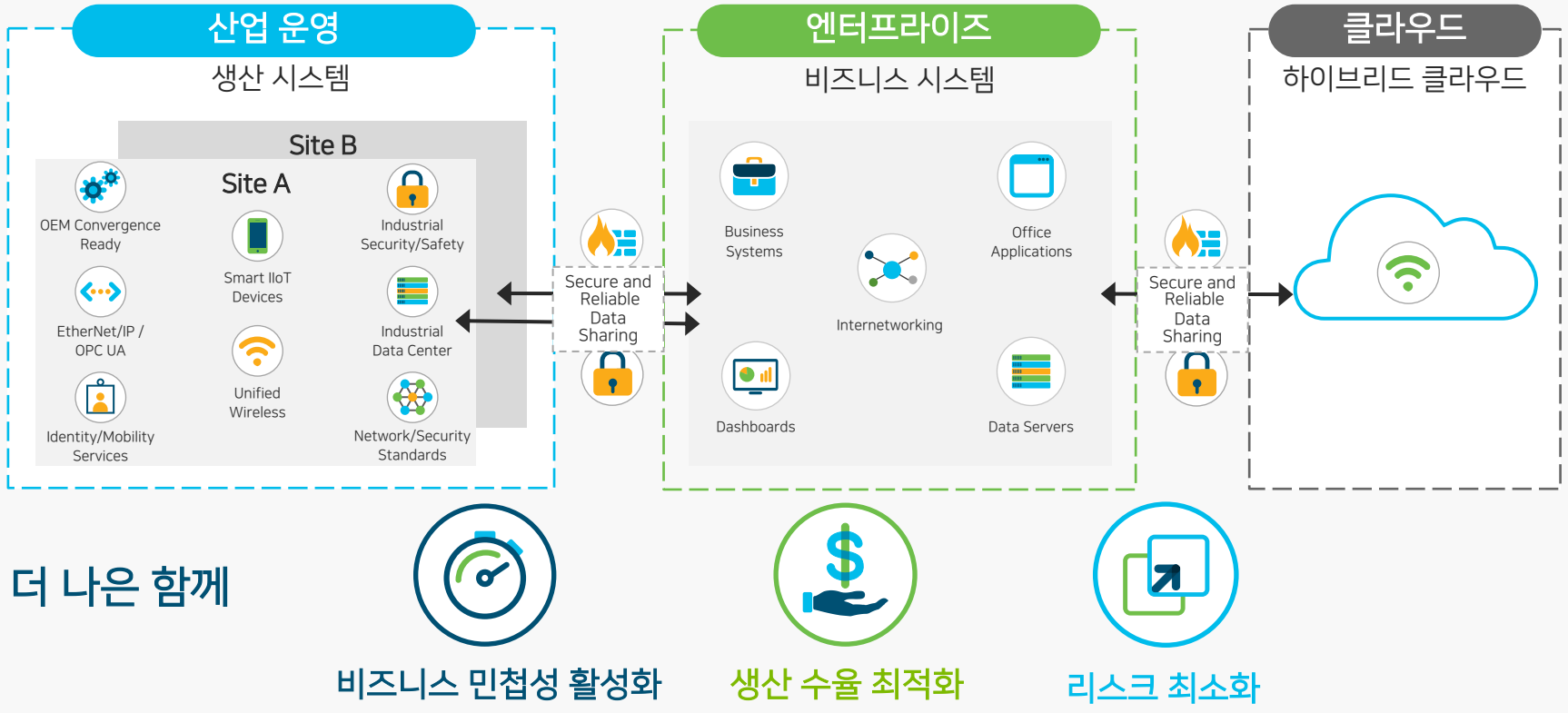
OT 및 IT 기술, 네트워크 및 문화 융합을 촉진하는 데 도움이 되는 교육, 훈련, 인증 및 서비스



참고: 모든 내용을 포함하지 않으며 현재 진행중인 작업, 사전 통지 없이 내용이 변경 될 수 있음

디지털 혁신을 위한 전체적인 청사진 CPwE
(Converged Plantwide Ethernet)

CPwE 융합 네트워크 아키텍처



더 나은 함께

- 비즈니스 민첩성 활성화
- 생산 수율 최적화
- 리스크 최소화

설계, 테스트 및 검증된 네트워크 및 보안 설계 모음

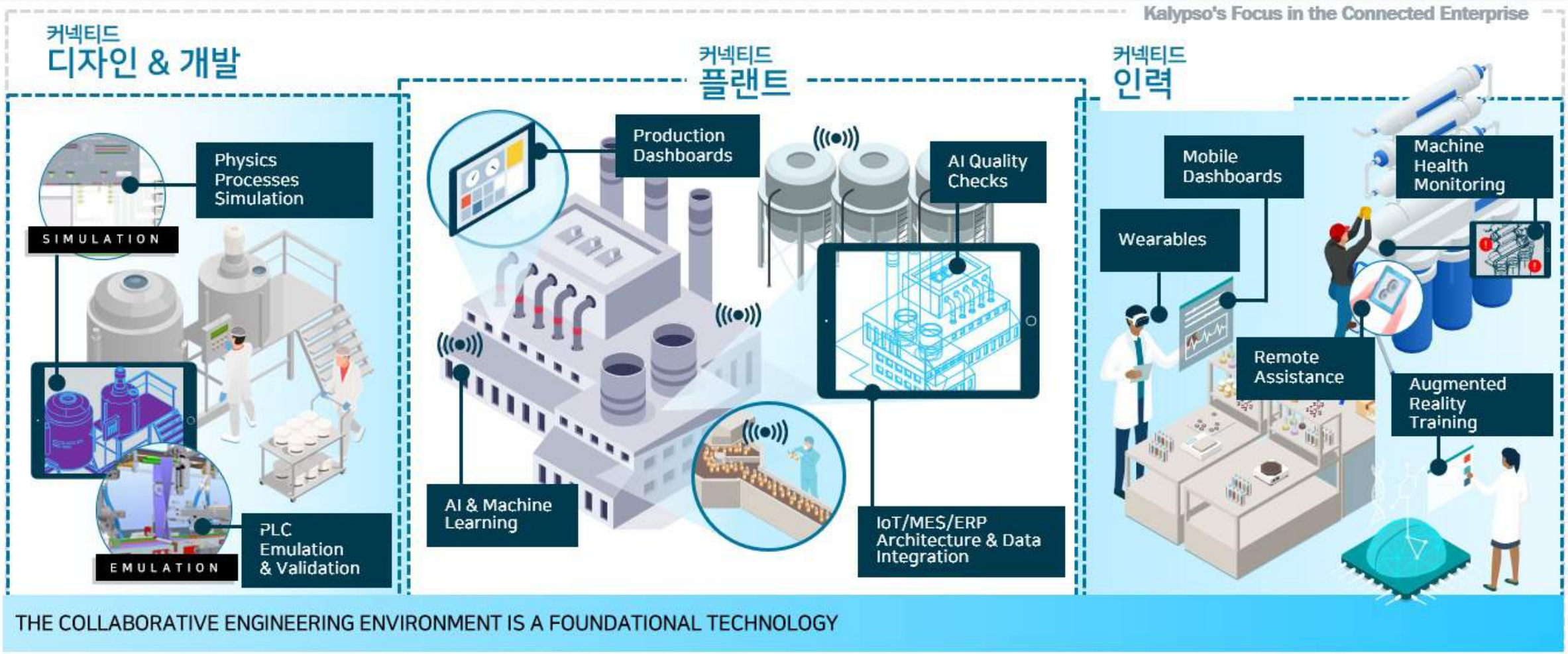
산업 운영 및 비즈니스 시스템 연결과 네트워크 및 보안 설계 간소화

규제 표준을 준수하는 개방형 솔루션은 유연성과 확장성을 제공

공통 아키텍처 프레임워크를 기반으로 구축된 인프라는 네트워크를 통한 데이터 가시성 확보

CPwE (Converged Plantwide Ethernet) 를 활용한 컨버지드 아키텍처 구현

스마트 팩토리의 기본 커넥티드 플랜트



스마트 팩토리의 기본 커넥티드 플랜트

기존 플랜트

IT 네트워크와 산업용 네트워크 혼용

IT 네트워크 인프라 (IT 표준 이더넷)

산업 표준 네트워크

인터페이스

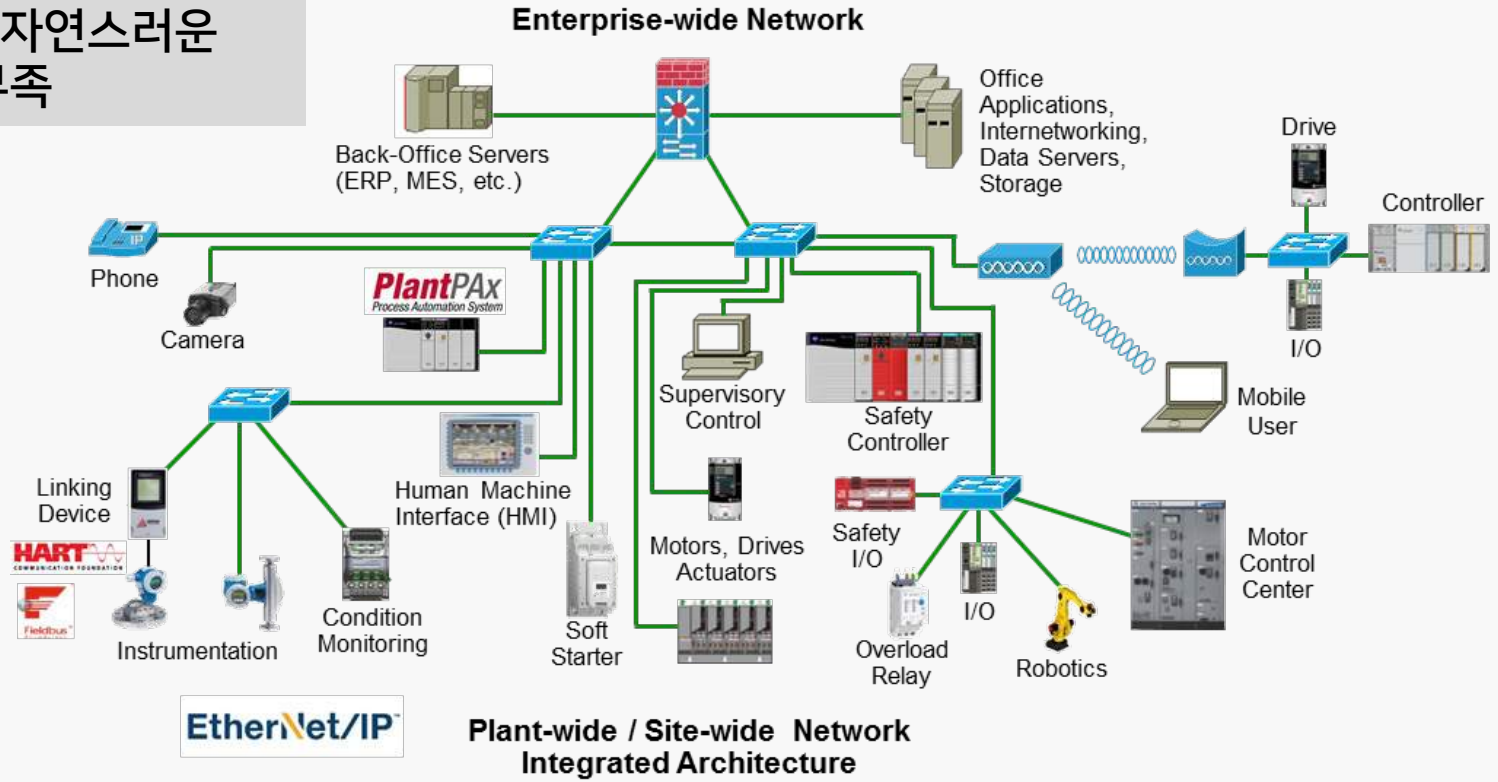
신규 플랜트

IT 네트워크 인프라 위에서 스마트 팩토리 운영

IT 네트워크 인프라 (IT 기반의 단일 표준 네트워크)

산업용 IoT (IIoT) – IACS 융합

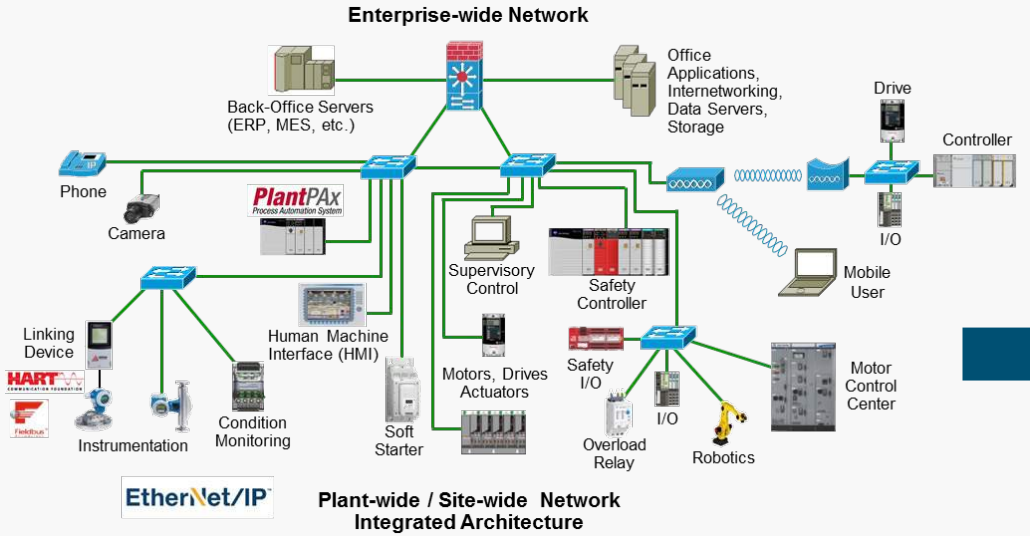
네트워크 확장 및 자연스러운 세분화 부족



수평적이고 개방적이며 비탄력적인
Industrial Automation and Control System (IACS)
네트워크 및 보안 인프라

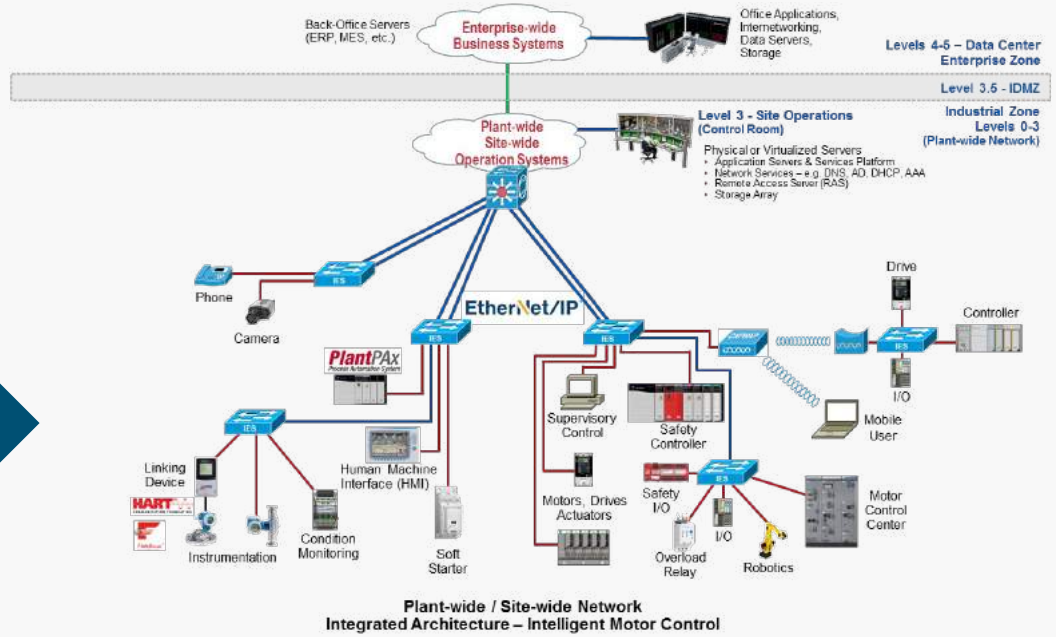
산업용 IoT (IIoT) – IACS 융합

더 큰 LAN 연결, 자연스러운 구분 및 세분화 부족



수평적이고 개방적이며 비탄력적인 IACS 네트워크 및 보안 인프라

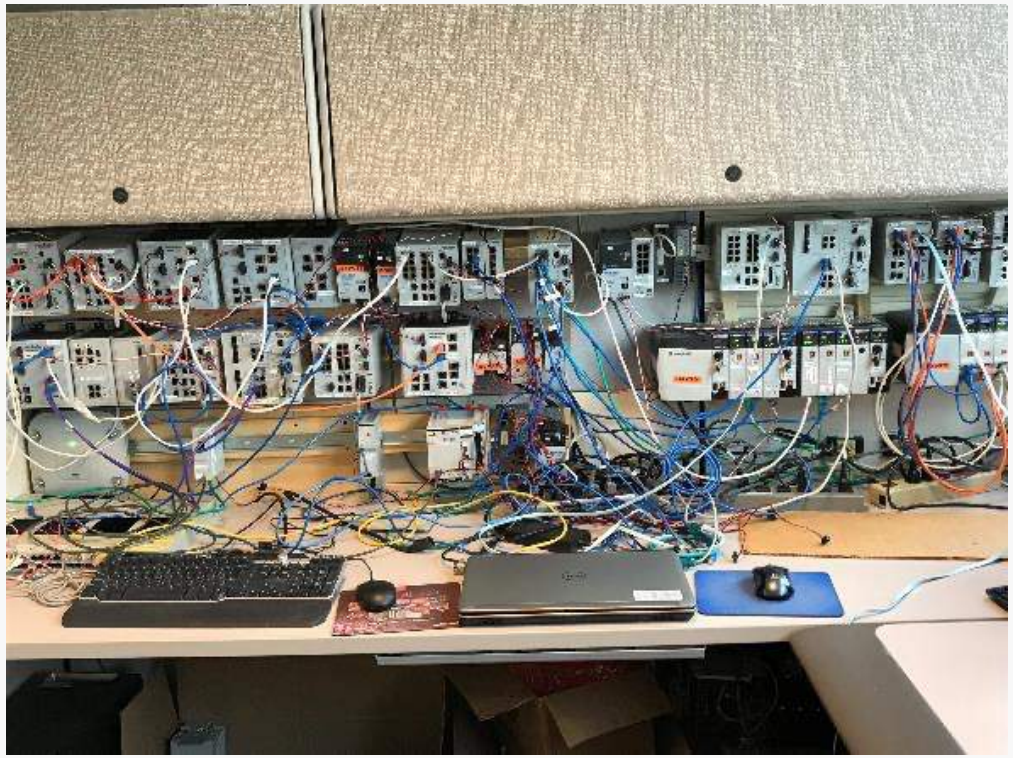
더 작은 LAN 연결, 경계 생성 및 세분화

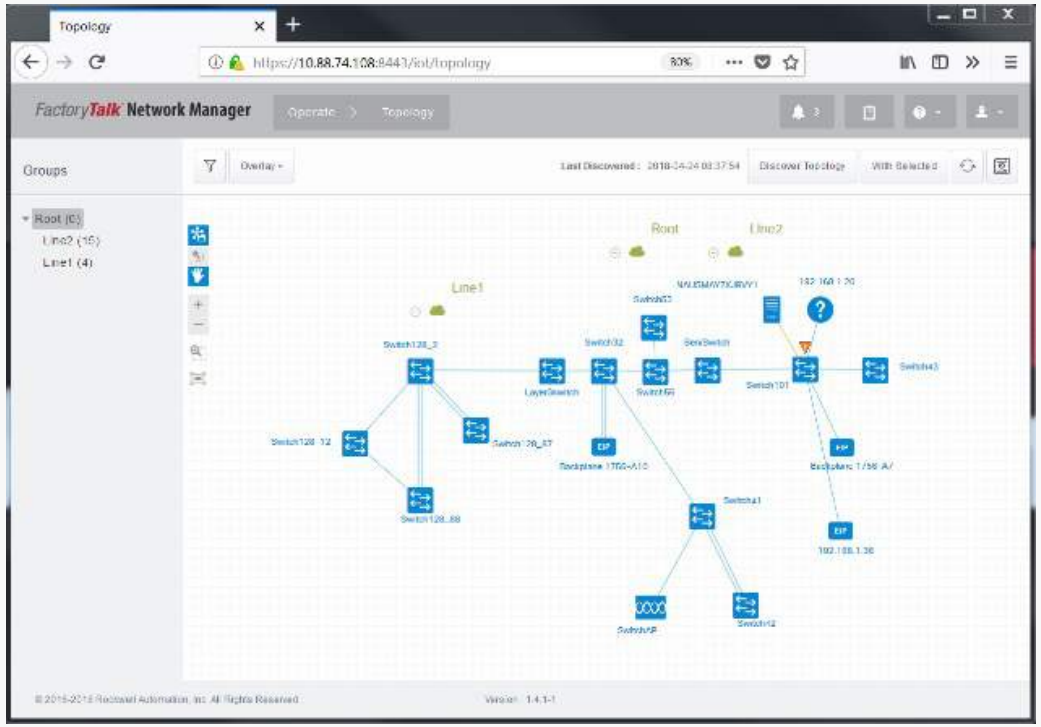


구조화 및 강화된 IACS 네트워크 및 보안 인프라

OT에서 사용할 수 있는 네트워크 관리 툴

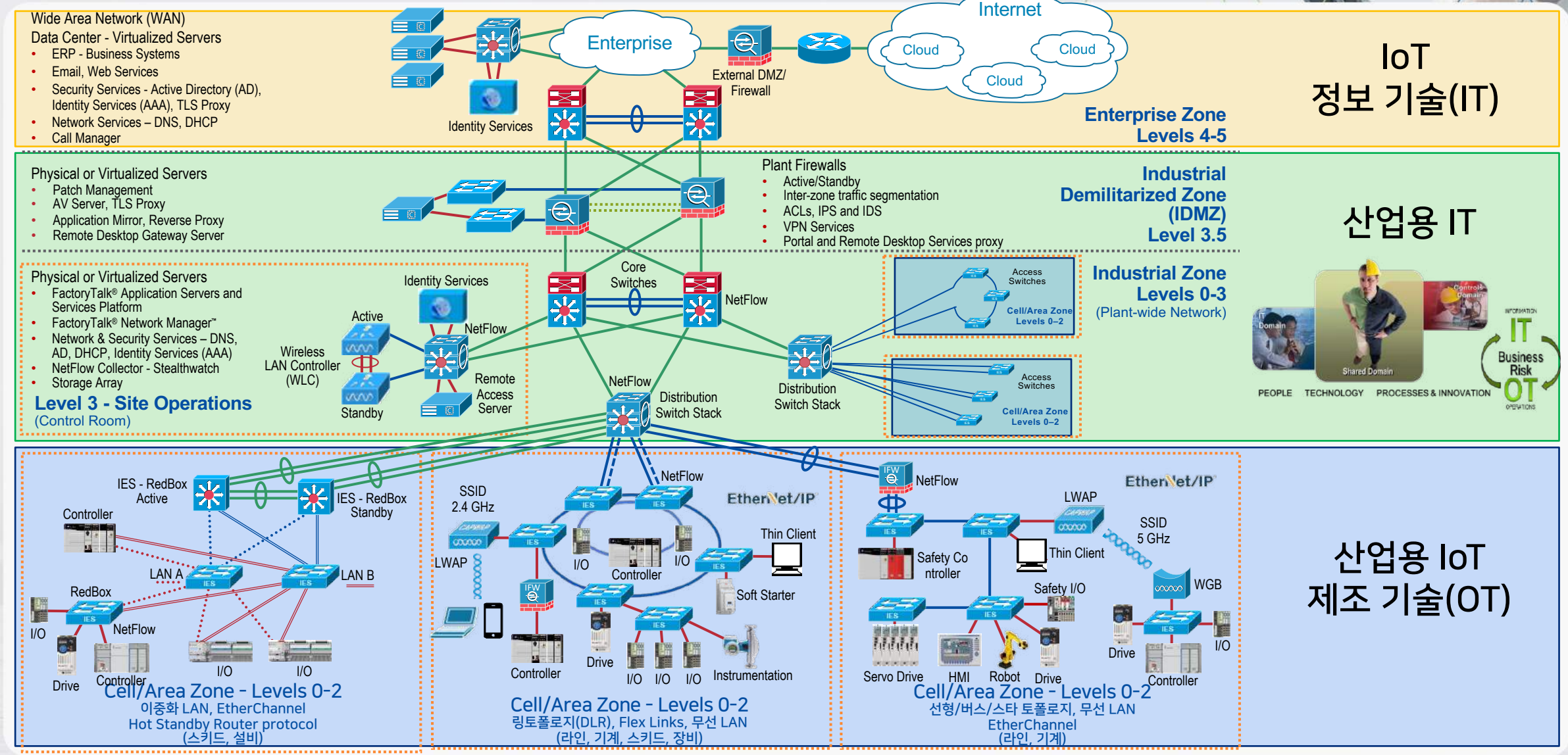
FT Network Manager



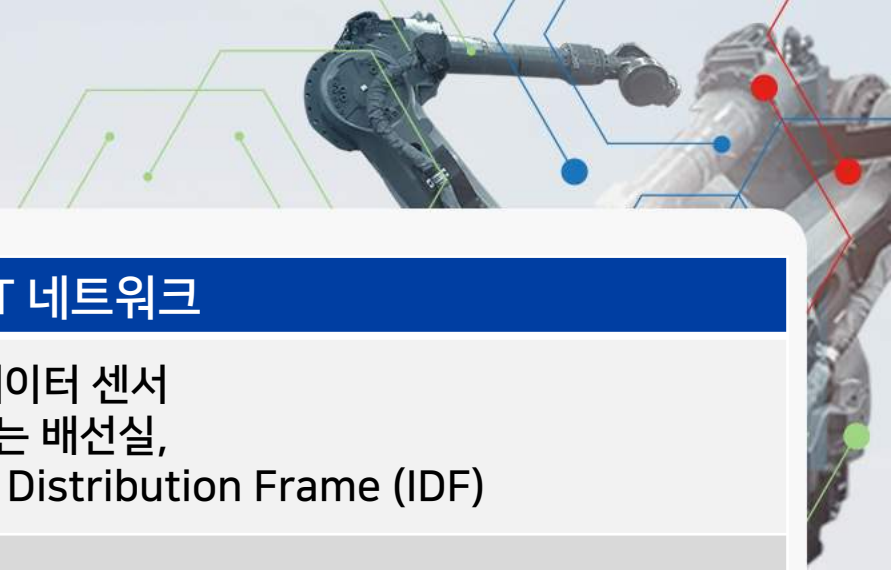


가시성 확보, 빠른 문제 해결, 신속한 네트워크 장비 설정 및 사용

OT-IT 협업/융합/통합 가능

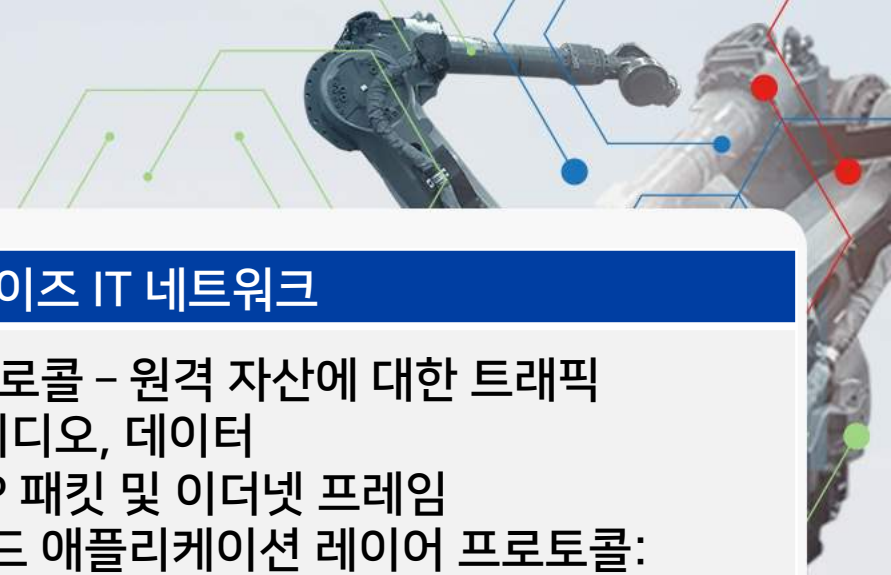


기술과 문화의 융합 – 유사점과 차이점



기준	산업 OT 네트워크	엔터프라이즈 IT 네트워크
환경	• Plant-floor • 제어실 • 제어 판넬, Industrial Distribution Frame (IDF)	• 카페트 공간, 데이터 센서 • 데이터 통신 또는 배선실, Intermediate Distribution Frame (IDF)
스위치	• 관리형, 비관리형 • Layer 2 주로 사용 • DIN 레일 또는 판넬 조립형	• 관리형 • Layer 2 와 Layer 3 • 랙 마운팅
무선	• 자율(로컬에서 관리) – 포인트 솔루션 • 모바일 장비(신규) 및 인력(일반적임)	• 통합(중앙 관리) 솔루션 • 모바일 인력 – 기업 제공 또는 BYOD (Bring Your Own Device) • 외부 접속
컴퓨팅	• 산업용 패널 내장 컴퓨터 및 모니터 • 데스크톱, 노트북 • 19” 랙 서버 • 가상화 – 보편화	• 데스크톱, 노트북 • 테블릿 • 19” 랙 서버 및 블레이드 서버 • 통합 컴퓨팅 시스템 • 가상화 – 널리 퍼짐

기술과 문화의 융합 – 유사점과 차이점



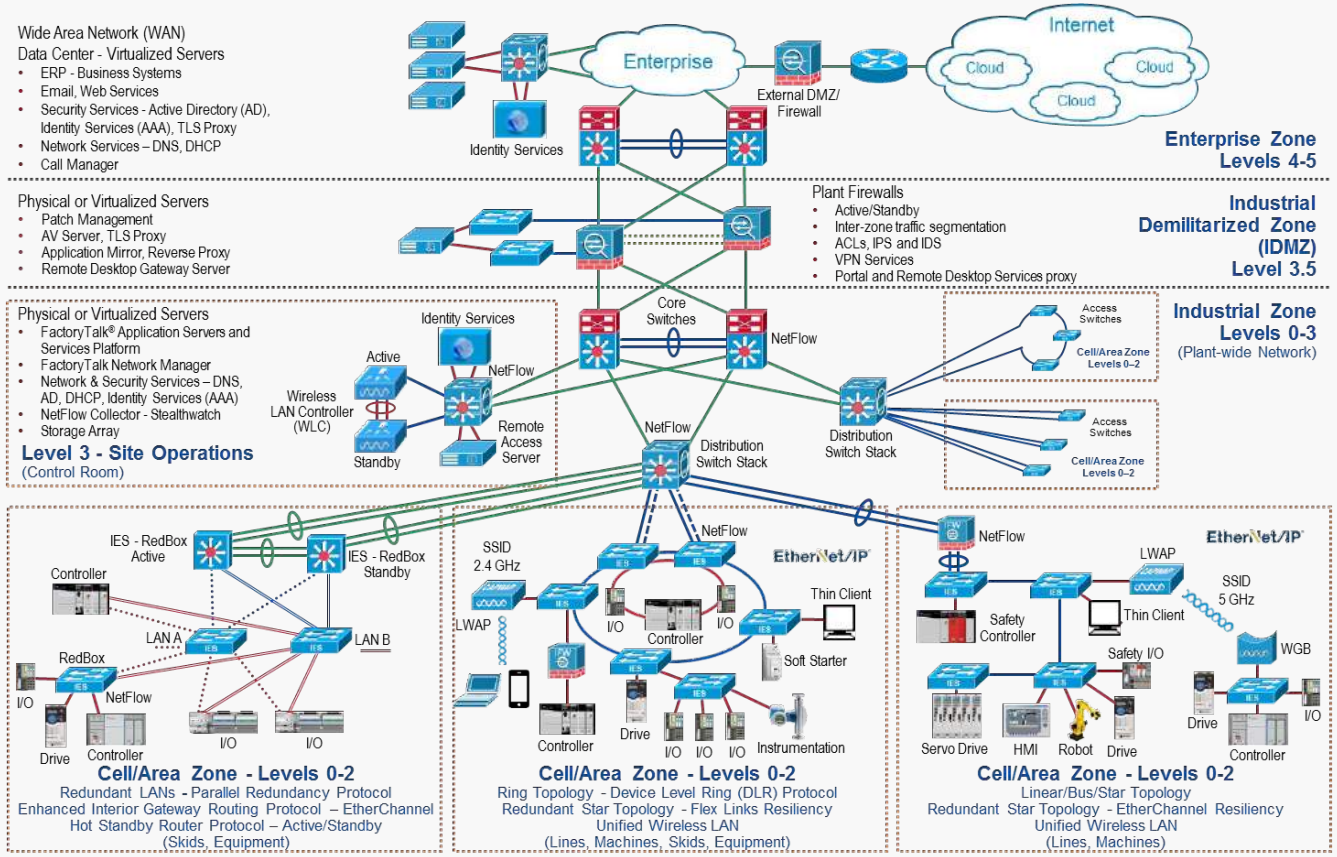
기준	산업 OT 네트워크	엔터프라이즈 IT 네트워크
트래픽 타입	• 주로 로컬 – 로컬 자산간의 트래픽 • 정보, 제어, 안전, 모션, 시간 동기화, 에너지 관리 • 산업용 애플리케이션 레이어 프로토콜: CIP, Profinet, IEC 61850, Modbus TCP, etc.	• 주로 비로콜 – 원격 자산에 대한 트래픽 • 음성, 비디오, 데이터 • 더 큰 IP 패킷 및 이더넷 프레임 • 스텐다드 애플리케이션 레이어 프로토콜: HTTP, SNMP, DNS, RTP, SSH, etc.
성능	• 낮은 지연 시간, 지터 (1 ms, 100s ns) • 데이터 우선순위 – QoS – Layer 2 and 3	• 낮은 지연 시간, 지터 (100s ms, 10s ms) • 데이터 우선순위 – QoS – Layer 3
보안	• 기본적으로 개방되어 있으며 설계, 아키텍처 및 구성에 의해 보호 • 산업 보안 표준 – e.g. IEC, NIST • 일관성 없는 보안 정책 배포 • 기업 또는 인터넷에 대한 연결 없음	• 전사적 연결 • 엔터프라이즈 보안 모법 사례 • 강력한 보안 정책 • 기업 전체와 인터넷에 대한 연결

CPwE(Converged Plantwide Ethernet) 레퍼런스 아키텍처 오버뷰

레퍼런스 아키텍처

❖ 레퍼런스 아키텍처란?

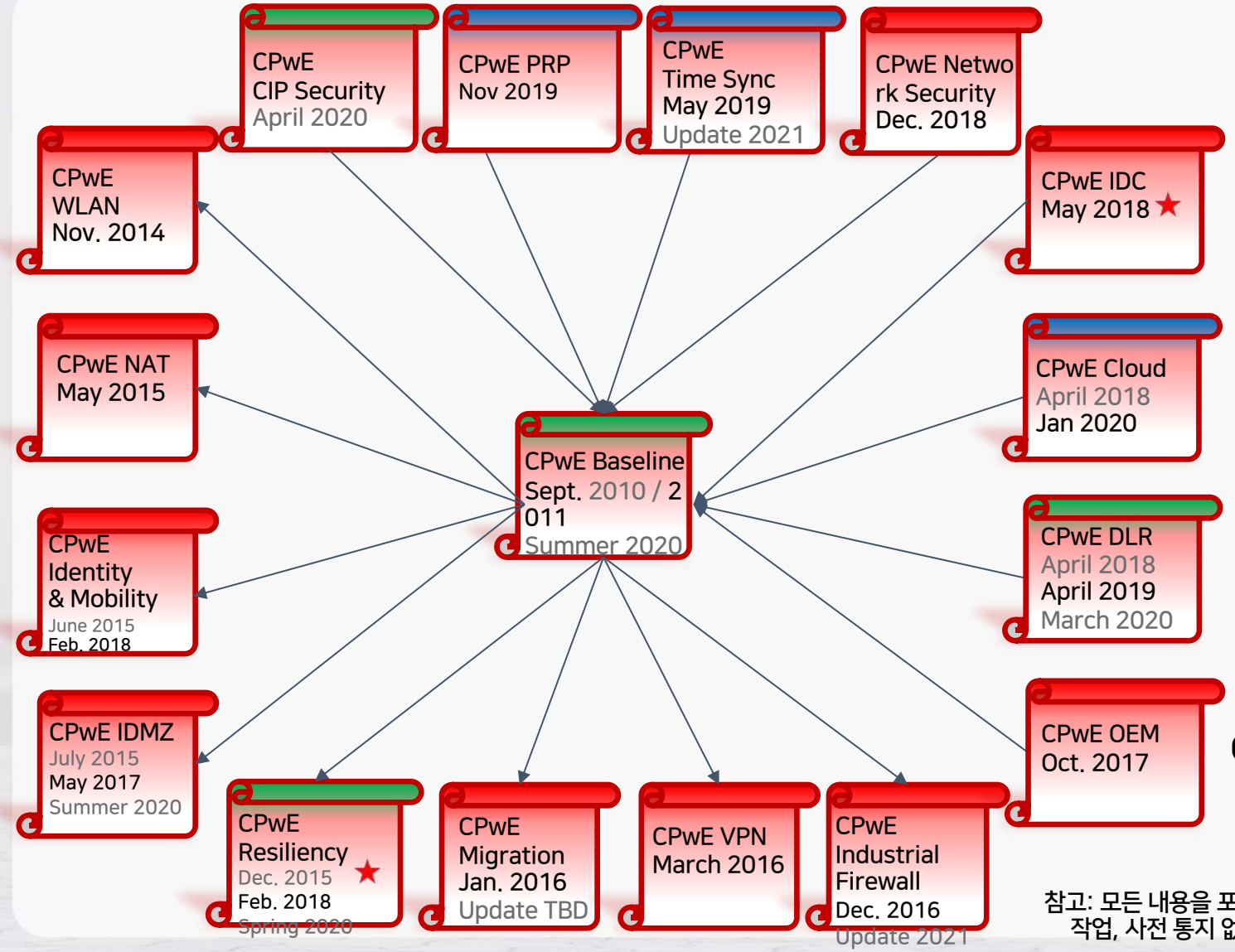
- 설계 및 배포를 위한 기본 아키텍처, 고려 사항 및 모범 사례에 대한 청사진



❖ 레퍼런스 아키텍처:

- 높은 수준의 마케팅 아키텍처 및 일러스트레이션
- 백서 및 지식기반 기사 기반의 PoC 테스팅
- Accelerator Toolkits:
  - 예 – 드라이브, 모션, 안전, 에너지 관리, 수처리 등
- System Configuration Drawings
  - 예 – Stratix®, MCC, Wi-Fi, ControlLogix®
- Converged Plantwide Ethernet (CPwE) Architectures:
  - 설계, 테스트 및 검증된 디자인 모음
    - Test labs – Cisco, Panduit, and Rockwell Automation
  - 백서, 디자인 가이드, 애플리케이션 가이드

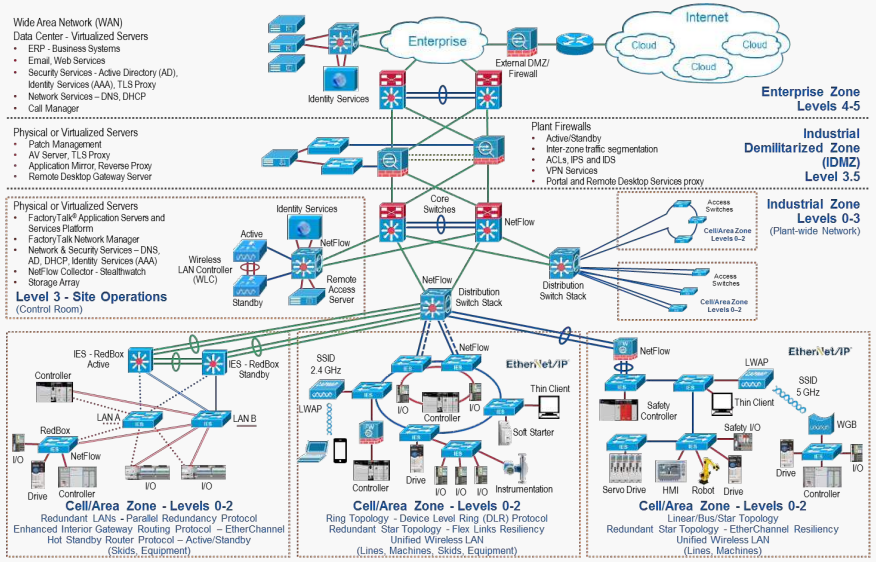
설계, 테스트 및 검증된 디자인 모음



Existing

Recently Published

Work in Progress



Rockwell Automation CISCO PANDUIT

CPwE 테스트 랩

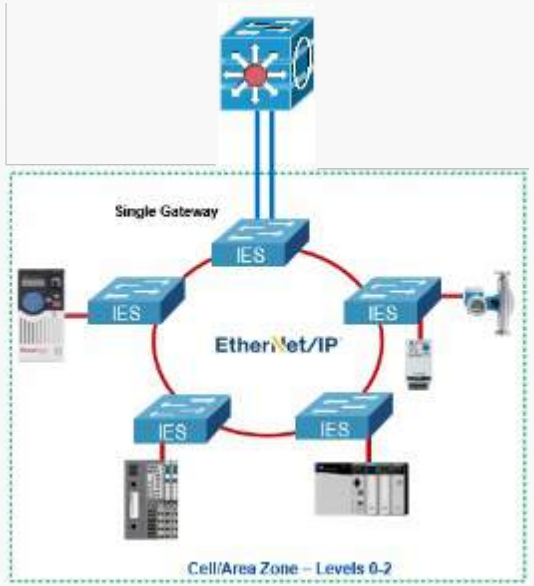
- Rockwell Automation – Mayfield Heights, OH
- Cisco – Raleigh, NC (RTP)
- Panduit – Tinley Park, IL ★

참고: 모든 내용을 포함하지 않으며 현재 진행중인 작업, 사전 통지 없이 내용이 변경 될 수 있음

지속적인 개발 및 업데이트

Phase 1:

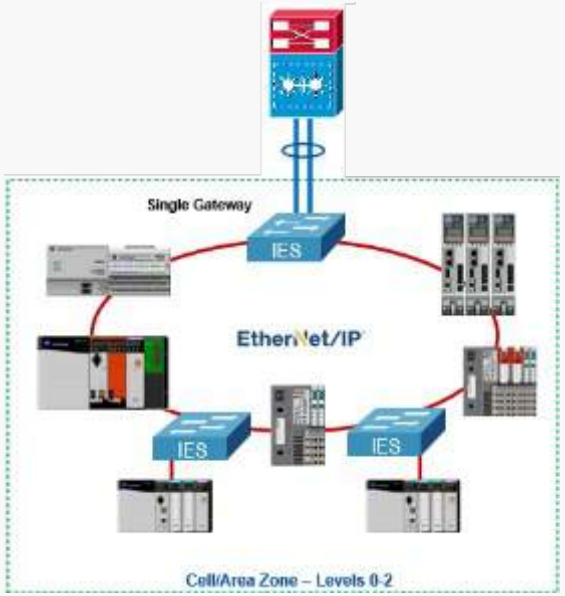
Switch-Level Ring



FY 2018

Phase 2:

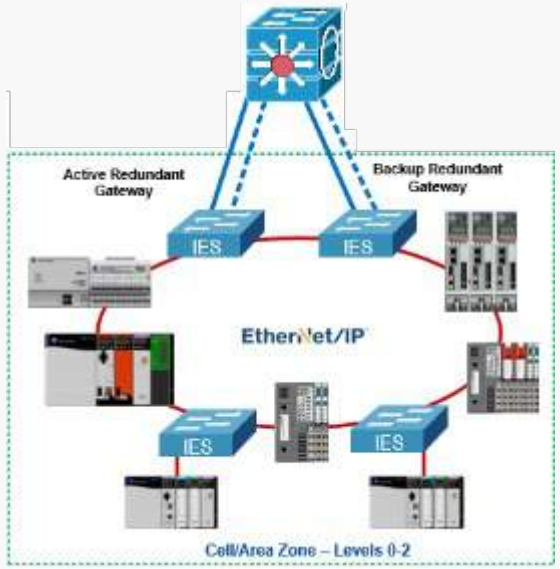
Mixed device/switch-Level Ring



FY 2019

Phase 3:

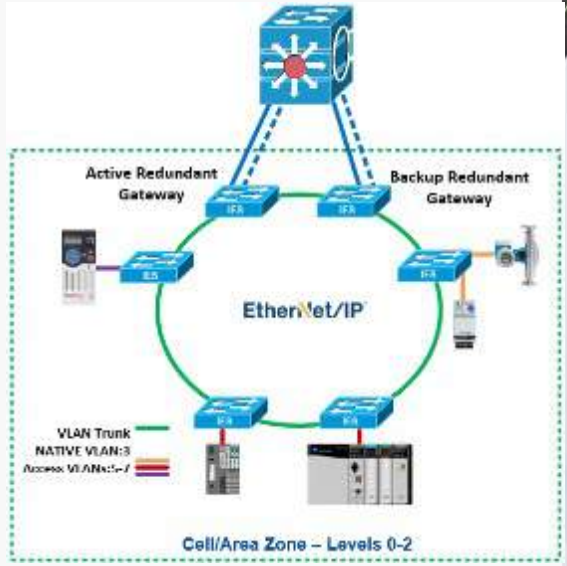
DLR Redundant Gateway



FY 2020

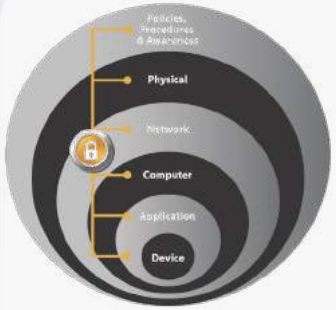
Phase 4:

DLR VLAN Trunking



FY2021

CPwE 산업용 보안 프레임워크



담당 인원

제어 시스템 엔지니어(OT)

IT 네트워크 엔지니어와 협업하는 제어 시스템 엔지니어 (산업용 IT)

제어 시스템 엔지니어와 협력하는 IT 보안 설계자

Web Security Appliance

Enterprise

External DMZ/ Firewall

Internet

Umbrella

Cloud

Cloud

Identity Services

Enterprise Zone: Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Physical or Virtualized Servers
- Patch Management
- AV Server, TLS Proxy
- Application Mirror, Reverse Proxy
- Remote Desktop Gateway Server

Plant Firewalls
- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Standard DMZ Design BEST Practices

Industrial Zone: Levels 0-3

Active Directory (AD)

Firepower Management Center (FMC) Cisco Security Manager

Identity Services Engine (ISE)

FactoryTalk® Security FactoryTalk Policy Manager

Remote Access Server (RAS)

Level 3 – Site Operations

Core Switches

Stealthwatch

FactoryTalk Network Manager™

Active

Wireless LAN Controller (WLC)

Standby

Distribution Switch Stack

NetFlow

Network Infrastructure
- Hardening
- Access Control
- Resiliency

Wireless LAN (WLAN)
- Access Policy
  - Equipment SSID
  - Plant Personnel SSID
  - Trusted Partners SSID
- WPA2 with AES Encryption
- Autonomous WLAN
  - Pre-Shared Key
  - 802.1X - (EAP-FAST)
- Unified WLAN
  - 802.1X - (EAP-TLS)
  - CAPWAP DTLS

Computer Hardening

Application Hardening

FactoryTalk® Client

Level 2 – Area Supervisory Control

NetFlow

Stratix® EtherNet/IP

Port Security
- Physical
- Electronic

LWAP

SSID 2.4 GHz

SSID 5 GHz

WGB

Zoning – Segmenting Domains of Trust (Security Groups)

IACS Device Hardening
- Policies and Procedures
- Physical Measures
- Electronic Measures
- Encrypted Communications

IFW

Industrial Firewall

Controller

Controller

Level 1 - Controller

I/O

Soft Starter

MCC

I/O

Drive

Level 0 - Process

IACS Device Hardening
- Policies and Procedures
- Physical Measures
- Electronic Measure

CIP Security

CIP Security

Defense-in-Depth
- 다양한 위협 탐지 및 보호를 위한 아키텍처 모범 사례

IEC 62443
- 존 & 통신 통로
- 가용성, 무결성, 기밀성

NIST 800-82
- 사이버 보안 프레임 워크
- 식별, 보호, 감지, 응답, 복구

DHS/INL/ICS-CERT
- 권장 사례

설계, 테스트 및 검증된 디자인 모음

토픽	디자인 가이드	백서
Converged Plantwide Ethernet – Baseline Document	ENET-TD001E-EN-P	N/A
Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture	ENET-TD006A-EN-P	ENET-WP034A-EN-P
Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture	ENET-TD008B-EN-P	ENET-WP037C-EN-P
Securely Traversing IACS Data Across the Industrial Demilitarized Zone (IDMZ)	ENET-TD009B-EN-P	ENET-WP038B-EN-P
Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture	ENET-TD007A-EN-P	ENET-WP036A-EN-P
Migrating Legacy IACS Networks to a Converged Plantwide Ethernet Architecture	ENET-TD011A-EN-P	ENET-WP040A-EN-P
Deploying A Resilient Converged Plantwide Ethernet Architecture	ENET-TD010B-EN-P	ENET-WP039D-EN-P
Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture	ENET-TD002A-EN-P	ENET-WP011B-EN-P
Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture	ENET-TD015C-EN-P	ENET-WP016D-EN-P
OEM Networking within a Converged Plantwide Ethernet Architecture	ENET-TD018A-EN-P	ENET-WP018A-EN-P
Cloud Connectivity to a Converged Plantwide Ethernet Architecture	ENET-TD017A-EN-P	ENET-WP019B-EN-P
Deploying Industrial Data Center within a Converged Plantwide Ethernet Architecture	ENET-TD014A-EN-P	ENET-WP013A-EN-P
Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture	ENET-TD016A-EN-P	ENET-WP017B-EN-P
Deploying Network Security within a Converged Plantwide Ethernet Architecture	ENET-TD019A-EN-P	ENET-WP023B-EN-P
Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture	ENET-TD021A-EN-P	ENET-WP041A-EN-P
Deploying CIP Security within a Converged Plantwide Ethernet Architecture	ENET-TD022A-EN-P	ENET-WP043A-EN-P

기술/제품/솔루션 제안

❖ Switching/Routing

Rockwell Automation

- Stratix® 5700, 5400 and 5410
- FactoryTalk® Network Manager™ software

❖ Integrated Architecture® system

- FactoryTalk® Production and Performance Suite
- Programmable Automation Controllers
- Kinetix® Servo Drives

❖ Intelligent Motor Control

- PowerFlex® Variable Frequency Drives
- Motor Control Centers, Soft Starters, Overloads
- Power Monitoring, Condition Monitoring

❖ Security

- Stratix® 5950, FactoryTalk® AssetCentre, FactoryTalk Security software, FactoryTalk Policy Manager software, CIP Security™ protocol

❖ Switching/Routing

- Catalyst 3850, 4500-X, 6800, 9300, 9500

❖ Unified WLAN

CISCO

- Wireless LAN Controller (WLC)
- Lightweight Access Point (LWAP)

❖ Unified Computing System (UCS)

❖ Security

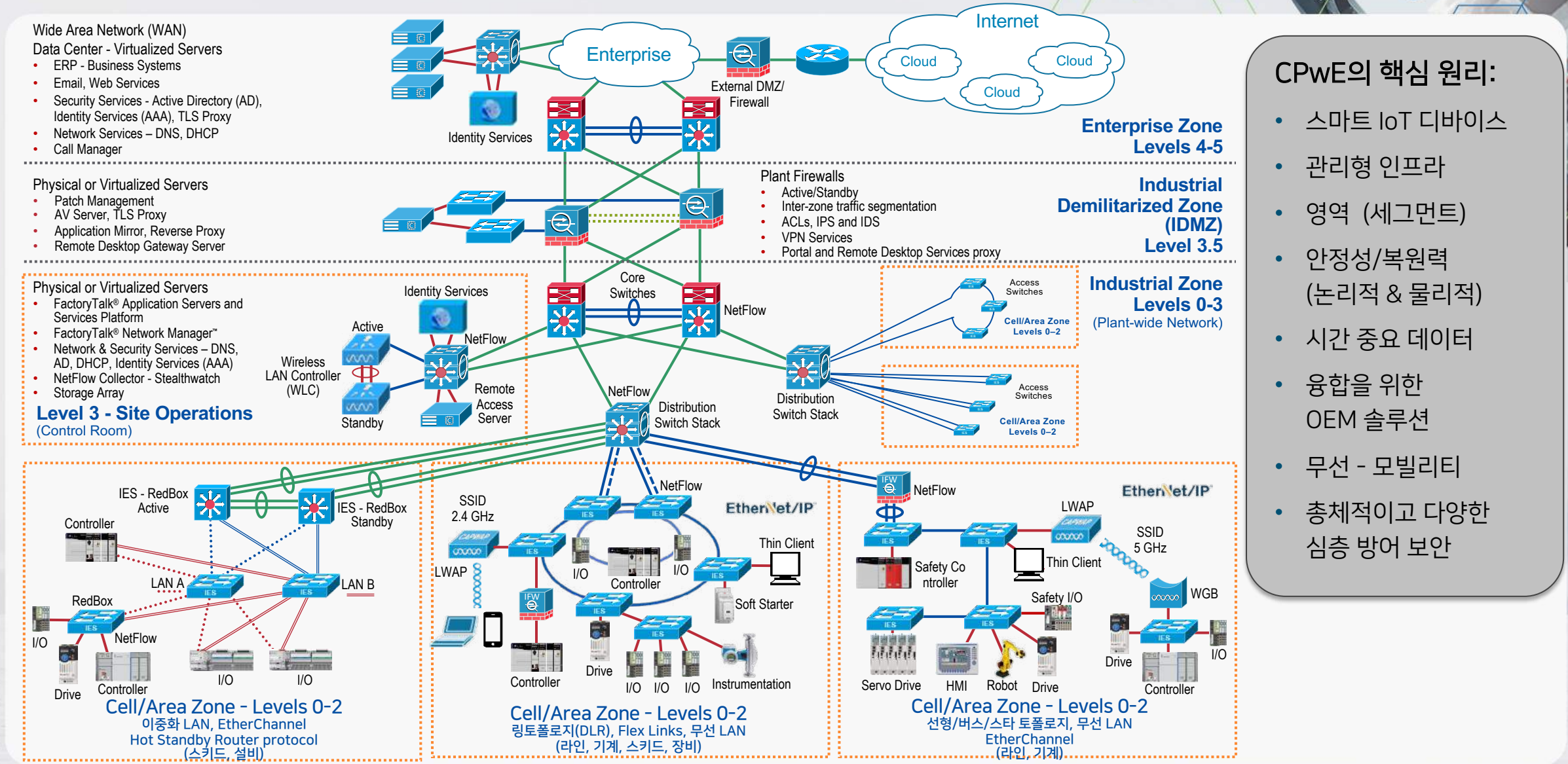
- NGFW - Firepower Firewall and Firepower Management Center
- Identity Services Engine (PAN, PSN, MnT)
- Stealthwatch – Network Traffic Flow Analysis
- Umbrella - OpenDNS

❖ Physical Infrastructure Solutions

PANDUIT®

CPwE 아키텍처의 주요 원리

설계, 테스트 및 검증된 디자인 모음



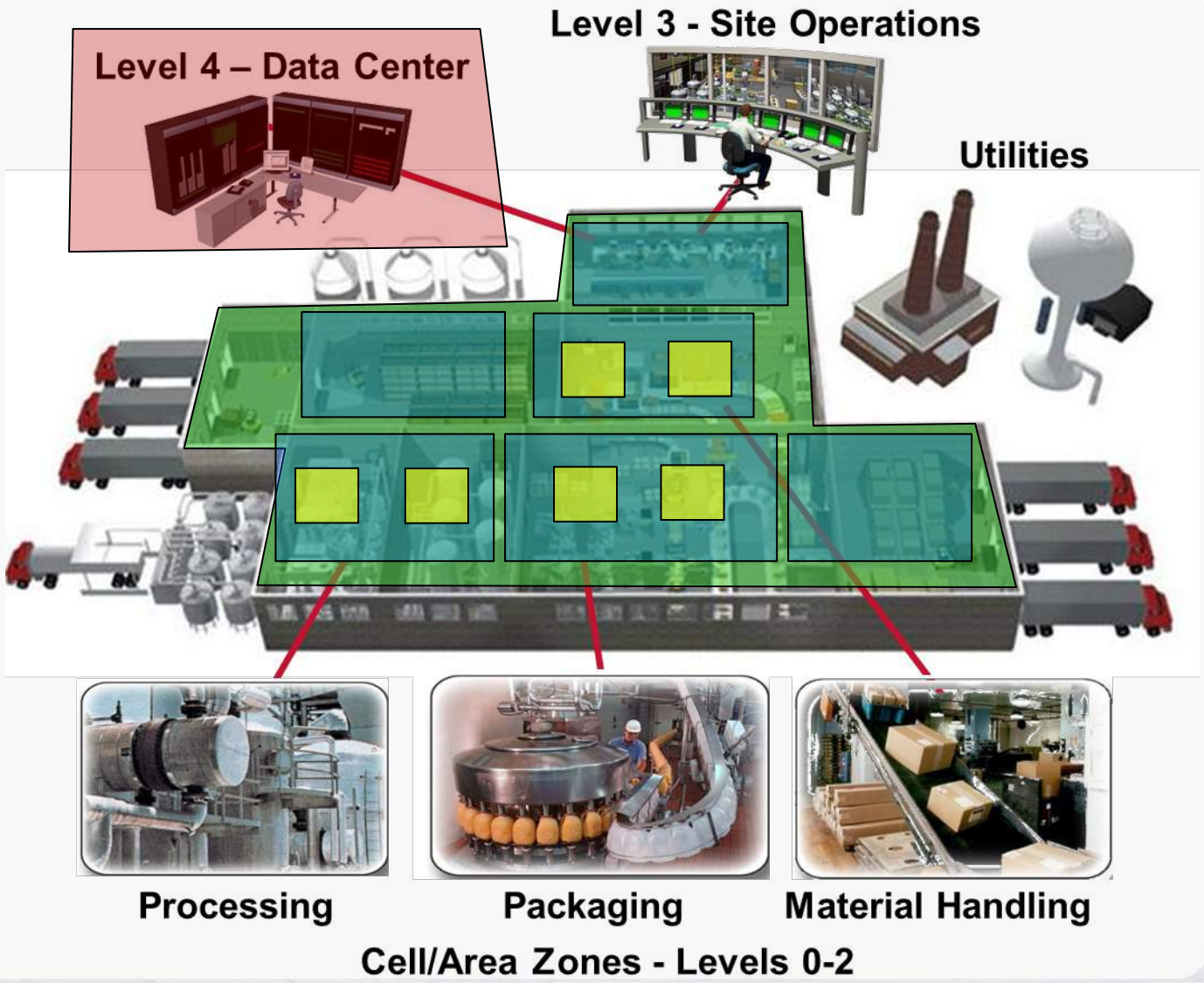
CPwE의 핵심 원리:

- 스마트 IoT 디바이스
- 관리형 인프라
- 영역 (세그먼트)
- 안정성/복원력 (논리적 & 물리적)
- 시간 중요 데이터
- 융합을 위한 OEM 솔루션
- 무선 - 모빌리티
- 총체적이고 다양한 심층 방어 보안

플랜트 전체 구역 설정 – OT 기준

플랜트 전체 구역 설정

- 기능 영역/보안 그룹
- 작게 연결된 LANs
  - 소규모 브로드 캐스트 및 장애 도메인
  - 더 작은 신뢰 영역(보안 그룹)
- IACS 애플리케이션 마이크로 세그먼트
- 보안 표준과 얼라인
  - IEC 62443-3-2, 보안 영역 및 보안 연결 모델
  - DHS/INL/ICS-CERT 권장 사항
- 산업용 IoT 기술 믹스
- 확장성을 위한 빌딩 블록 접근 방식



OT-IT 협업/융합/통합 소프트웨어 보안 그룹 세분화

OT 기반 보안,
OT IIoT 장치에 대한 가시성,
OT 사용자의 컨텍스트 및 의도,
IT에 의한 시행

산업용 자산


HMI


Controller


Drive


I/O

CIP™

CIP™

CIP™

CIP™

Other Protocols

OT 플랫폼

VISIBILITY

INTENT

pxGrid

FactoryTalk®
Network Manager™

IT 플랫폼

ISE

Network Security Use Cases

CONTEXT

SGACL
Enforcement Policies

산업용 이더넷 스위칭

다이나믹 보안 그룹 세분화

CONTEXT

SXP
(IP to SGT Mappings)

차세대 방화벽

온디맨드 원격 접속

pxGrid

CONTEXT

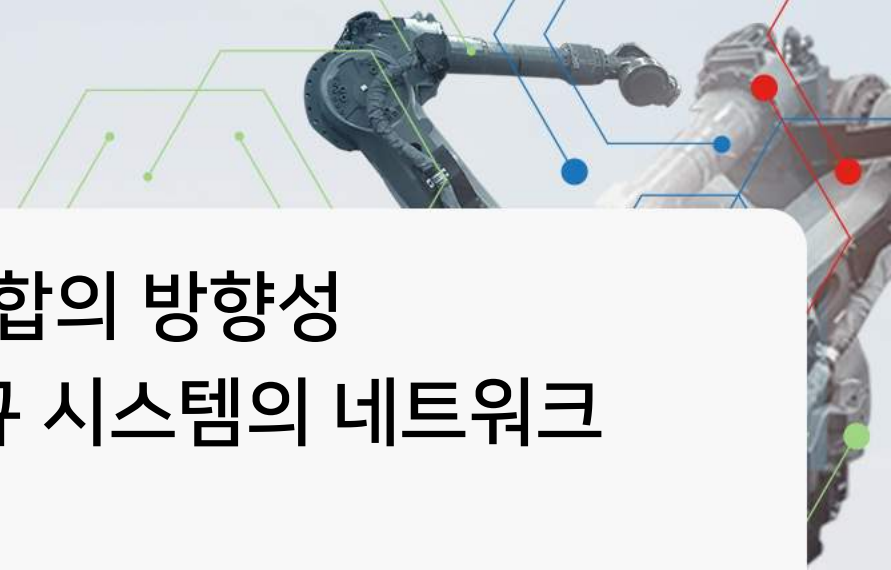
스텔스 위치

컨텍스트 기반 이상 감지

Rockwell Automation

CISCO

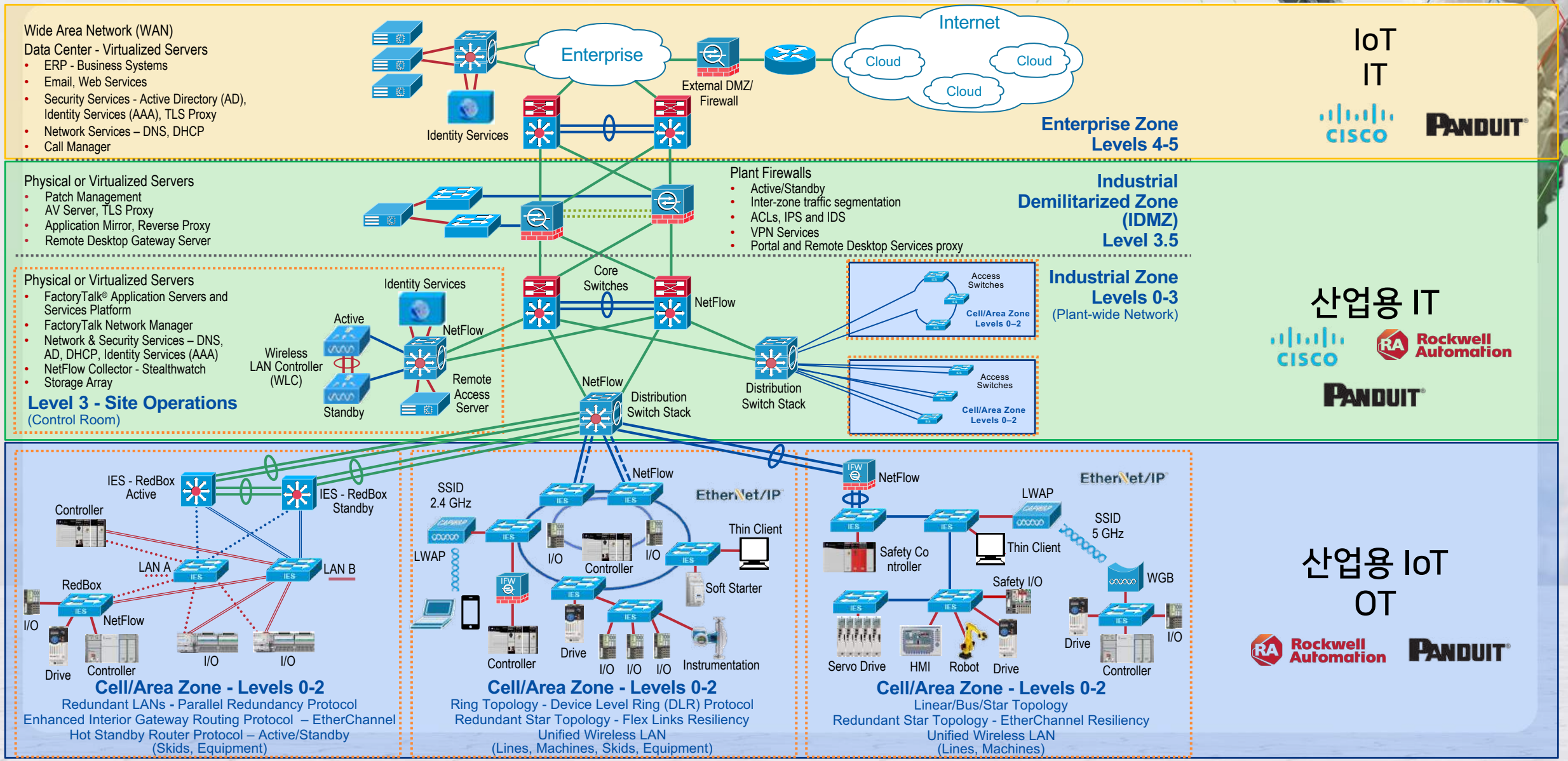
Summary



- ✓ 스마트 팩토리 여정을 위한 IT-OT 네트워크 융합의 방향성
- ✓ 비즈니스 확장을 위한 기존 시스템 개선 및 신규 시스템의 네트워크 표준화

- ✓ 로크웰 오토메이션과 시스코, Panduit은 전략적 파트너
- ✓ 17개 이상의 설계, 테스트 및 검증된 디자인 모음
- ✓ 검증된 레프런스 아키텍처

CPwE – OT-IT 연결


Wide Area Network (WAN)
Data Center - Virtualized Servers
• ERP - Business Systems
• Email, Web Services
• Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
• Network Services – DNS, DHCP
• Call Manager
Enterprise
Internet
Cloud
Cloud
Cloud
External DMZ/ Firewall
Identity Services
Enterprise Zone Levels 4-5
IoT
IT
CISCO
PANDUIT
Physical or Virtualized Servers
• Patch Management
• AV Server, TLS Proxy
• Application Mirror, Reverse Proxy
• Remote Desktop Gateway Server
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services
• Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ) Level 3.5
Physical or Virtualized Servers
• FactoryTalk® Application Servers and Services Platform
• FactoryTalk Network Manager
• Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
• NetFlow Collector - Stealthwatch
• Storage Array
Level 3 - Site Operations
(Control Room)
Identity Services
Active
NetFlow
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Core Switches
NetFlow
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone Levels 0-3
(Plant-wide Network)
산업용 IT
CISCO
Rockwell Automation
PANDUIT
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBox
NetFlow
I/O
Drive
Controller
I/O
I/O
Cell/Area Zone - Levels 0-2
Redundant LANs - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
NetFlow
SSID 2.4 GHz
EtherNet/IP
LWAP
I/O
Controller
I/O
Thin Client
Soft Starter
Drive
Controller
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0-2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
NetFlow
EtherNet/IP
LWAP
SSID 5 GHz
Safety Co ntroller
Thin Client
Safety I/O
WGB
Servo Drive
HMI
Robot
Drive
Drive
I/O
Controller
Cell/Area Zone - Levels 0-2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
산업용 IoT
OT
Rockwell Automation
PANDUIT

Thank you