ODVA 2017
Industry Conference
and 18th Annual Meeting

IT and OT Convergence - Recommendations for Building an Industrial IoT-Ready Manufacturing Network

Arun Siddeswaran, Cisco Systems, Inc.

Gregory Wilcox, Rockwell Automation, Inc.

February 22, 2017

Agenda

- Secure Connectivity between Manufacturing and Business Systems
  - Business Outcomes
  - Bridging OT-IT
  - Key Requirements / Key Tenets
- Key Takeaways
- Recommended Resources

ODVA 2017
Industry Conference
and 18th Annual Meeting

Industrial IoT - Business Outcomes

Industrial IoT - Business Outcomes

Reduced Downtime

48%

Unplanned downtime down from 11% to 5.8%

Reduction in Defects

49%

Defect rate down from 4.9% to 2.5%

New Product Introduction

23%

New product introduction cycle time reduced from 15 to 11 months

OEE Improvement

16%

Average OEE improved from 74% to 86%

Improved Inventory

35%

Inventory turns increased from 14 to 19

Reduction in Energy Use

18%

Annual energy cost down from $8.4M to $6.9M

SCM World

Source: SCM World/Cisco “Smart Manufacturing and the Internet of Things 2015” survey of 418 Manufacturing Business Line Executives and Plant Managers across 17 vertical industries.

Industrial IoT - Business Outcomes

- Smart Devices, Smart Machines, Smart Manufacturing
- Customer choice of best-in-class products through Industrial IoT device coexistence and interoperability
- Standard Network Services; Standard Network Tools
- Pervasive Asset Optimization and Utilization
  - Common infrastructure devices and tools
  - Human assets: knowledge, experience, training
- Better Analytics
  - Device/Machine, System/Plant, Enterprise
- Enables Innovative Technologies
  - Mobility – Personnel and Equipment
  - Cloud –On Premise and Off Premise

ODVA 2017
Industry Conference
and 18th Annual Meeting

Industrial OT vs Enterprise IT Networks

Industrial OT vs. Enterprise IT Networks

Criteria	Industrial OT Network	Enterprise IT Network
Network Technology	Standard IEEE 802.3 Ethernet and proprietary (non-standard) versions Standard IETF Internet Protocol (IPv4) and proprietary (non-standard) alternatives	Standard IEEE 802.3 Ethernet Standard IETF Internet Protocol (IPv4 and IPv6)
Network Availability	Switch-Level and Device-Level Topologies Ring Topology is predominant for both, Redundant Star for switch topologies is emerging Standard IEEE, IEC and vendor specific Layer 2 resiliency protocols	Switch-Level topologies Redundant Star Topology is predominant Standard IEEE, IETF, and vendor specific Layer 2 and Layer 3 resiliency protocols
Service Level Agreement (SLA)	Mean time to recovery (MTTR) - Minutes, Hours	Mean time to recovery (MTTR) - Hours, Days
IP Addressing	Mostly Static	Mostly Dynamic

Industrial OT vs. Enterprise IT Networks

Criteria	Industrial OT Network	Enterprise IT Network
Traffic Type	Primarily local – traffic between local assets Information, control, safety, motion, time synchronization, energy management Smaller frames for control traffic Industrial application layer protocols: CIP, PROFINET, IEC 61850, Modbus TCP, etc.	Primarily non-local – traffic to remote assets Voice, Video, Data Larger packets and frames Standard application layer protocols: HTTP, SNMP, DNS, RTP, SSH, etc.
Performance	Low Latency, Low Jitter Data Prioritization – QoS – Layer 2 & 3	Low Latency, Low Jitter Data Prioritization – QoS – Layer 3
Security	Open by default, must close by configuration and architecture Industrial security standards – e.g. IEC, NIST Inconsistent deployment of security policies No line-of-sight to the Enterprise or to the Internet	Pervasive Enterprise security standards Strong security policies Line-of-sight across the Enterprise and to the Internet

ODVA
2017
Industry Conference
and 18th Annual Meeting

What are best practices

Structured and Hardened Architectures

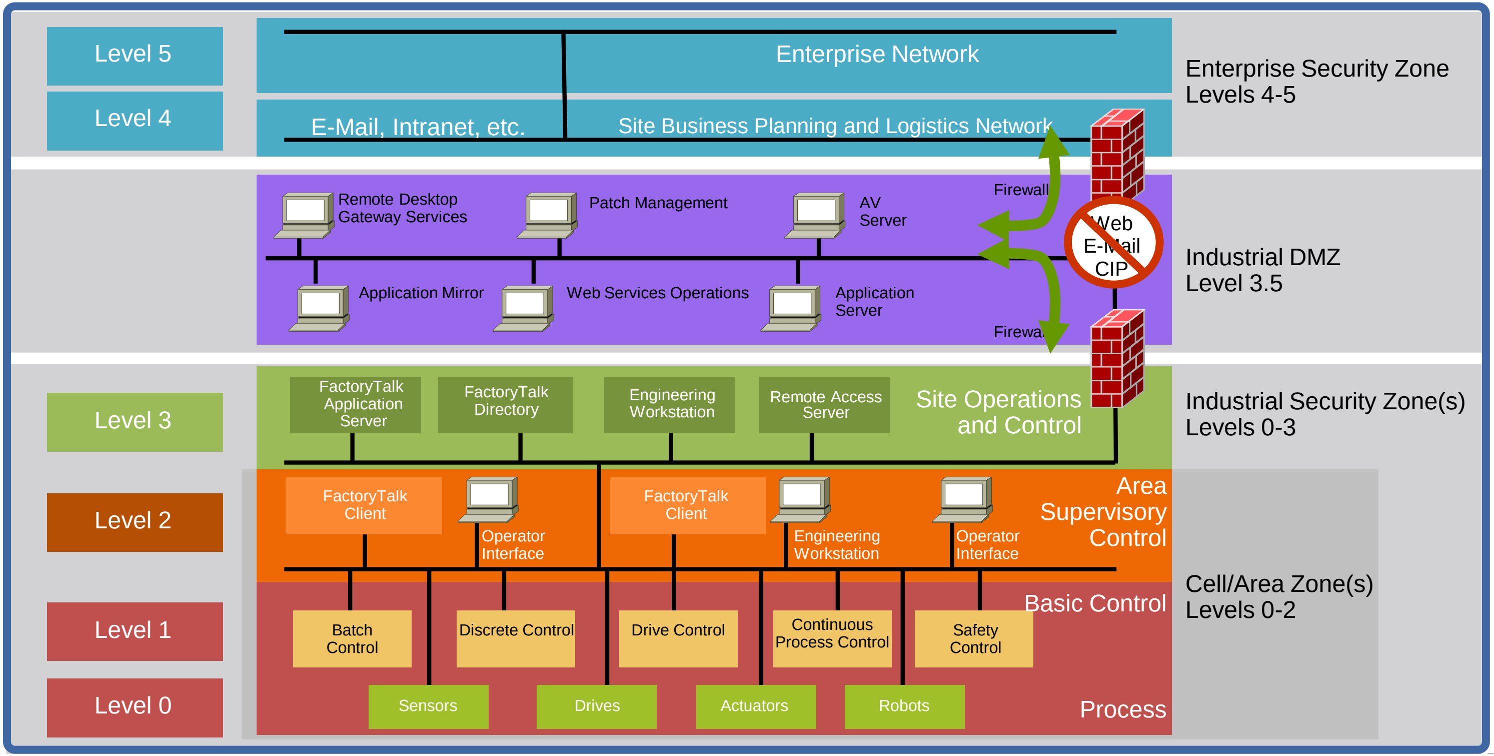
Key Requirements

- Scalable
- Reliable
- Safe
- Secure
- Future-ready

Key Tenets

- Smart Endpoints
- Segmentation (Zoning)
- Managed Infrastructure
- Resiliency
- Time-critical Data
- Wireless - Mobility
- Holistic Defense-in-Depth Security
- Convergence-ready

Zoning Through Segmentation



Level 5

Level 4

Enterprise Network

E-Mail, Intranet, etc.

Site Business Planning and Logistics Network

Enterprise Security Zone
Levels 4-5

Remote Desktop Gateway Services

Patch Management

AV Server

Firewall

Web
E-Mail
CIP

Application Mirror

Web Services Operations

Application Server

Firewall

Industrial DMZ
Level 3.5

Level 3

FactoryTalk Application Server

FactoryTalk Directory

Engineering Workstation

Remote Access Server

Site Operations and Control

Industrial Security Zone(s)
Levels 0-3

Level 2

FactoryTalk Client

Operator Interface

FactoryTalk Client

Engineering Workstation

Operator Interface

Area Supervisory Control

Level 1

Batch Control

Discrete Control

Drive Control

Continuous Process Control

Safety Control

Basic Control

Cell/Area Zone(s)
Levels 0-2

Level 0

Sensors

Drives

Actuators

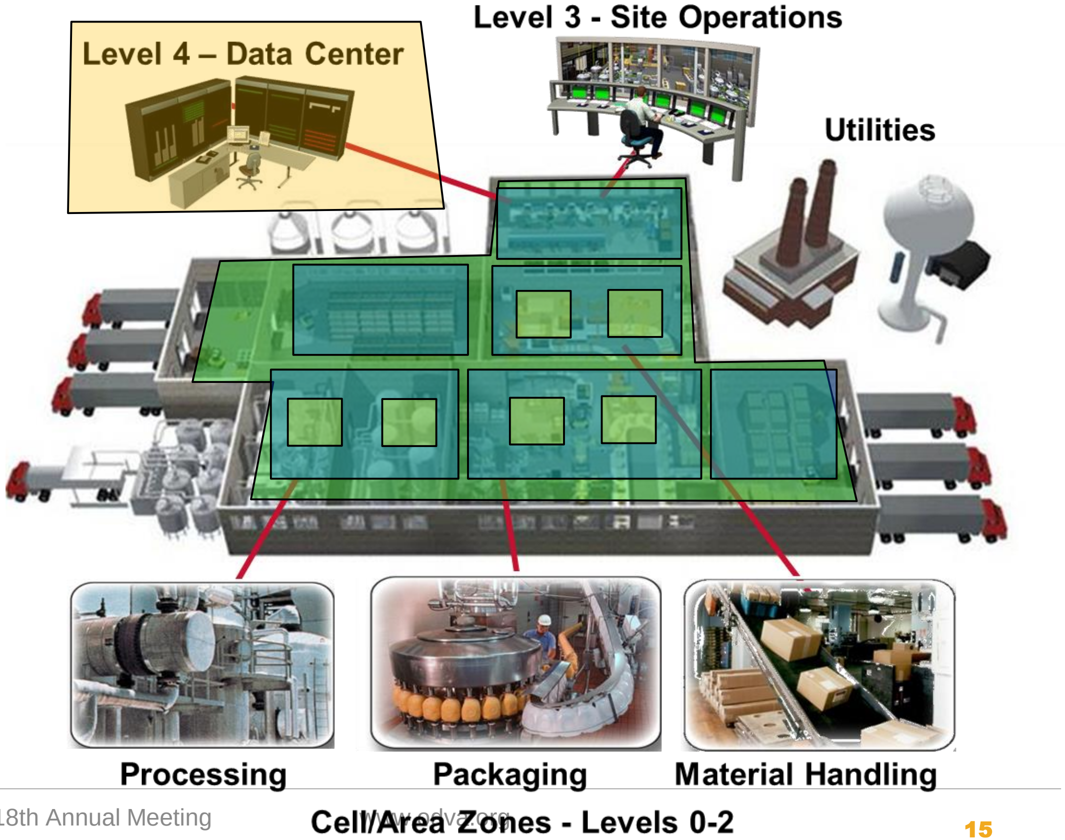
Robots

Process

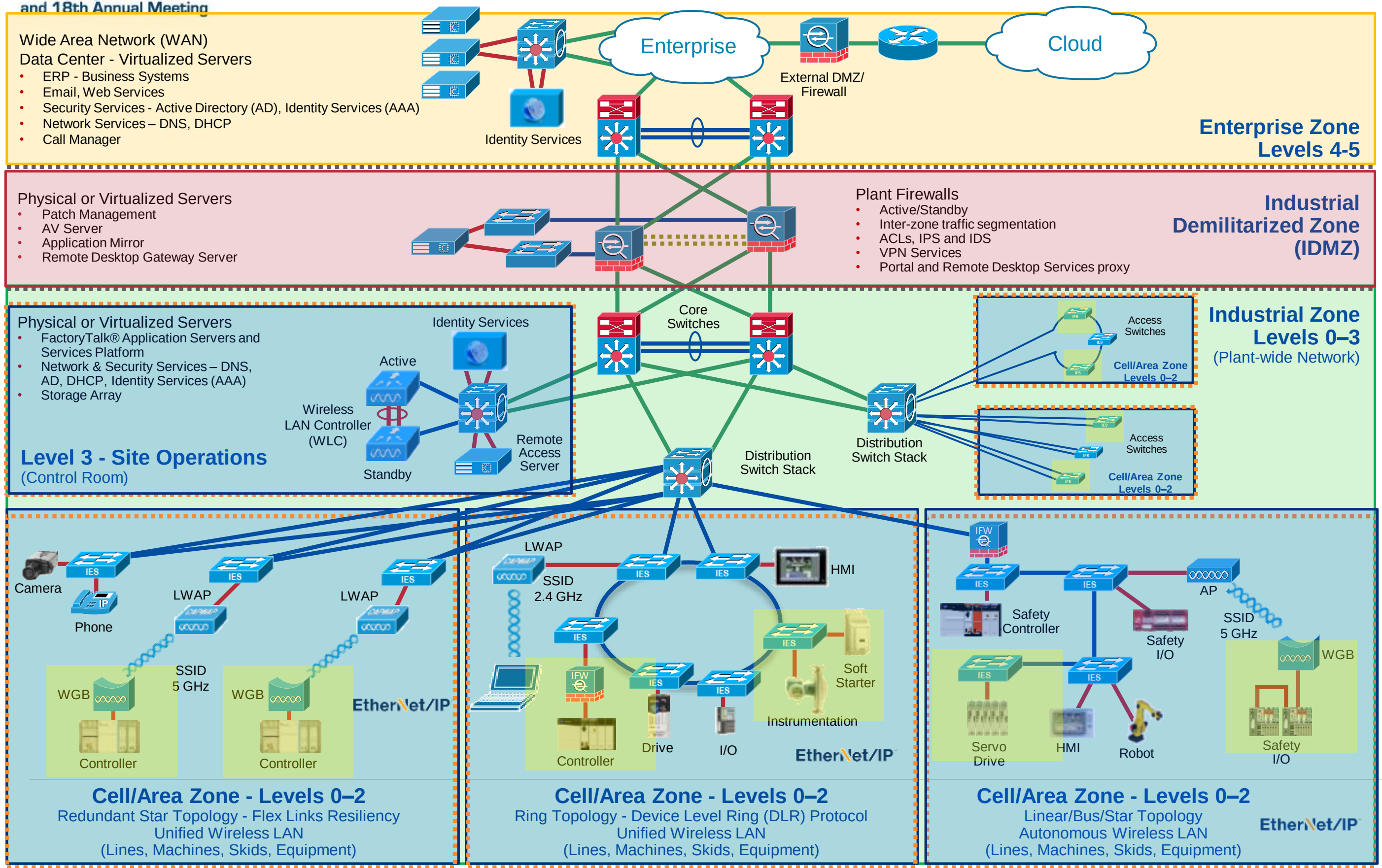
Zoning Through Segmentation

Plant-wide Zoning

- Functional / Security Areas
- Smaller Connected LANs
  - Smaller Broadcast Domains
  - Smaller Fault Domains
  - Smaller Domains of Trust
- Industrial IoT Technology
- Building Block Approach for Scalability



Zoning Through Segmentation



Wide Area Network (WAN)
Data Center - Virtualized Servers
- ERP - Business Systems
- Email, Web Services
- Security Services - Active Directory (AD), Identity Services (AAA)
- Network Services – DNS, DHCP
- Call Manager

Enterprise Zone
Levels 4-5

Physical or Virtualized Servers
- Patch Management
- AV Server
- Application Mirror
- 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)

Physical or Virtualized Servers
- FactoryTalk® Application Servers and Services Platform
- Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
- Storage Array

Level 3 - Site Operations
(Control Room)

Industrial Zone
Levels 0–3
(Plant-wide Network)

Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)

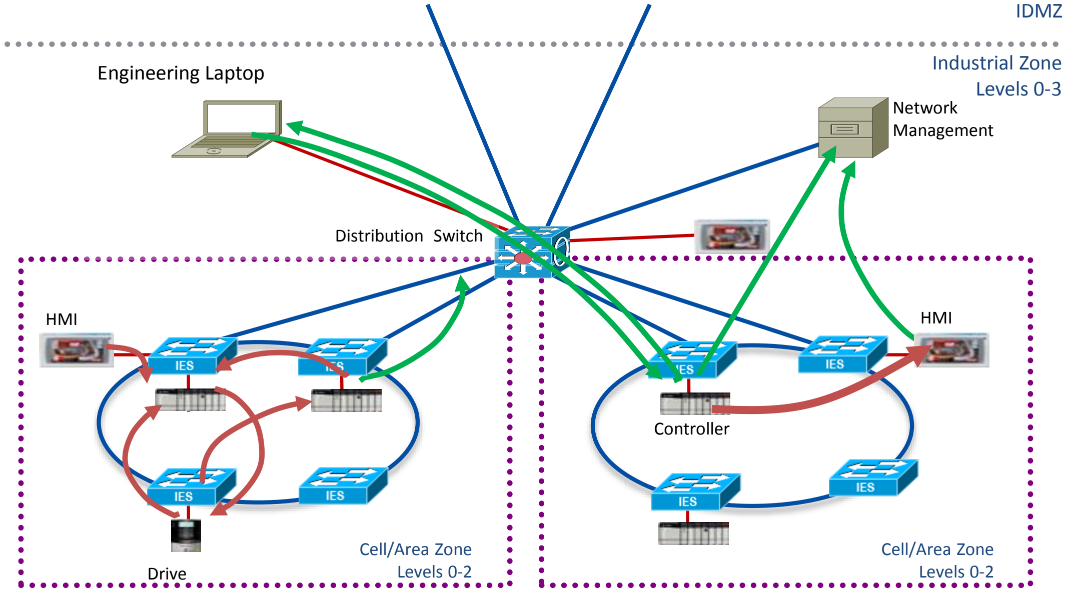
Key Tenets

- Smart Endpoints
- Segmentation (Zoning)
- Managed Infrastructure
- Resiliency
- Time-critical Data
- Wireless - Mobility
- Holistic Defense-in-Depth Security
- Convergence-ready

ODVA 2017
Industry Conference
and 18th Annual Meeting

Wired Access Overview

Typical Zone Traffic Flows



CIP Implicit Traffic- 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 Traffic - Informational control and administration

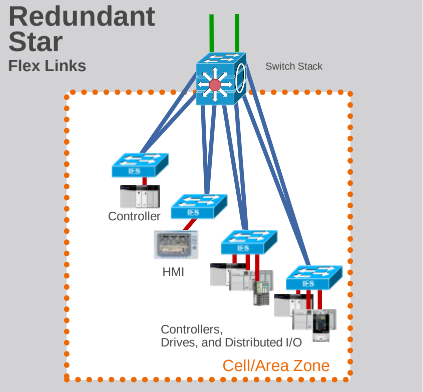
Intra- and inter-cell/area zone traffic flow

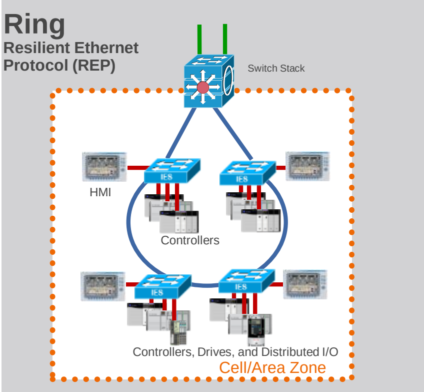
Non-critical administrative or data traffic using **TCP**

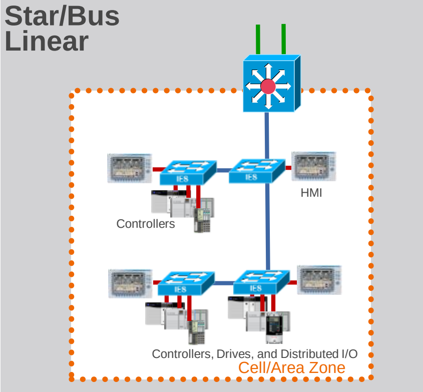
~1500 Bytes, **infrequent**

Industrial Network Topologies

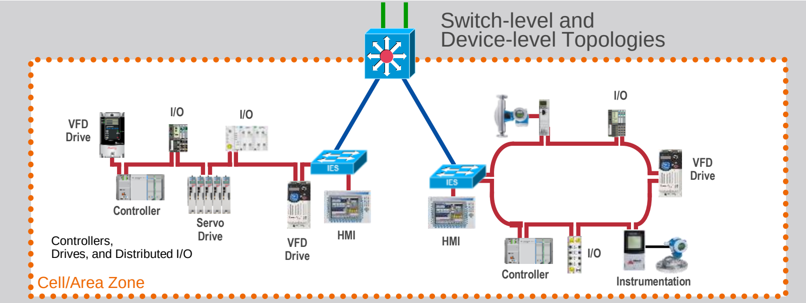
Switch-level Topologies







Device-level Topologies



Performance Requirements

	Process Automation	Discrete Automation	Loss Critical
Function	Information Integration, Slower Process Automation	Time-critical Discrete Automation	Multi-axis Motion Control
Comm. Technology	.Net, DCOM, TCP/IP	Industrial Protocols, CIP, Profinet	Hardware and Software solutions, e.g. CIP Motion, PTP
Period	1 second or longer	1 ms to 100 ms	100 µs to 10 ms
Industries	Oil & Gas, chemicals, energy, water	Auto, food and beverage, electrical assembly, semiconductor, metals, pharmaceutical	Utilities Subset of Discrete automation
Applications	Pumps, compressors, mixers; monitoring of temperature, pressure, flow	Material handling, filling, labeling, palletizing, packaging; welding, stamping, cutting, metal forming, soldering, sorting	Life/equipment safety, Synchronization o multiple axes: printing presses, wire drawing, web making, picking and placing

Source: ARC Advisory Group

Network Resiliency Protocols

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

ODVA 2017
Industry Conference
and 18th Annual Meeting

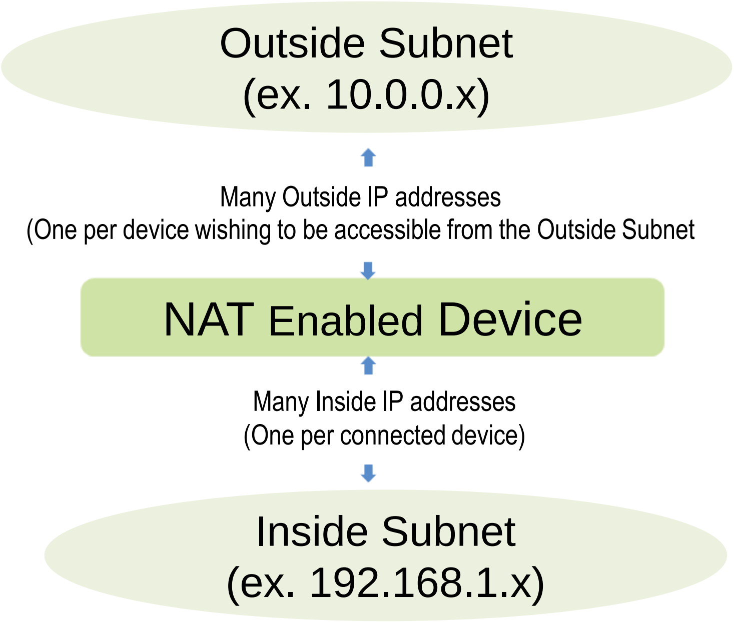
Convergence-Ready

Challenge - Ethernet Growing Pains

- Ethernet networks continue to grow:
  - Each skid/machine adds another 5 - 50 EtherNet/IP enabled devices
  - Every line adds another 250 - 1,000 EtherNet/IP enabled devices

How do I connect all these skids/machines into a plant network to gain the advantages?

Layer 2 Network Address Translation (NAT)



Outside Subnet
(ex. 10.0.0.x)

Many Outside IP addresses
(One per device wishing to be accessible from the Outside Subnet

NAT Enabled Device

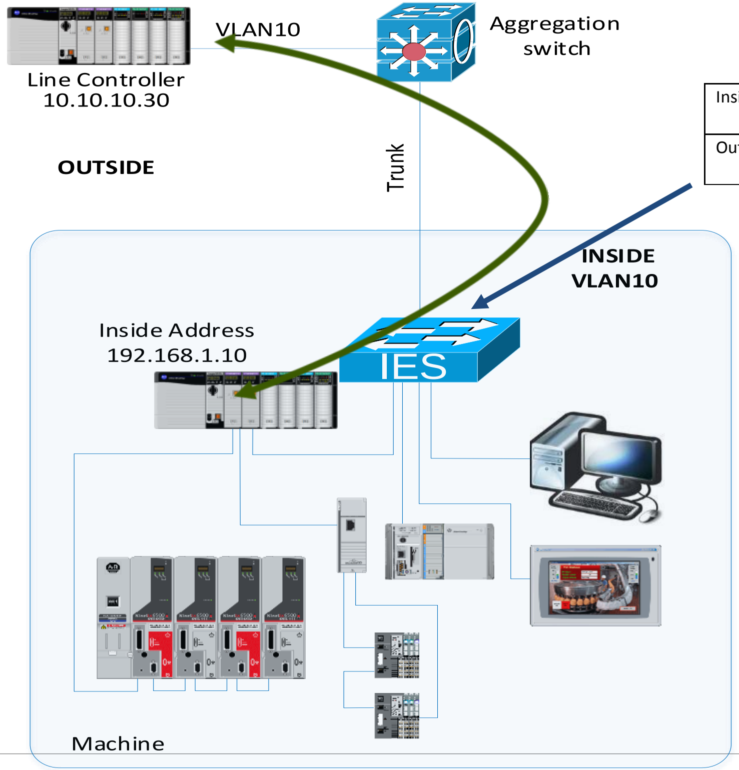
Many Inside IP addresses
(One per connected device)

Inside Subnet
(ex. 192.168.1.x)

One to One (1:1) NAT

Layer 2 NAT Design Scenario #1

Single-Cell, Single VLAN per Switch



Inside to Outside NAT Table	Inside	Outside
	192.168.1.10	10.10.10.10
Outside to inside NAT Table	Outside	Inside
	10.10.10.30	192.168.1.30

ODVA 2017
Industry Conference
and 18th Annual Meeting

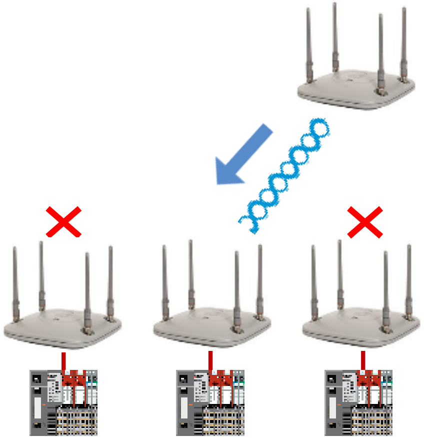
Wireless Access Overview

Wireless Technology Overview - Benefits of Industrial WLAN

- Lower installation and operational costs
  - Cabling and hardware reduction
  - Minimizing cable failures
- Connection to hard-to-reach and restricted areas
- Equipment mobility
  - New and more efficient applications
- Workforce mobility
  - Higher productivity and less downtime
  - Operators, engineering and maintenance, Industrial IT
- Asset Tracking
  - Track assets of people to optimize cost and for safety

Challenges of wireless communication

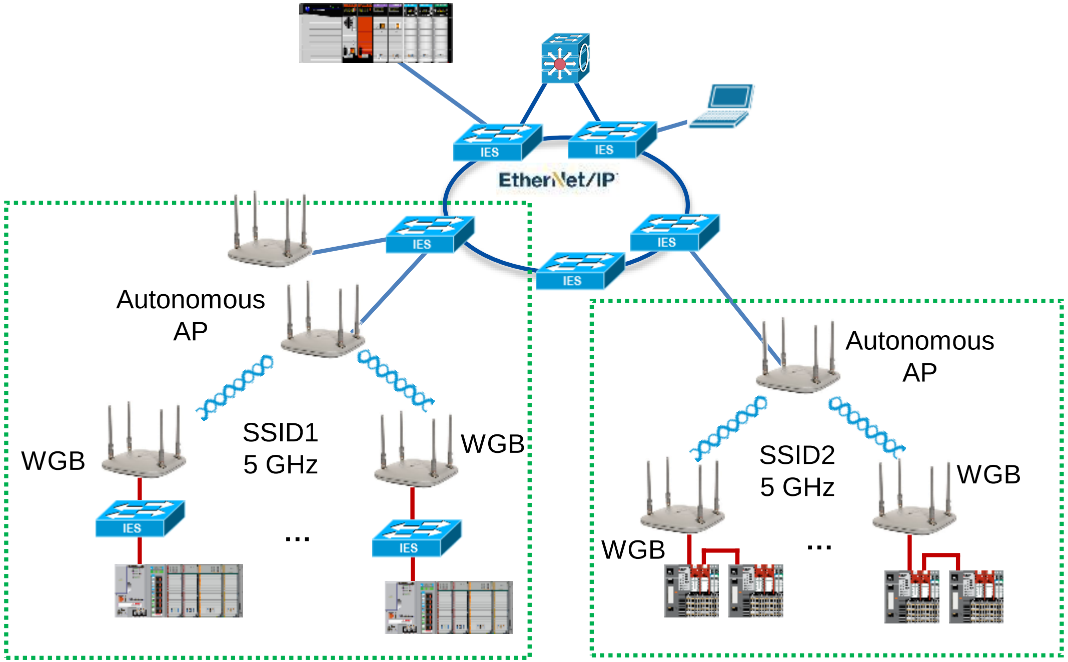
- **Half-duplex shared medium**:
  - Only one radio can transmit on a particular wireless channel
  - A radio cannot transmit and receive at the same time on the same channel
- Higher latency, jitter and packet loss compared to wired Ethernet
  - Media contention, collisions and interference
  - Can be minimized but not eliminated
- Signal quality may change over time



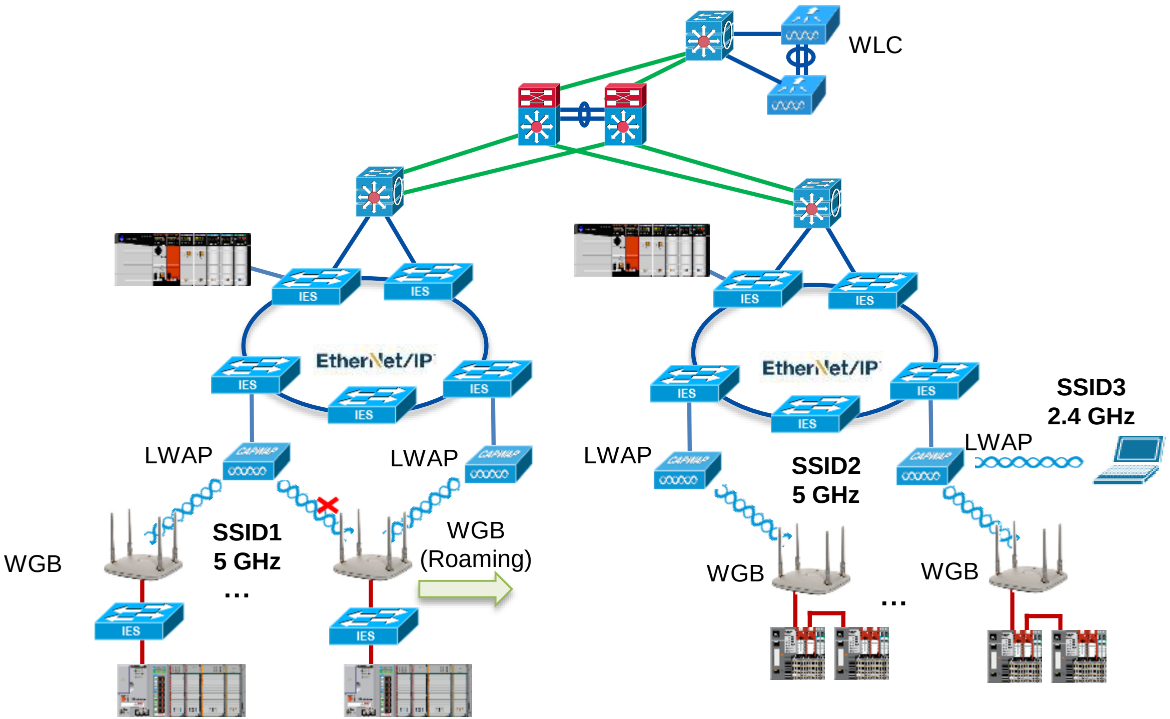
Wireless advantages > challenges when

- ***WLAN is designed and maintained properly***
- ***Used for appropriate applications***

Autonomous WLAN Architecture



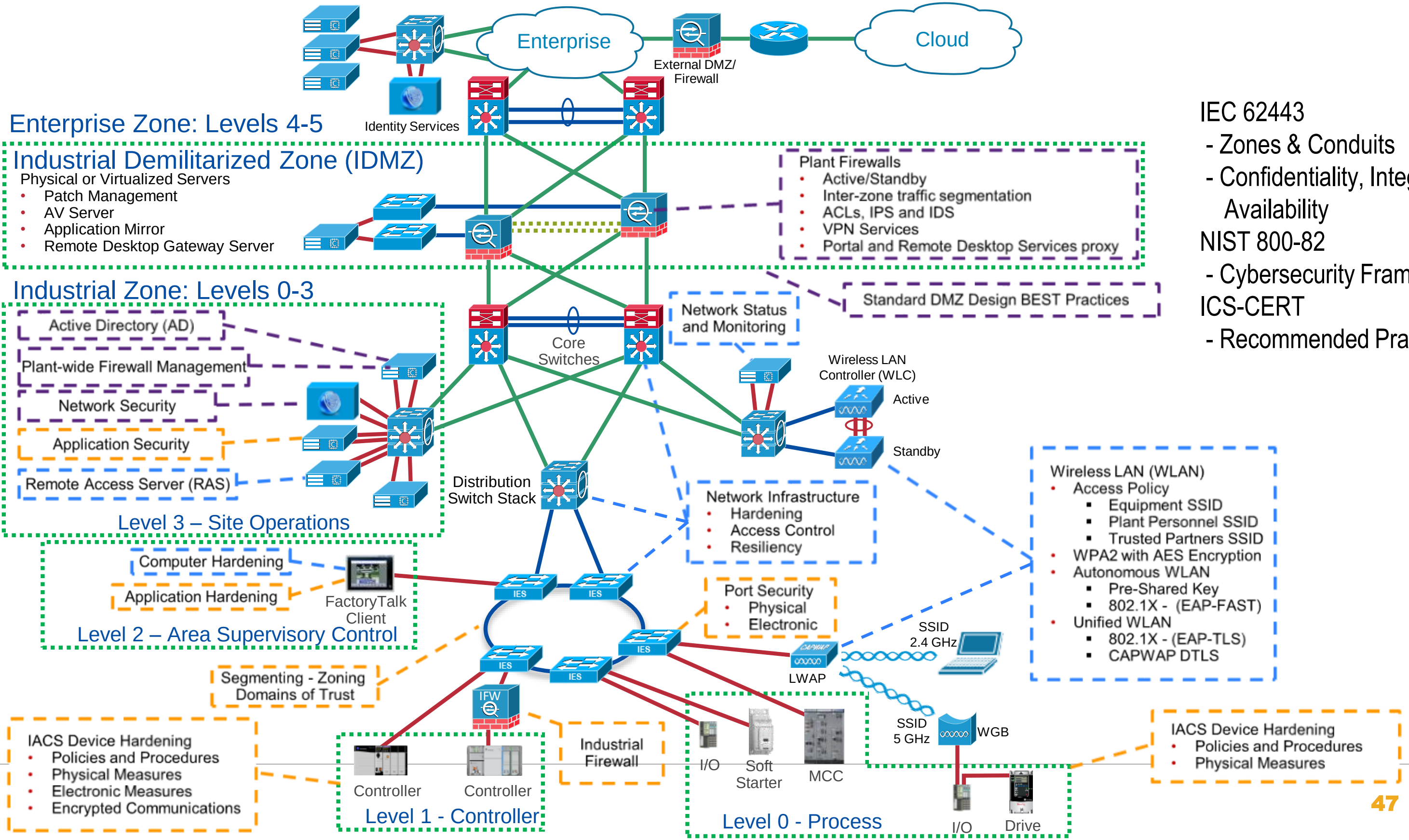
Unified WLAN Architecture



ODVA 2017
Industry Conference
and 18th Annual Meeting

Holistic Defense-in-Depth Security

Industrial Network Security Framework



Enterprise Zone: Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Physical or Virtualized Servers

- Patch Management
- AV Server
- Application Mirror
- 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)

Plant-wide Firewall Management

Network Security

Application Security

Remote Access Server (RAS)

Level 3 – Site Operations

Network Status and Monitoring

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

Level 2 – Area Supervisory Control

Port Security

- Physical
- Electronic

Segmenting - Zoning
Domains of Trust

IACS Device Hardening

- Policies and Procedures
- Physical Measures
- Electronic Measures
- Encrypted Communications

Industrial
Firewall

Level 1 - Controller

Level 0 - Process

IACS Device Hardening

- Policies and Procedures
- Physical Measures

Control System Engineers (OT)

Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)

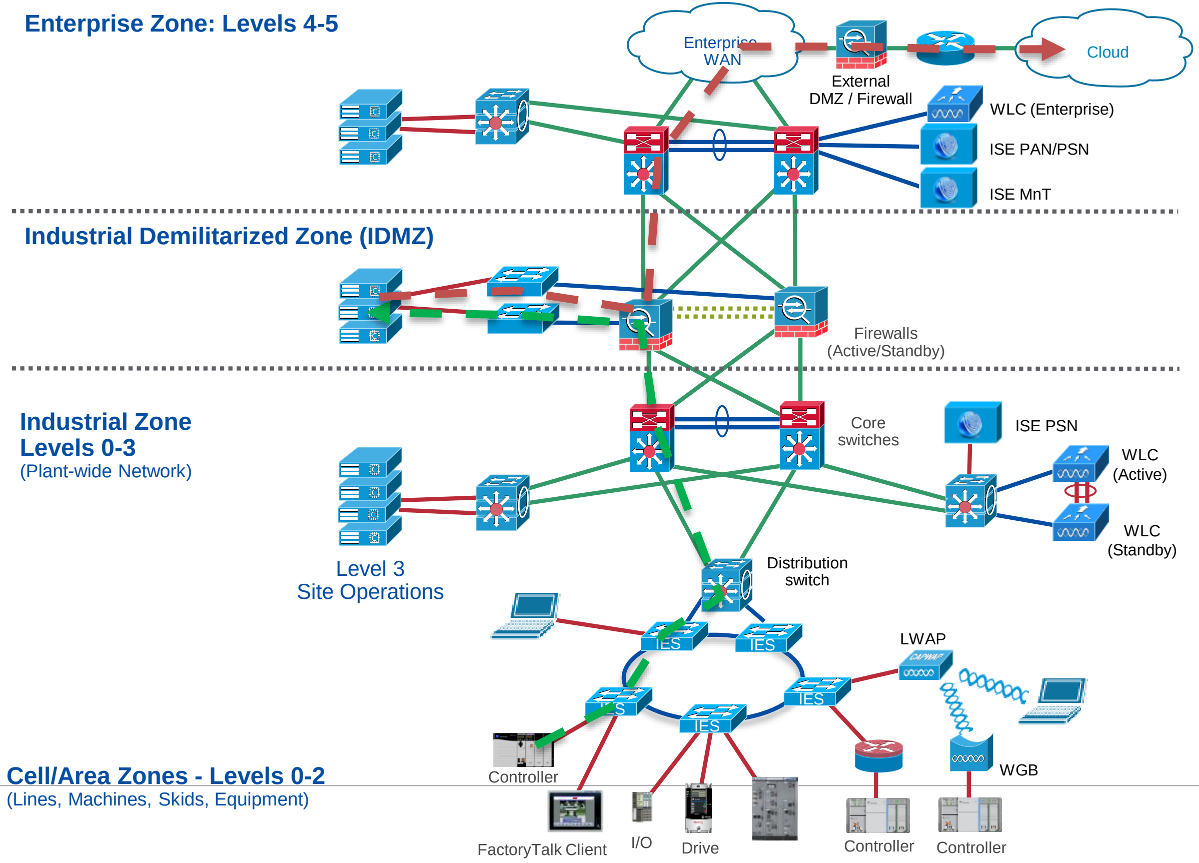
IT Security Architects in Collaboration with Control Systems Engineers

IEC 62443
- Zones & Conduits
- Confidentiality, Integrity, Availability

NIST 800-82
- Cybersecurity Framework

ICS-CERT
- Recommended Practices

Secure Remote Connectivity



Enterprise Zone: Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Industrial Zone Levels 0-3

(Plant-wide Network)

Cell/Area Zones - Levels 0-2

(Lines, Machines, Skids, Equipment)

Key Takeaways

- Plant-wide reference architectures - Simplified design, quicker deployment, reduced risk in deploying new technology
- Wired access topology and protocols based on plant layout, convergence and application requirements
- Layer 2 NAT helps end users to easily integrate skids/machines into their larger plant network without extensive coordination with OEMs
- Wireless access offers multiple advantages, enables secure personnel access, equipment to equipment communication and asset tracking
- Defense-in-depth security offers multiple layers of threat detection and prevention

Recommended Resources

- ODVA
  - The Common Industrial Protocol (CIP) and the Family of CIP Networks
  - Network Infrastructure for EtherNet/IP: Introduction and Considerations
  - Media Planning and Installation Manual
  - Guidelines for Using Device Level Ring (DLR) with EtherNet/IP
  - Securing EtherNet/IP Networks

- Converged Plantwide Ethernet (CPwE) Architectures
  - Cisco
  - Rockwell Automation
- Education / Awareness
  - Industrial IP Advantage (IIPA) eLearning industrial–ip.org
- Training / Certification
  - Industrial Networking Specialist
    - IMINS Training, 200-401 Exam
  - CCNA Industrial
    - IMINS2 Training, 200-601 Exam

ODVA
2017
Industry Conference
and 18th Annual Meeting

Thank You