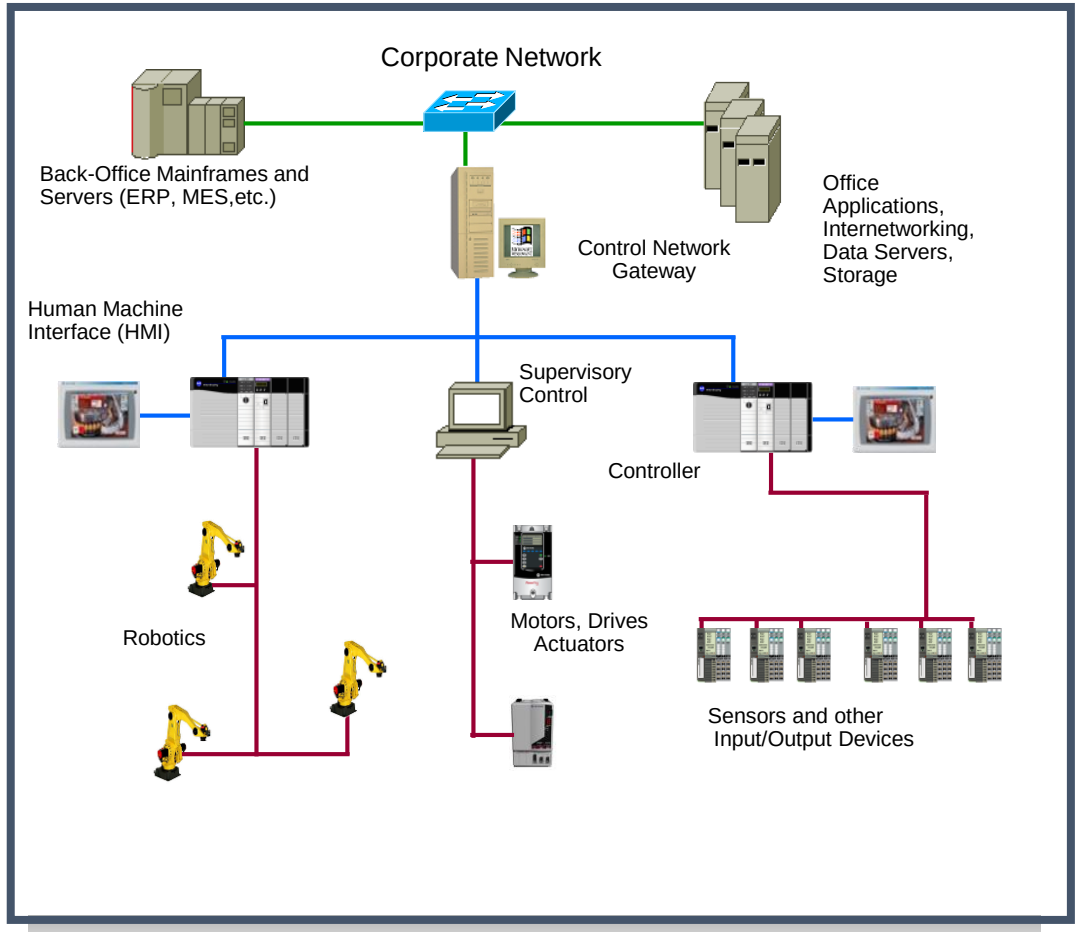
IT / OT Network Design

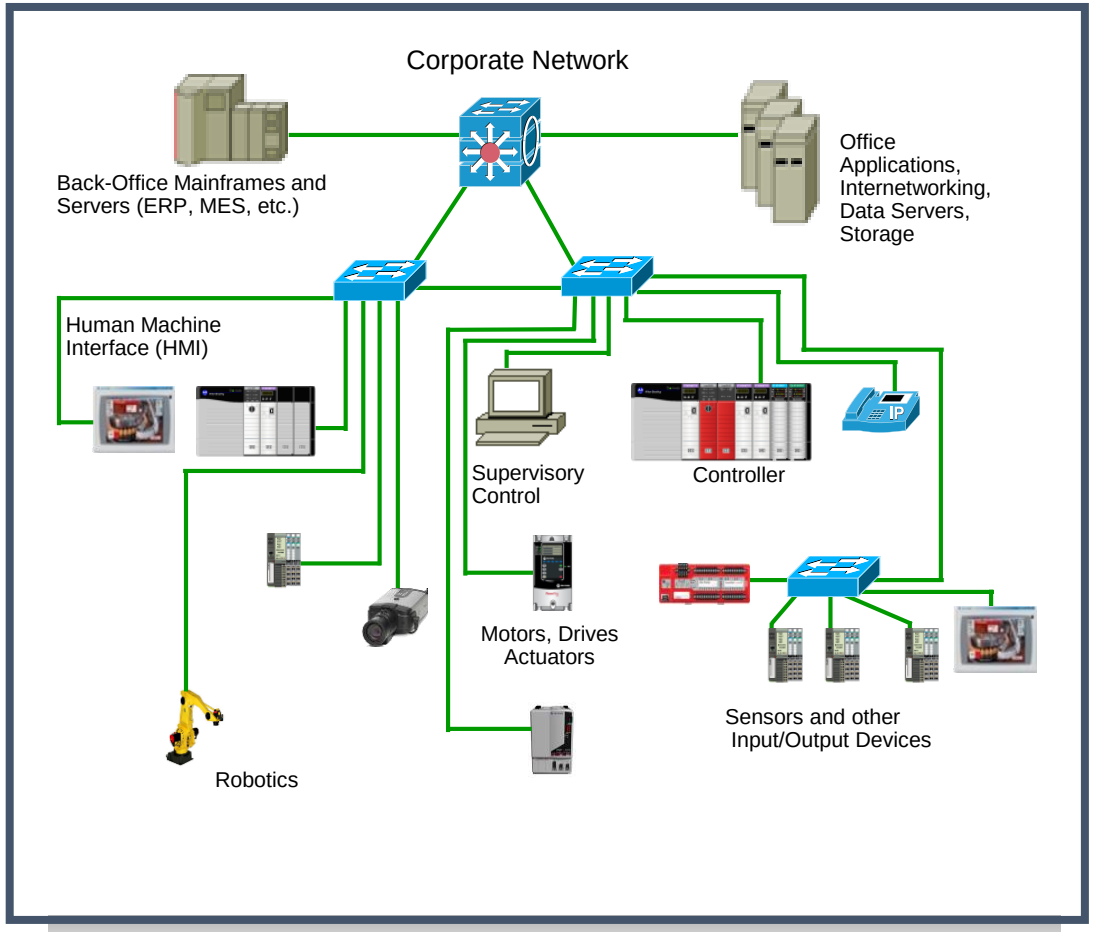
Best Practices

Mikkel Brodersen
Systems Engineer, Cisco Systems, Danmark

Oktober 2018

Industrial Network Convergence





Traditional

Converged Ethernet

Benefits of Industrial Ethernet in Factory Networks

Increased Visibility

- Connectivity to devices and controllers
- Manufacturing—enterprise integration

Uptime and Performance

- Security and reliability
- Network resiliency

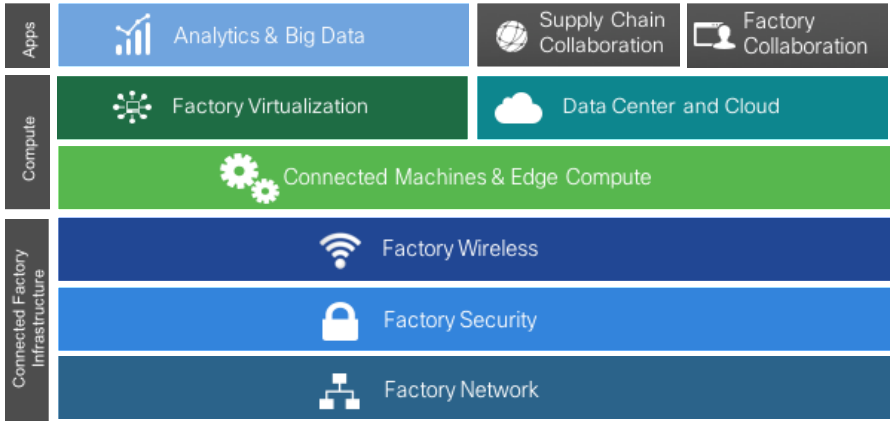
Increased Efficiency

- Standard architecture—integration and support
- Scalable network platform—multiple applications

Improved Event Response

- Remote access
- Improved diagnostics and support

Connected Factory Solution



WHAT IS IT

Unified Converged Factory Network

CHALLENGE

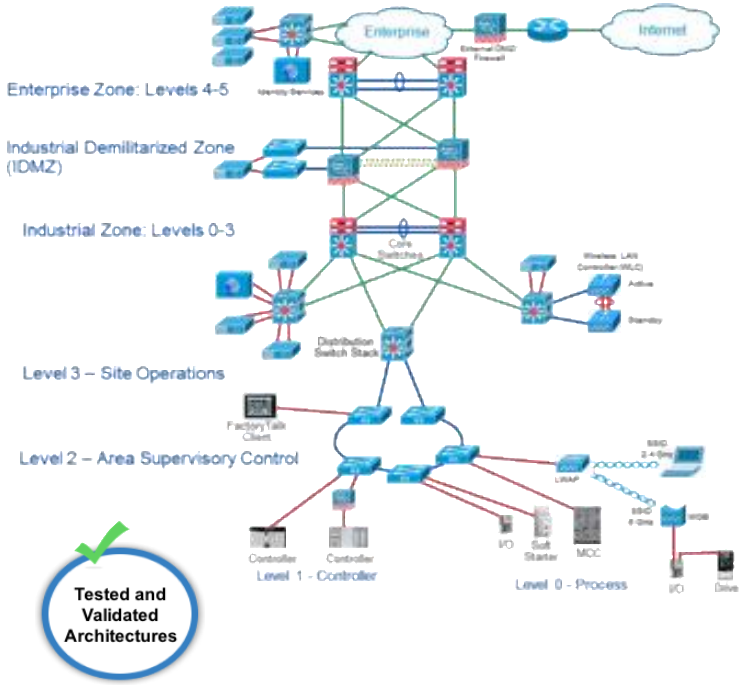
Complex network silos creating downtime, data isolation and vulnerabilities. Inflexible and high TCO.

"Network issues took us hours and sometimes days to troubleshoot. The downtime associated with these issues was extremely costly." *- Dave Gutshall – Harley Davidson*

CRITICAL NEEDS

- Converged Network for Flexible Automation
- Security Built-in
- Simple
- Rapid Fault Isolation
- Resiliency
- Quality of Service
- Ease of use (NAT)
- App / Data Integration
- Ruggedized

ARCHITECTURE



BUSINESS OUTCOMES

OEE Improvement

Reduced Downtime

Connected Factory
Designed for Digital Manufacturing

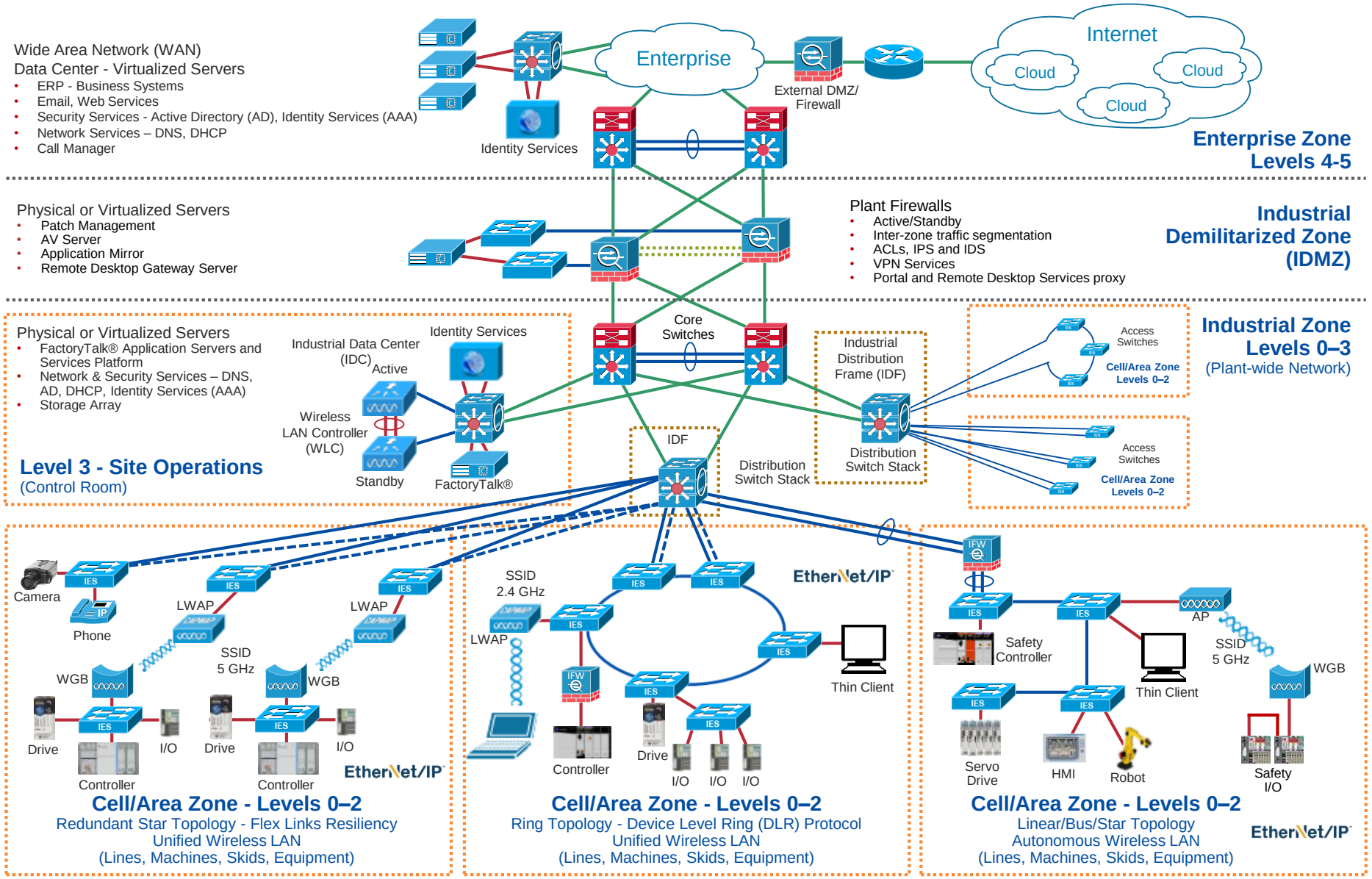
PROFINET INDUSTRIAL ETHERNET

EtherNet/IP™

Modbus

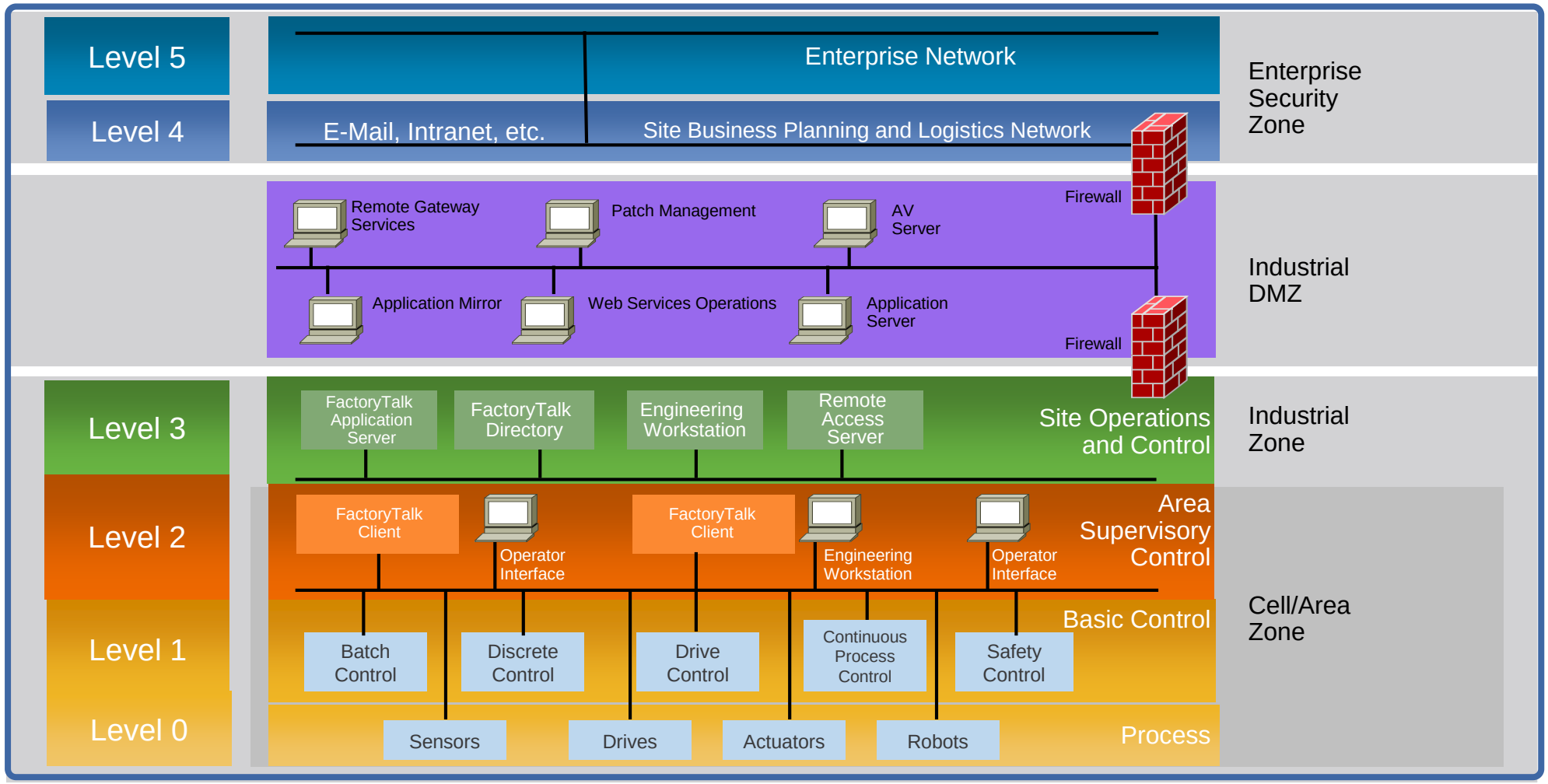
CC-Link IE

Connected Plantwide Ethernet Architectures



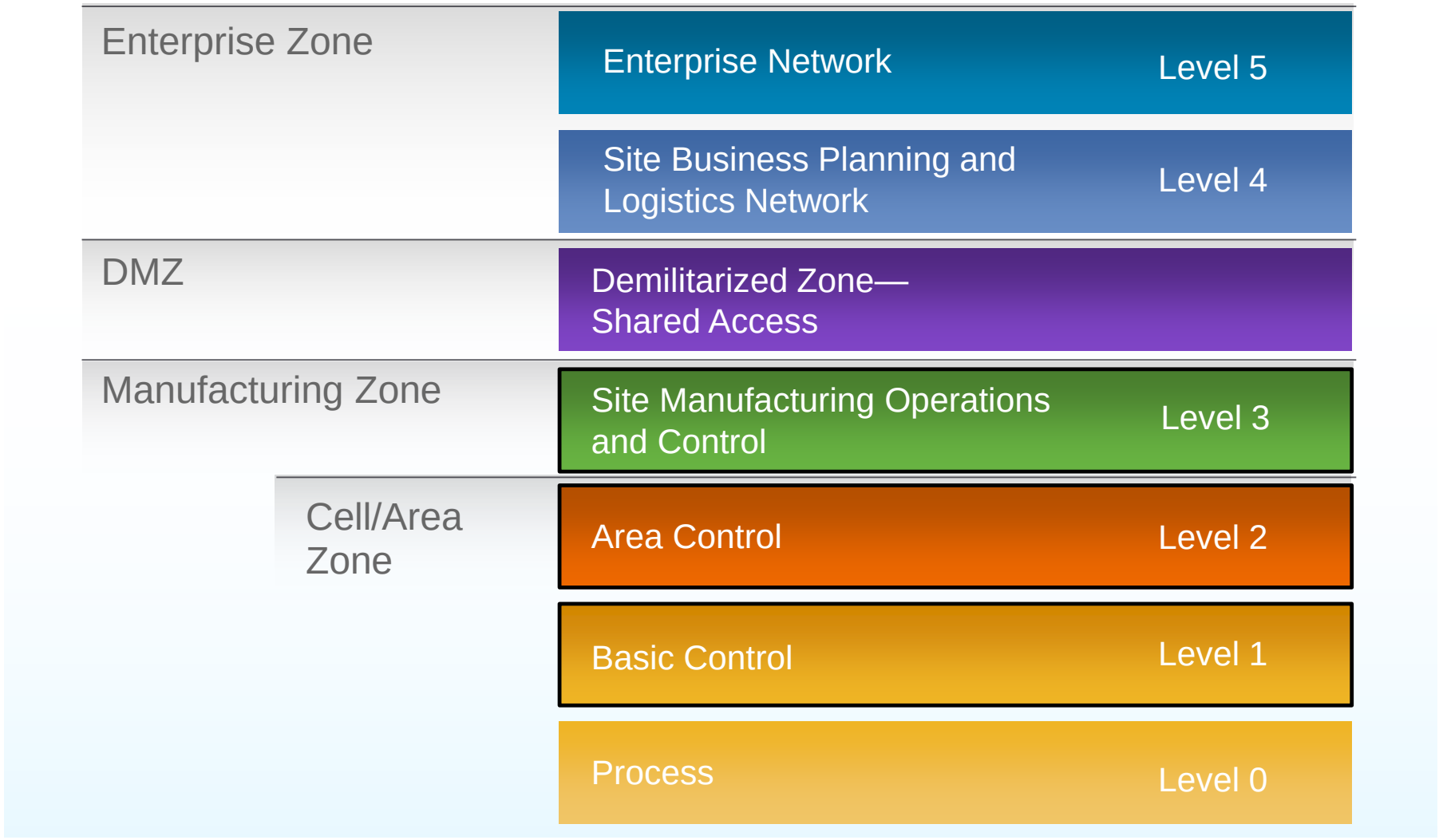
Built on Industry Standards

ISA95/Purdue Reference Model



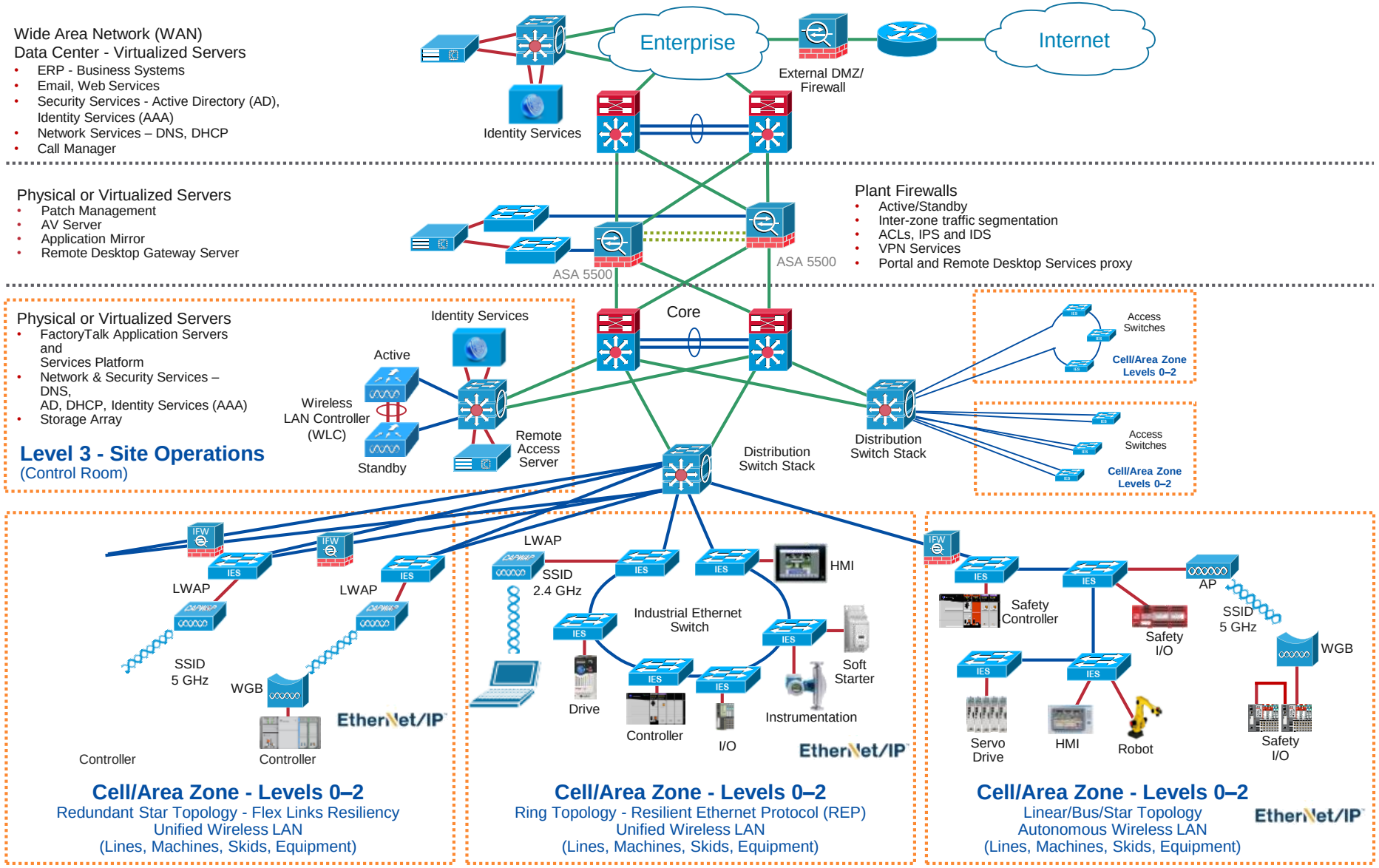
Logical Architecture

Built on Industry Standards



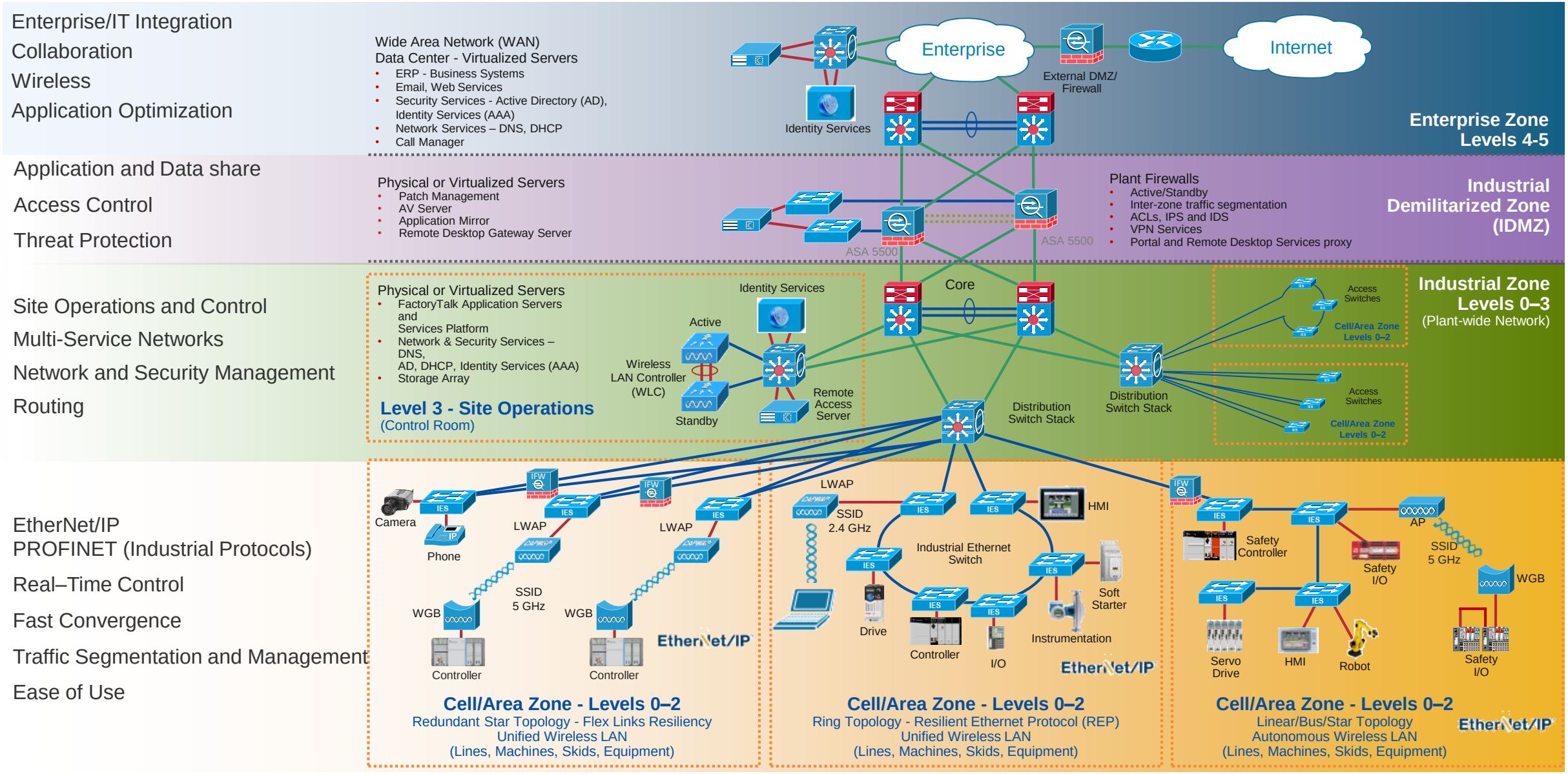
Converged Plantwide Ethernet (CPwE)

Reference Architecture



Converged Plantwide Ethernet (CPwE)

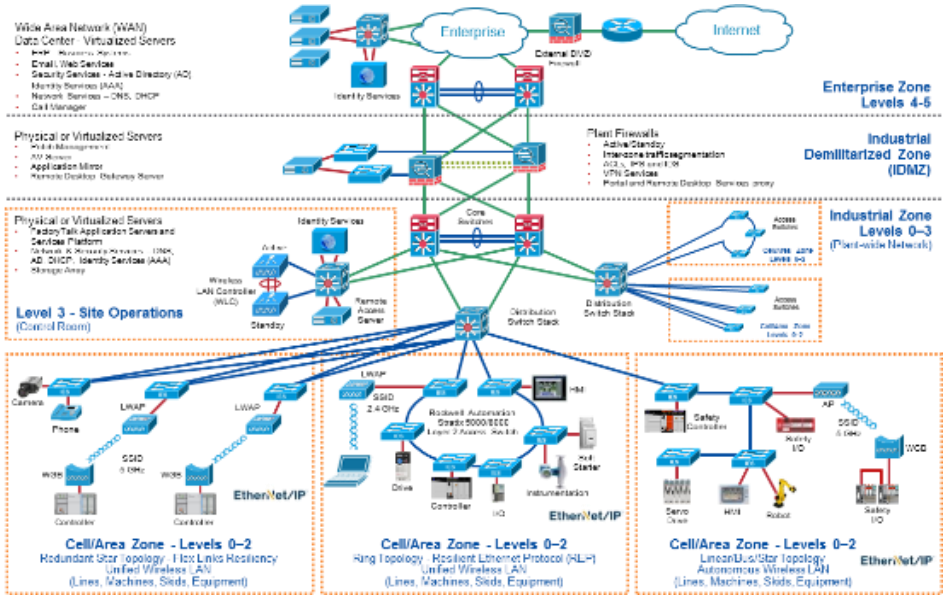
Reference Architecture



Connected Factory Reference Architectures

Converged Plantwide Ethernet (CPwE)

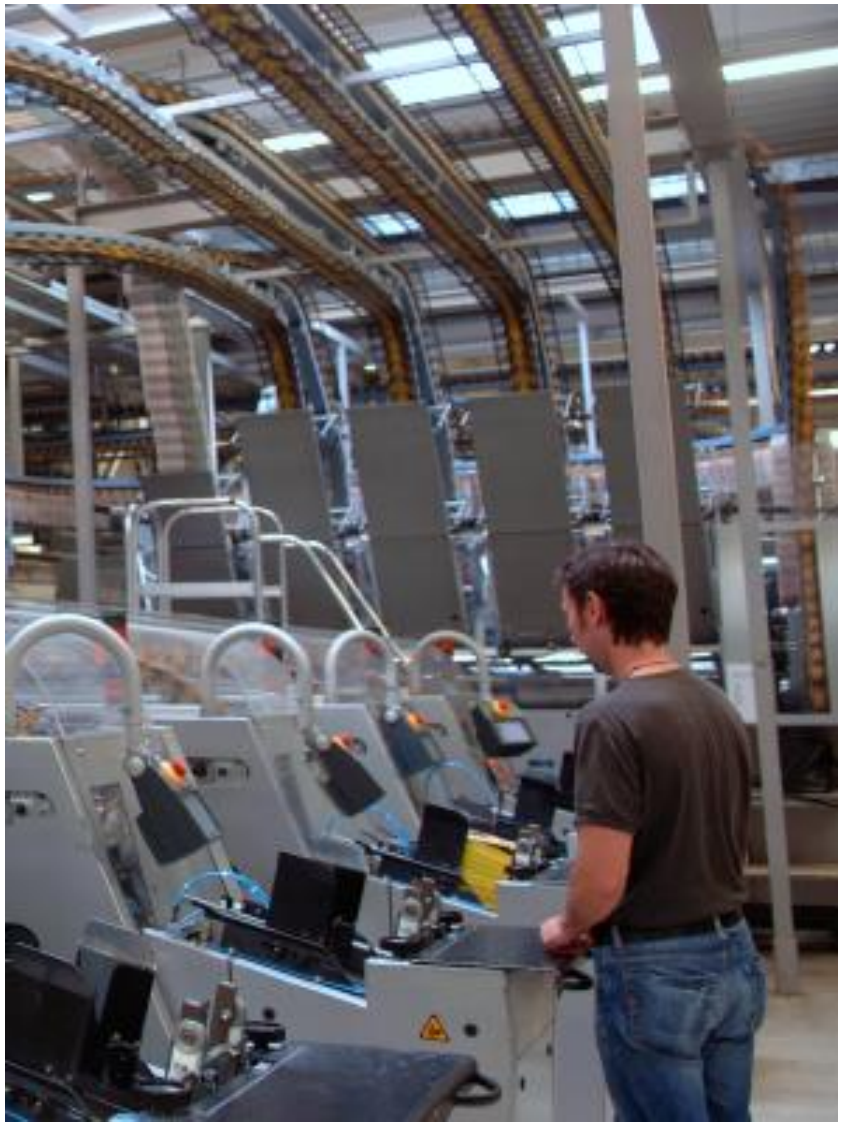
- Tested, validated and documented reference architectures
  - Developed from use cases - customer and application
  - Tested for performance, availability, repeatability, scalability and security
  - Comprised of Cisco® and Rockwell Automation® Validated Designs
- Built on technology and industry standards
  - "Future-ready" network design
- Content relevant to both OT and IT Engineers
- Deliverables
  - Recommendations, best practices, design and implementation guidance, documented test results and configuration settings
  - Simplified design, quicker deployment, reduced risk in deploying new technology



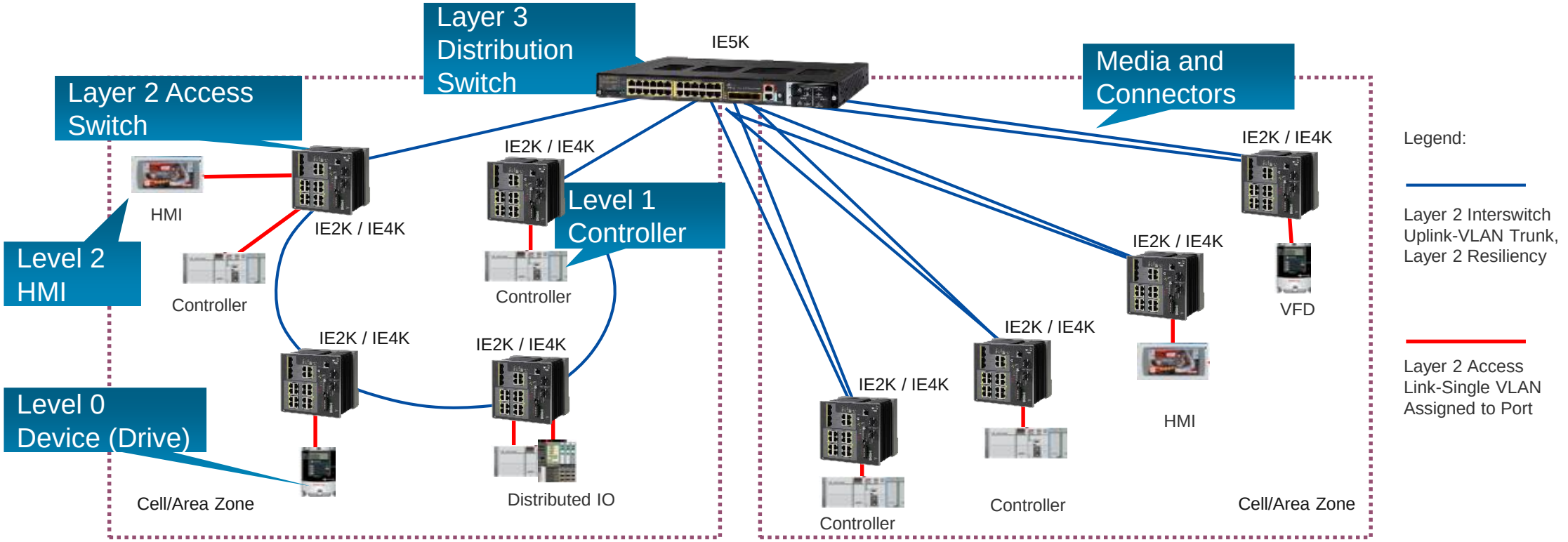
Networking Best Practices – Cell/Area Zone

Best Practices For Reducing Latency and Jitter,
and to Increase Data Availability, Integrity and Security

- IP Multicast Control
  - IGMP Management
- Segmentation
  - Virtual LANs (VLANs)
- Prioritization
  - Quality of Service (QoS)
- Apply Resiliency Protocols and multi-path topologies
  - Use Fiber-media uplinks for fast convergence
- Defense-in-Depth Security



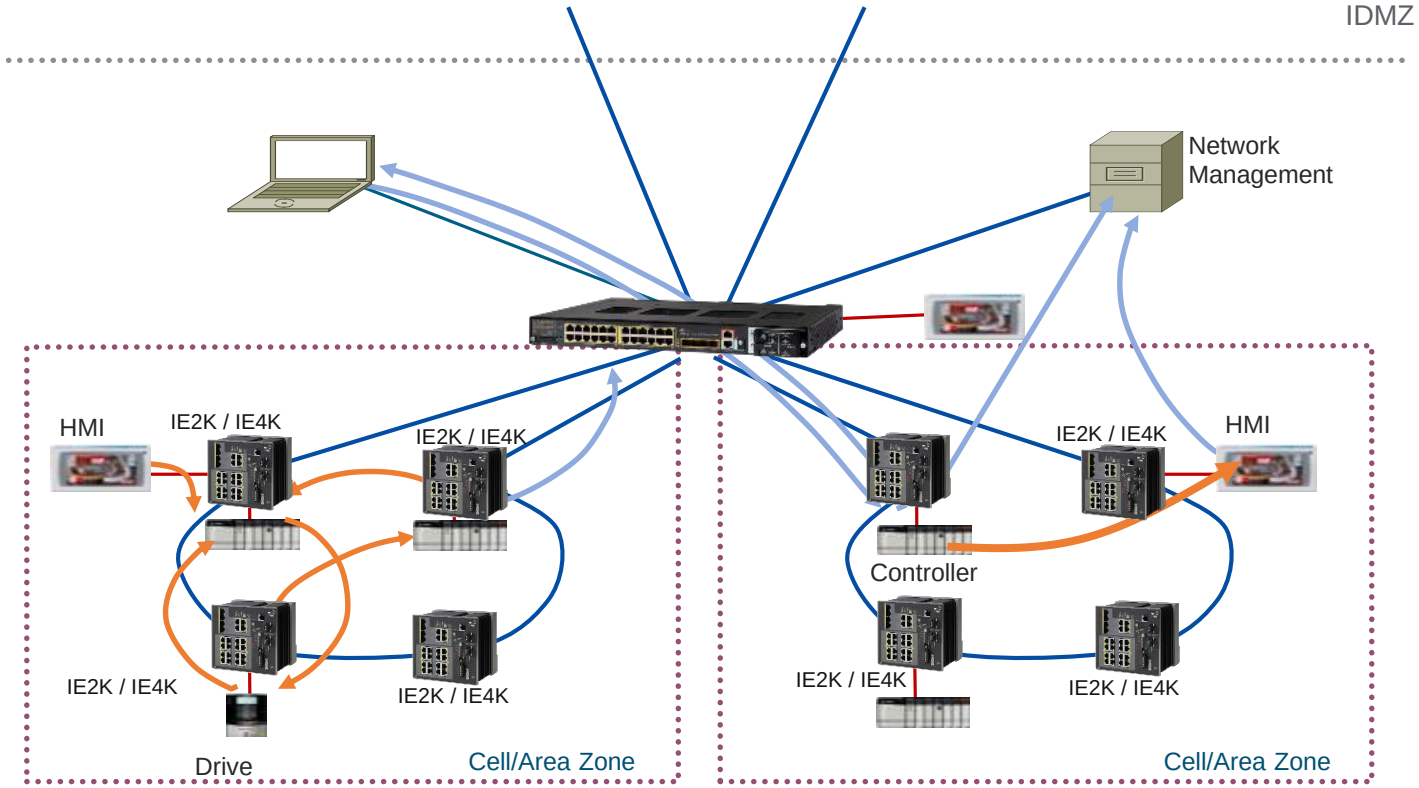
Cell/Area Zone Overview



Cell/Area Zone - Functional Area of a Production Facility.
Considerations Include:

- Environmental constraints
- Range of device intelligence
- Time-sensitive applications

Typical Cell/Area Zone Traffic Flows



CIP Implicit - Producers & Consumer

>80% local

Cyclical I/O traffic, **UDP** unicast and multicast

<500 Bytes, **Frequent**

0.5 to 10's of ms, typically 20 ms

CIP Explicit - Informational control and administration

Intra- and inter-cell/area zone traffic flow

Non-critical administrative or data traffic using **TCP**

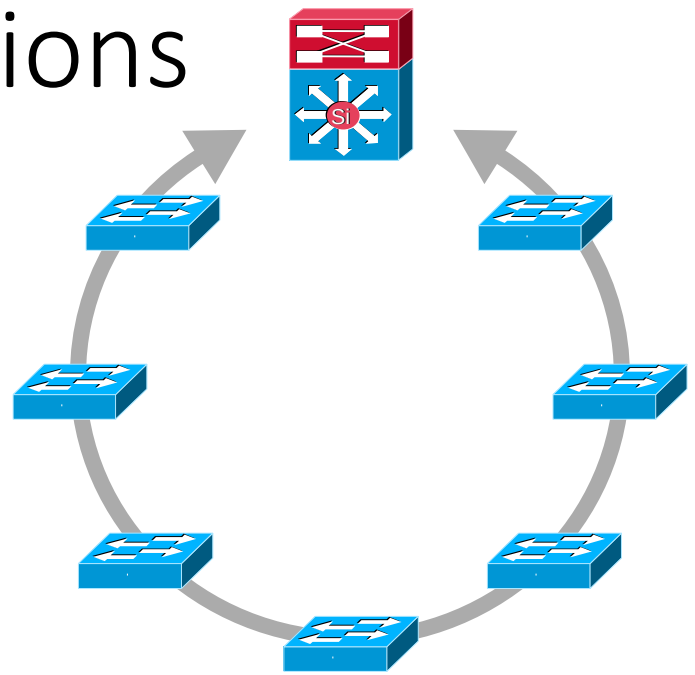
~1500 Bytes, **infrequent**

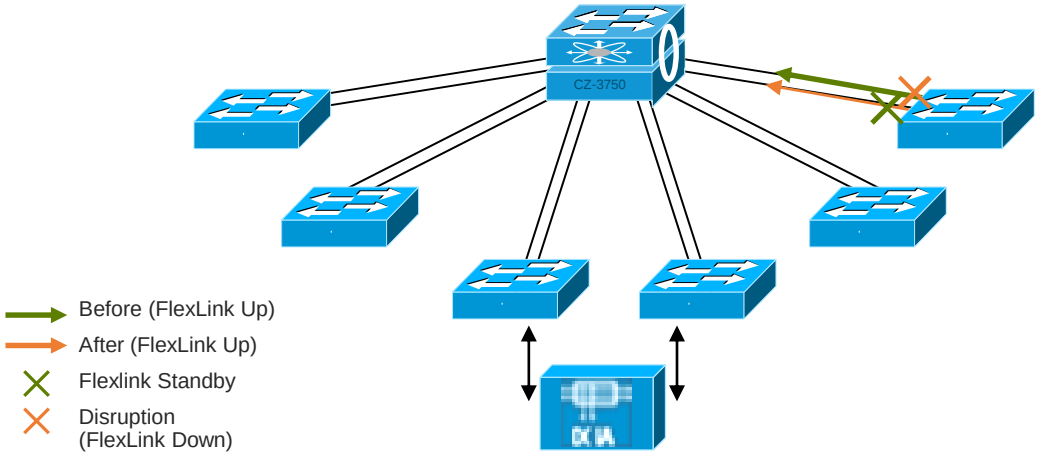
Above 500 ms

Resiliency for Industrial Applications

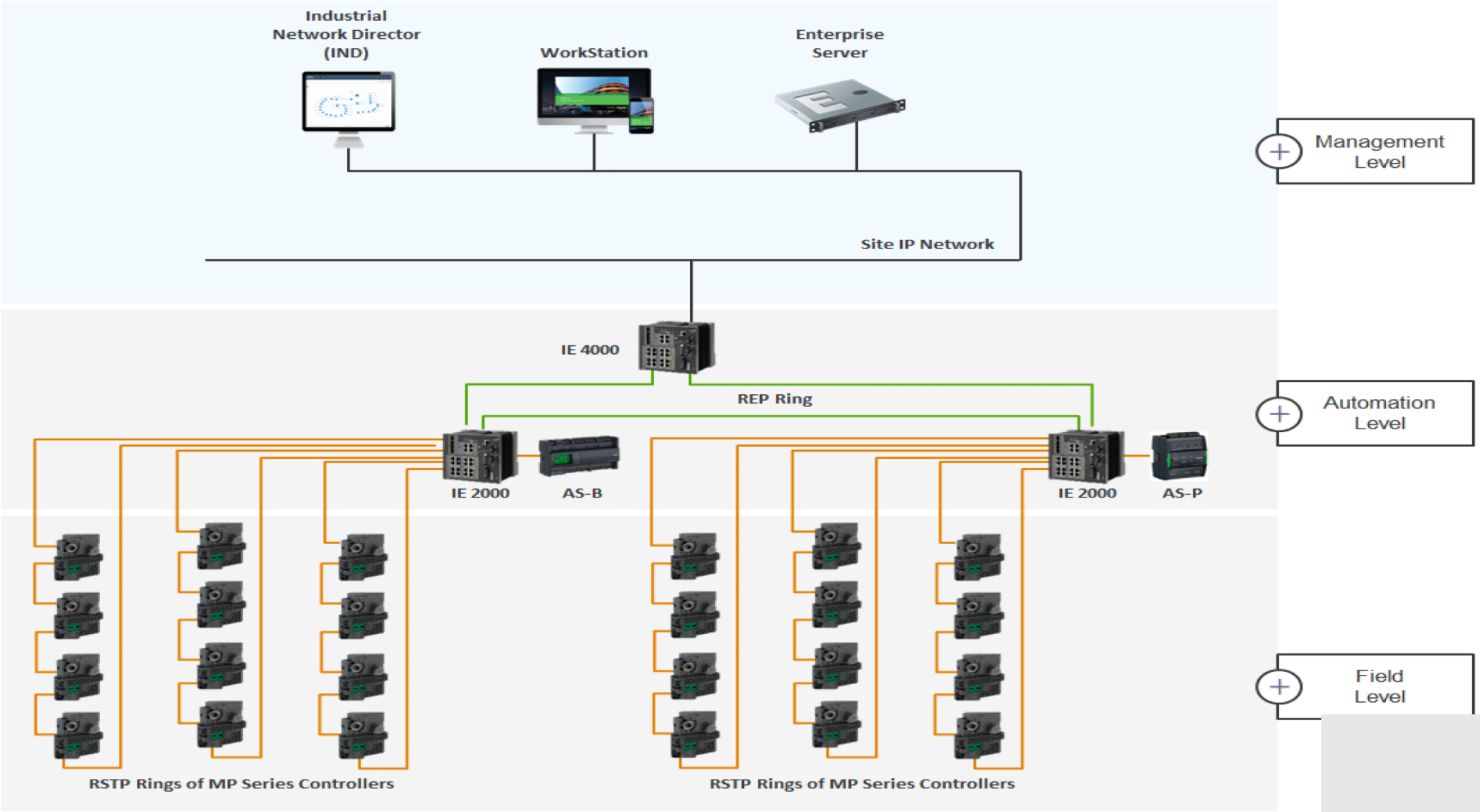
Supporting Multiple Topologies

- Ring Convergence
  - Resilient Ethernet Protocol (REP)
  - Achieves ~50 ms convergence in large, complex networks
- Redundant Star Convergence
  - Multiple protocol options
  - Convergence times of <100ms for Flexlinks and Etherchannel
- Tested with Rockwell applications and multicast traffic
- Fast convergence avoids application reset and improves uptime
- Critical for industrial applications





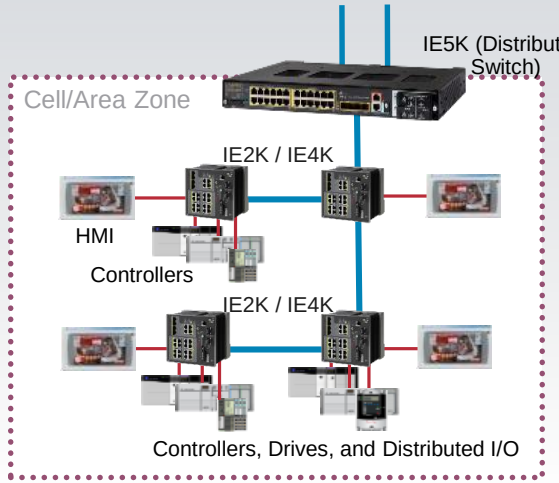
Schneider EcoStructure Building Network



Industrial Network Topologies

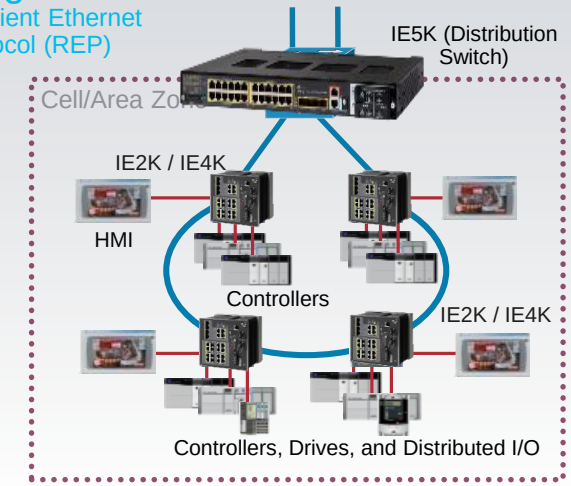
Cell/Area Zone Topology Options

Star/Bus Linear



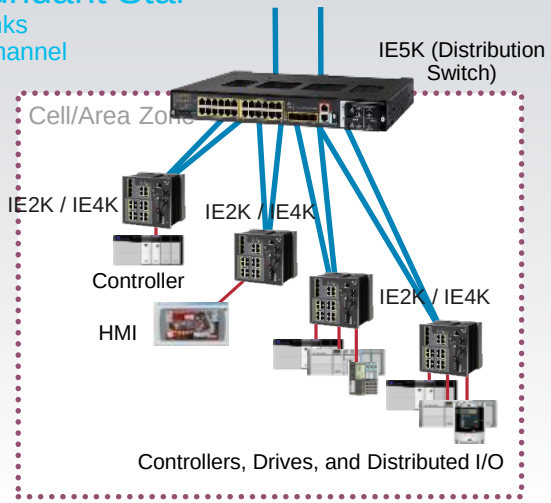
Ring

Resilient Ethernet Protocol (REP)



Redundant Star

Flex Links
EtherChannel



	Linear	Ring	Redundant Star
Cabling Requirements	●	●	●
Ease of Configuration	●	●	●
Implementation Costs	●	●	●
Bandwidth	●	●	●
Redundancy and Convergence	●	●	●
Disruption During Network Upgrade	●	●	●
Readiness for Network Convergence	●	●	●
Overall in Network TCO and Performance	Worst	OK	Best

Network Resiliency Protocols

Selection is Application Driven

Resiliency Protocol	Mixed Vendor	Ring	Redundant Star	Net Conv >250 ms	Net Conv 50-100 ms	Net Conv < 0~10 ms	Layer 3	Layer 2
STP (802.1D)	●	●	●					●
RSTP (802.1w)	●	●	●	●				●
MSTP (802.1s)	●	●	●	●				●
PVST+		●	●	●				●
REP		●			●			●
EtherChannel (LACP 802.3ad)	●		●		●			●
MRP (IEC 62439-2)*	●	●		●	●			●
Flex Links			●		●			
PRP/HSR (IEC 62439)*	●	●	●			●		●
DLR (IEC & ODVA)	●	●				●		●
StackWise		●	●	●			●	●
HSRP		●	●	●			●	
VRRP (IETF RFC 3768)	●	●	●	●			●	

Process and Information

Time Critical

Loss Critical

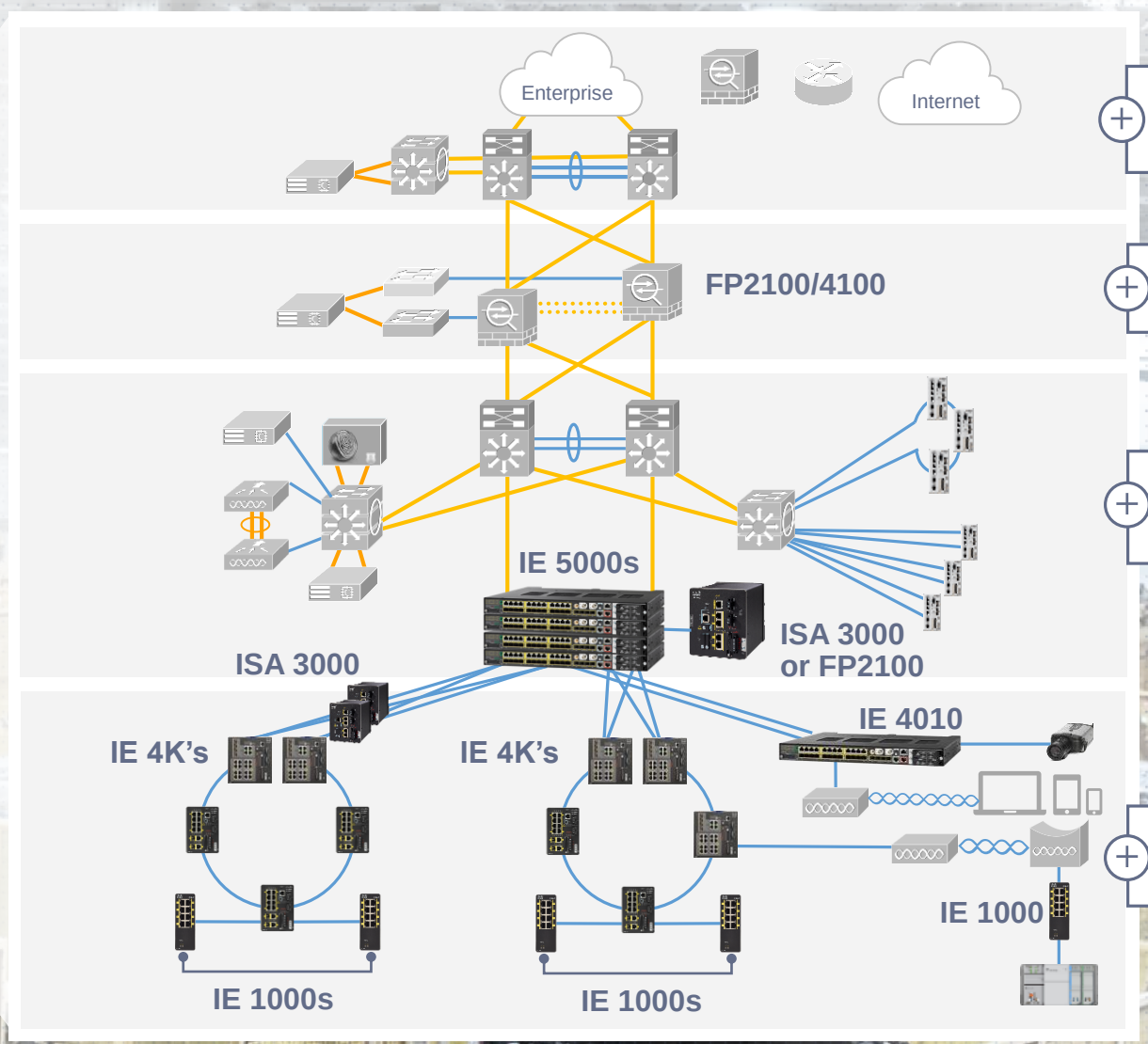
* Not part of CPwE

Security - an enabler of IoT and ISA 99

- Increased resiliency
- Integrated OT/IT security

- Industrial threat protection
- Simplified compliance

- Secure connectivity
- Unmanaged switch replacement



Enterprise Zone
Levels 4 and 5

Industrial DMZ

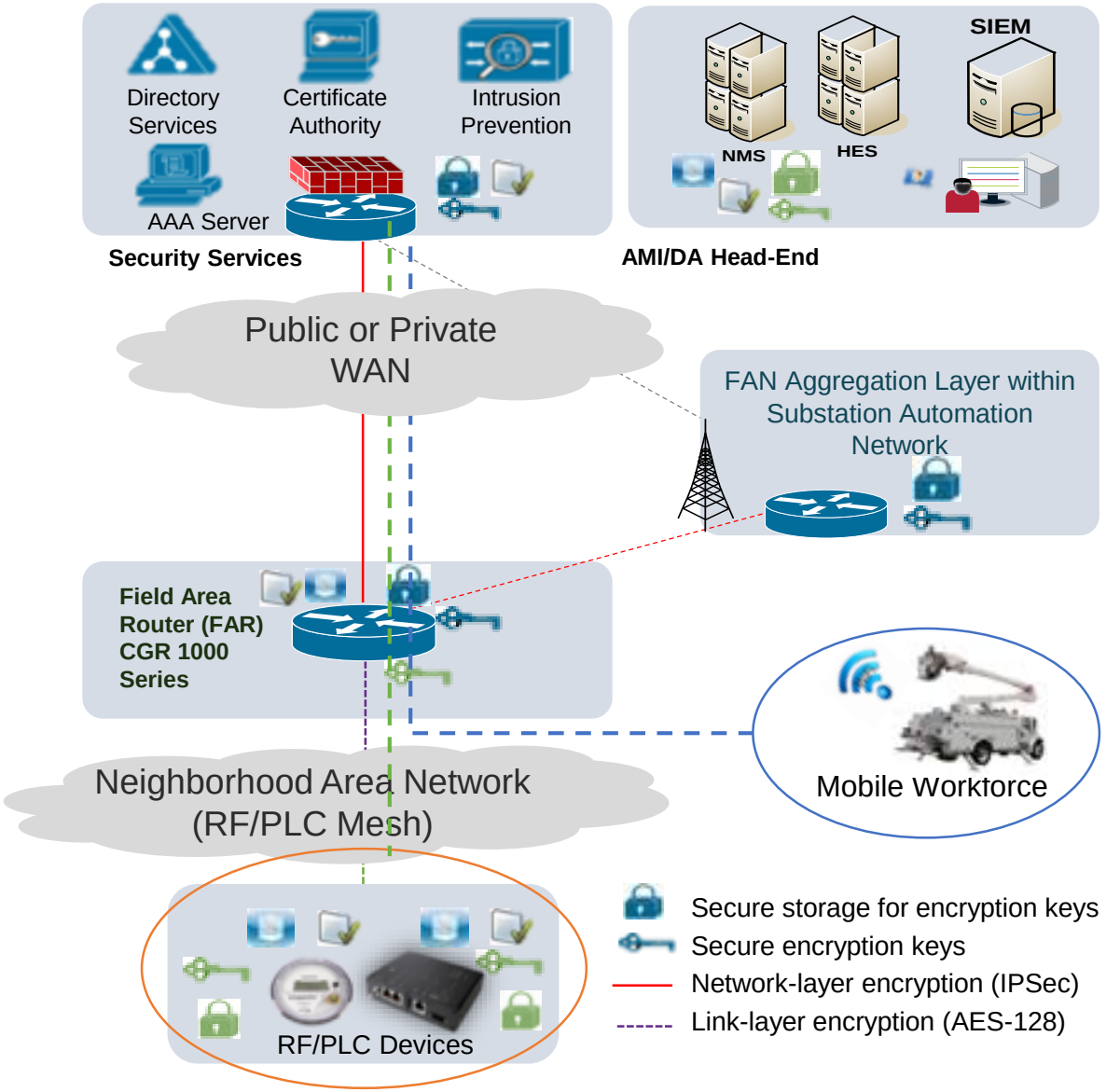
Industrial Zone
Level 3

Cell Area Zone
Levels 0–2

Securely Connect › › Increase Resilience › › Simplify Operations

Security Architecture for IoT

- Device hardening with 802.1AR and ACT2 security chip
- Network hardening tools
- Certificate-based identities, user names & passwords
- Role based Access Control
- 802.1x-based access control for meters, routers, grid devices
- Link-layer encryption in RF Mesh
- Group-based key generation and management (mesh)
- Network-layer encryption for WAN Backhaul (IPSec)



Secure Device Identity via Digital Certificates

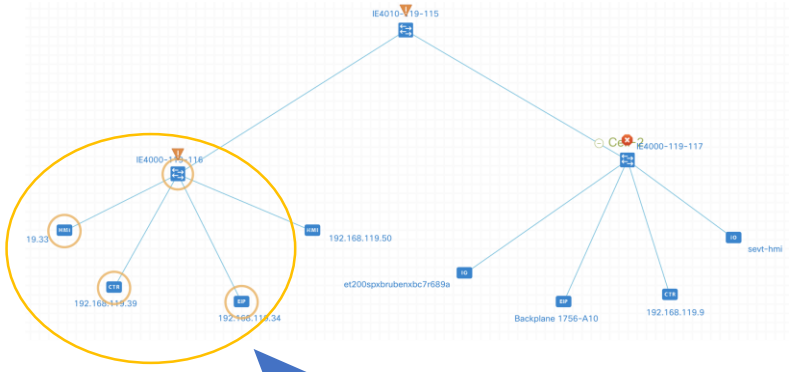
Strong user identities with Role-Based Access

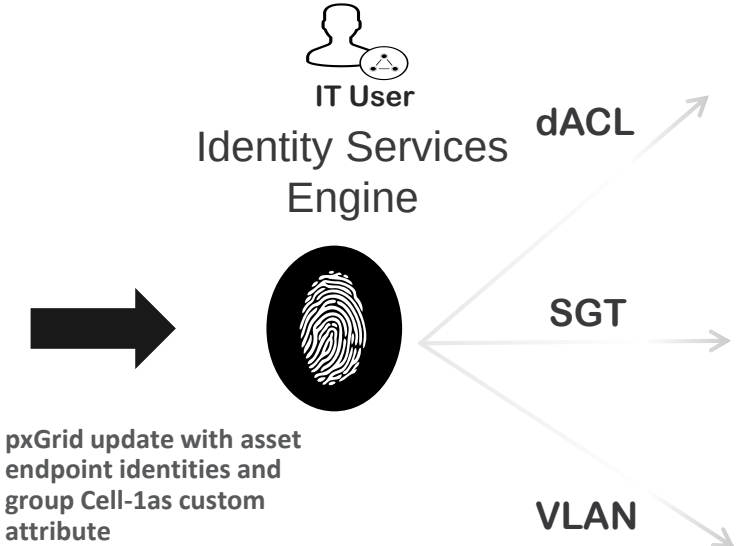
Time-stamped logs, correlation at SIEM

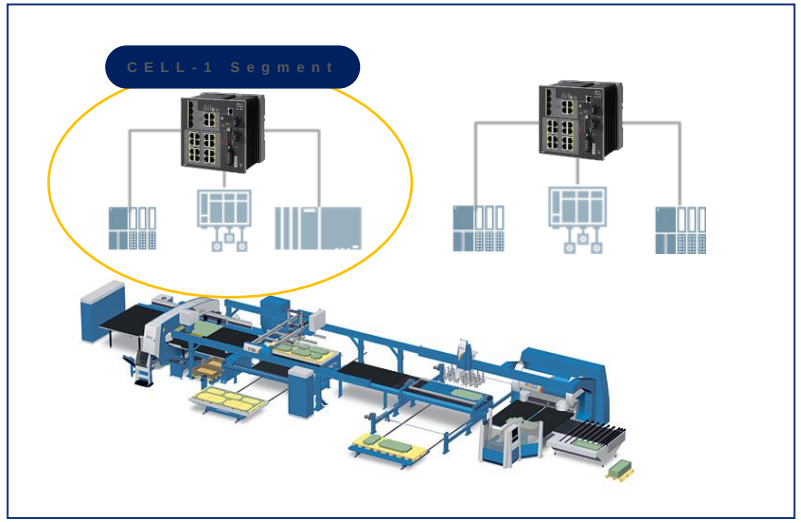
Separation of AMI vs. non-AMI traffic, segmentation

Network Segmentation

IND Topology Screen

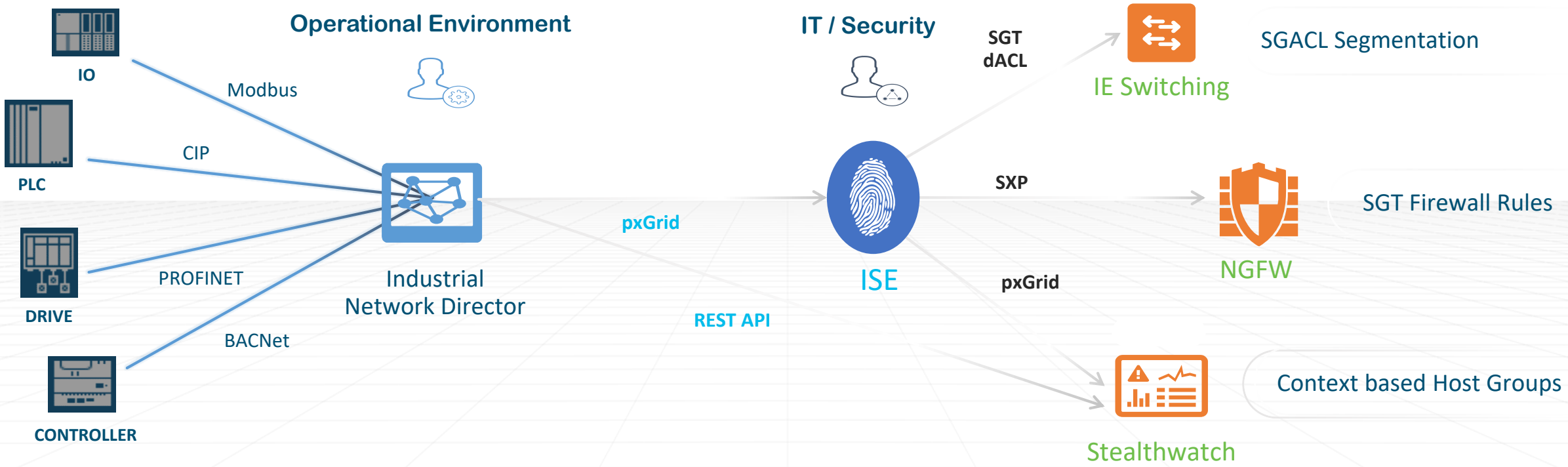






- Default Auth policy on ISE for switchport is configured as “open access” – i.e no NAC blocking
- PxGrid attribute “**Cell-1”** matches a Profiling policy on ISE and triggers corresponding Authorization policy
- ISE Authorization policy can be used to dynamically apply dACL, SGT or VLAN to switchports to segment the assets
- OT user and IT user are working with asset identities rather than IP addresses

Enabling IT-OT partnership to secure the OT network



How do we secure all this things?

Manufacturer **U**sage **D**escription

IoT Device Business Challenges

Device Visibility

Do you know devices well enough to differentiate service?

Intent-based Policy

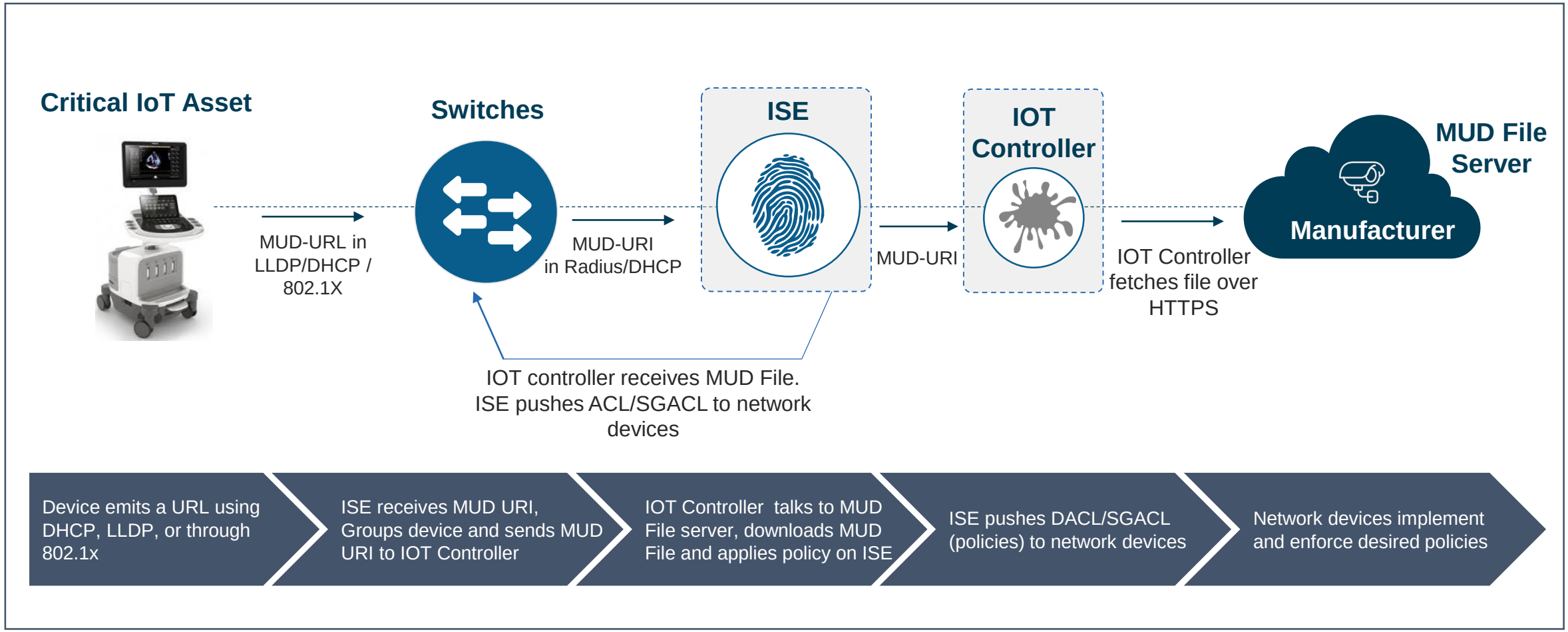
Does customer knows behavior of devices to build their policy?

Standard based

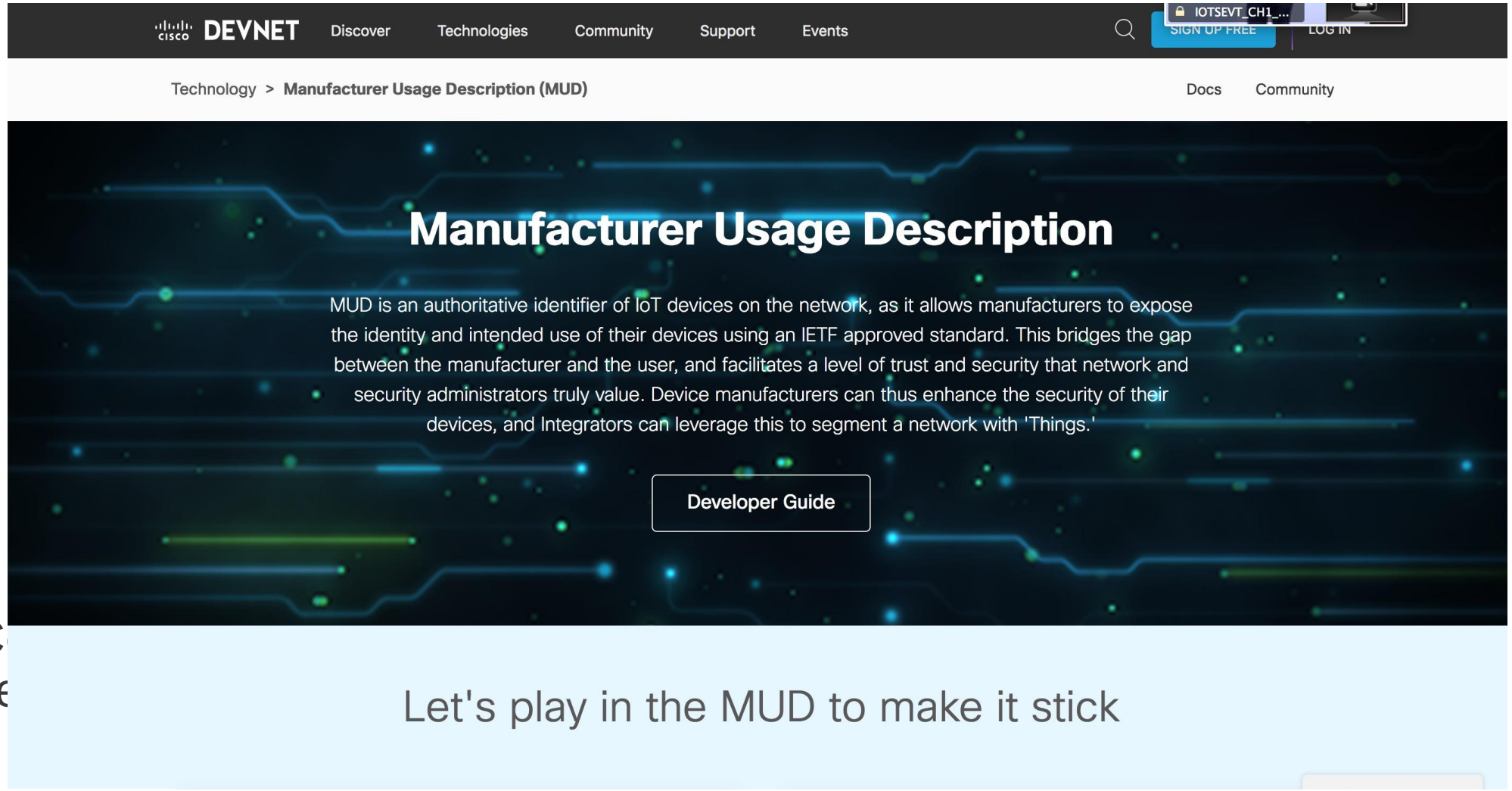
Is there any industry standard way of connecting IoT devices to enterprise network?

MUD Ecosystem Architecture

Phase 1: Visibility
Phase 2: Policy
Phase 3: Trusted Introduction



DevNet site commissioned to support developers



Benefits

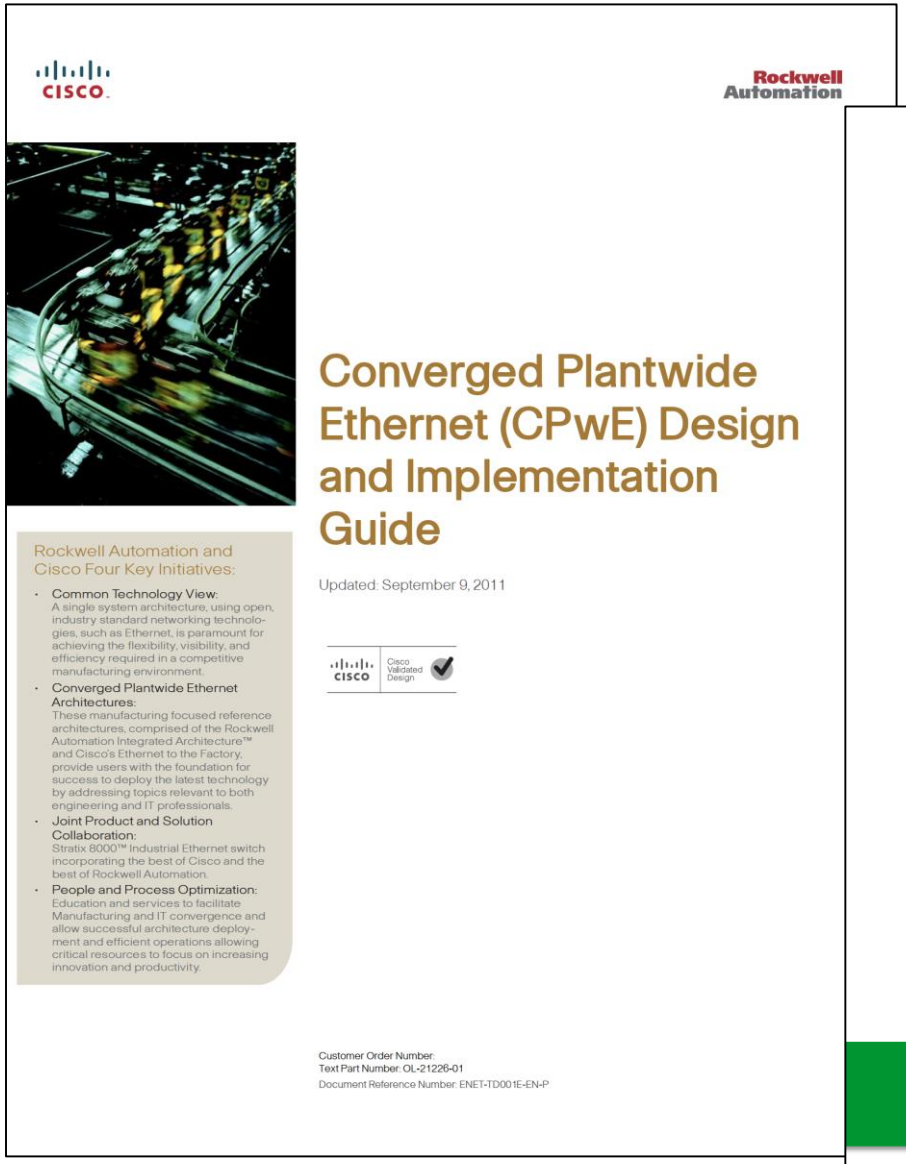
Customer

- **Reduces threat surface** of exploding number of devices
- Almost no additional CAPEX
- Standard approach to determining manufacturer intent
- Eases and scales access management decisions

Manufacturer

- Reduces manufacturer product risk at almost no cost
- Will increase customer satisfaction and reduce support costs
- **Avoids the front page**
- **Standards-based approach**

Cisco Validated Design (CVD)



Rockwell Automation

Converged Plantwide Ethernet (CPwE) Design and Implementation Guide

Updated: September 9, 2011

Rockwell Automation and Cisco Four Key Initiatives:

- Common Technology View: A single system architecture, using open, industry standard networking technologies, such as Ethernet, is paramount for achieving the flexibility, visibility, and efficiency required in a competitive manufacturing environment.
- Converged Plantwide Ethernet Architectures: These manufacturing focused reference architectures, comprised of the Rockwell Automation Integrated Architecture™ and Cisco's Ethernet to the Factory, provide users with the foundation for success to deploy the latest technology by addressing topics relevant to both engineering and IT professionals.
- Joint Product and Solution Collaboration: Stratix 8000™ Industrial Ethernet switch incorporating the best of Cisco and the best of Rockwell Automation.
- People and Process Optimization: Education and services to facilitate Manufacturing and IT convergence and allow successful architecture deployment and efficient operations allowing critical resources to focus on increasing innovation and productivity.

Customer Order Number:
Text Part Number: OL-21226-01
Document Reference Number: ENET-TD001E-EN-P

EcoStruxure Building Ethernet Network Design for MP Series Controllers

How to combine Cisco Industrial Ethernet Switches with the EcoStruxure Building system to create a secure and resilient BMS architecture

Network Solution Guide

Document Version 1.2.1 September 22, 2018

Life Is On Schneider Electric

Cisco Connected Factory—PROFINET Wireless Design and Implementation Guide

First Published: October 2017

Cisco Systems, Inc. www.cisco.com