Rockwell Automation

Innovation & Technology Forum

T53 - Design Considerations for Reliable EtherNet/IP Networking

Petr **DRAHOTA**
Commercial Engineer Power & Componets

Agenda

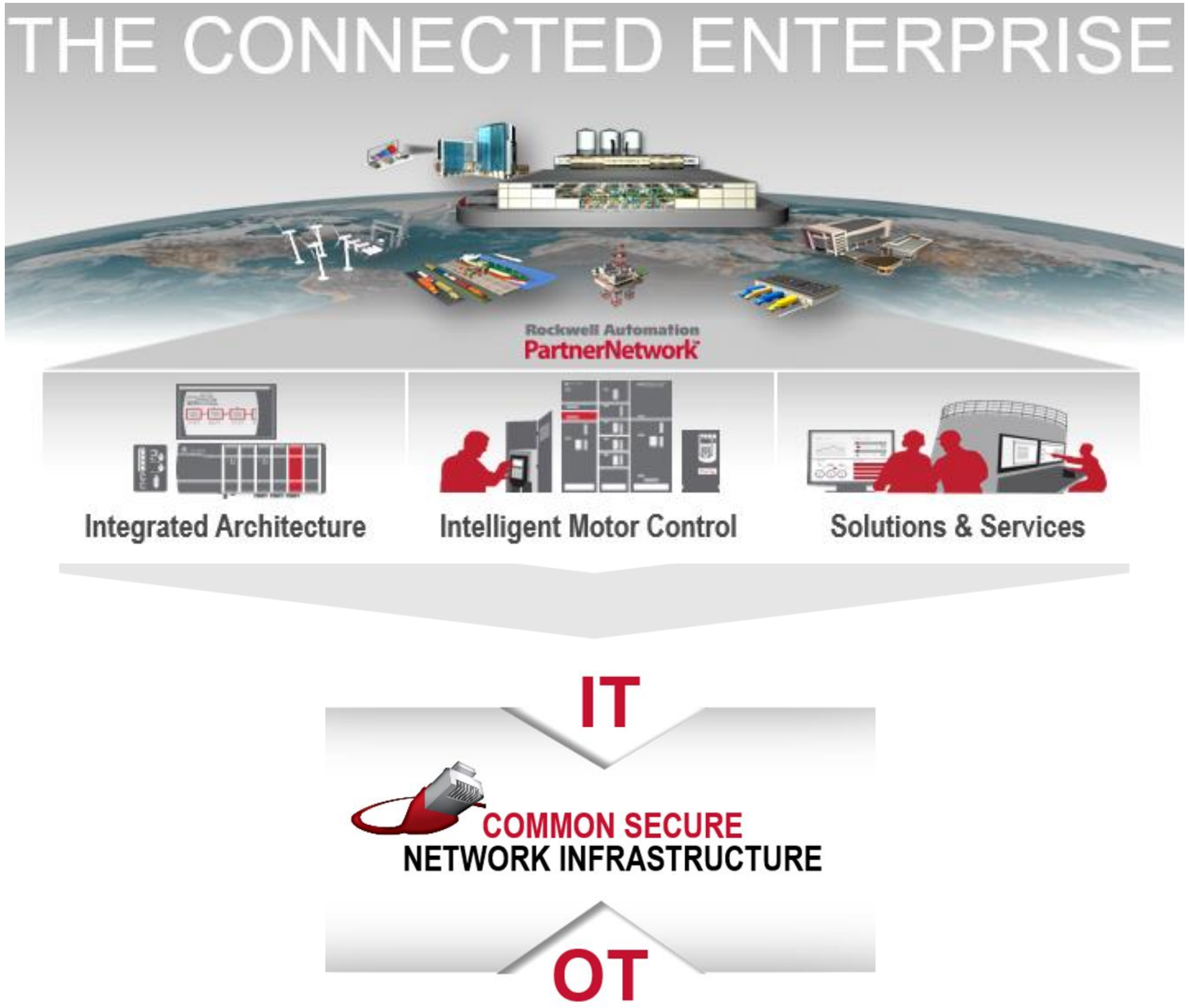
- Challenges Associated with Technology Convergence
- Industrial Network Design Methodology
- Key Requirements, Key Tenets
  - Smart Endpoints, Zoning (Segmentation)
  - Managed Infrastructure, Resiliency, Time-critical Data
- Additional Material

Challenges Associated with Technology Convergence


The Connected Enterprise
Optimized fo
Connected Architectures
Enterprise Zone Levels 4-5
Industrial Demilitarized Zone (IDMZ)
Industrial Zone Levels 0–3
Level 3 - Site Operations
Cell/Area Zone - Levels 0–2
Industrial Standards
ISA
IEEE
ODVA
TIA
Rockwell Automation
PartnerNetwork™
SIMPLIFY · COLLABORATE · INNOVATE
ENTERPRISE
Strategic Alliance Partners
SALES AND SOLUTIONS
Distributors • System Integrators • OEMs
PRODUCTS AND TECHNOLOGIES
Encompass™ Referenced Products • Licensed Developers
rity Threats
Threat Actors
Malware DDoS
Spyware
Phishing
Ransomware
Internal
Hackers
Hacktivist
State
Criminal
Rockwell Automation
COMMON SECURE NETWORK INFRASTRUCTURE
OT
PANDUIT
Endress+Hauser
Supply Chain
Distribution Center
Rockwell Automation

Challenges Associated with Technology Convergence

Scalable, Reliable, Safe and Secure Architectures for The Connected Enterprise



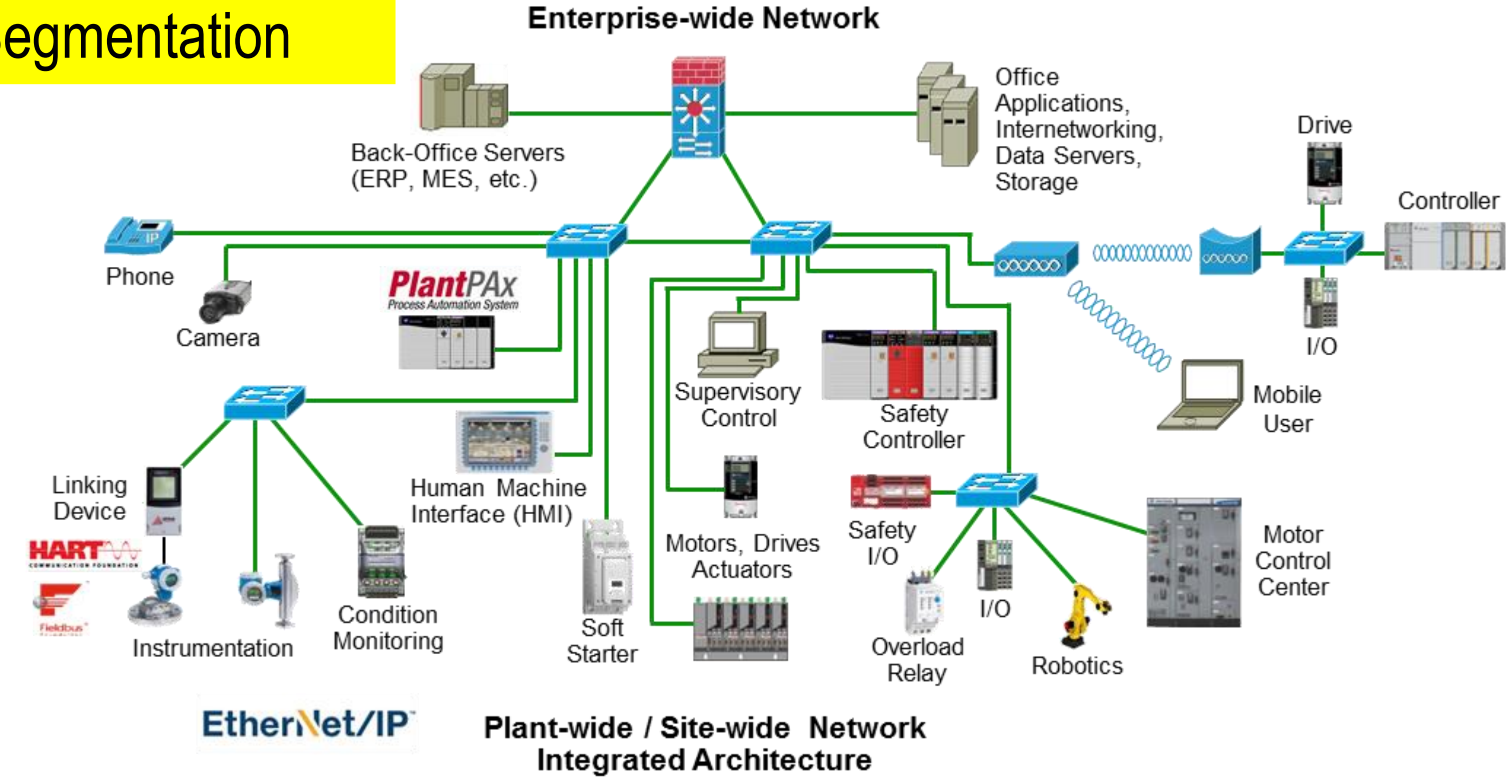
A reliable and secure architecture from an ecosystem of partners is critical to building a Connected Enterprise.

- Application — Rockwell Automation; Rockwell Automation PartnerNetwork™
- Software — Rockwell Automation; Rockwell Automation PartnerNetwork™
- Network — Rockwell Automation; Rockwell Automation PartnerNetwork™; EtherNet/IP™ ODVA

Industrial IoT (IIoT) – IACS Convergence

Challenges Associated with Technology Convergence

Large LAN, Lacking Natural Boundaries and Segmentation



Flat, Open and Non-Resilient
Industrial Automation and Control System (IACS)
Network Infrastructure

Rockwell Automation

Industrial IoT (IIoT) – IACS Convergence

Challenges Associated with Technology Convergence

- Plant-wide Industrial Ethernet Deployments
  - Single network technology for industrial automation and control system (IACS) control and information disciplines – e.g. drive, safety and motion
    - Different performance and resiliency requirements between IACS disciplines
  - Migration from isolated LANs to large flat and open LANs:
    - Loss of boundaries and natural segmentation
    - Network sprawl – lack of design discipline

- Open Doesn't Mean Easy; Standard Doesn't Mean Foolproof
  - Open by default – must secure by design, architecture and configuration
  - Varying implementations of Layer 2/3 network services within and across IIoT technologies may create incompatibilities
  - Customers required to invest in their own test labs to validate technology and products to meet their application requirements

IACS Application Requirements

Challenges Associated with Technology Convergence

What is secure? **What is real-time?** **What is resilient?**

	Process Automation	Discrete Automation	Loss Critical
			
Function	Information Integration, Slower Process Automation	Time-critical Discrete Automation	Multi-axis Motion Control
Communication Technology	.Net, DCOM, TCP/IP	Industrial Protocols - CIP	Hardware and Software solutions, e.g. CIP Motion, PTP
Period	10 ms to 1 second or longer	1 ms to 100 ms	100 µs to 10 ms
Industries	Oil & Gas, chemicals, energy, water	Auto, food and beverage, semiconductor, metals, pharmaceutical	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	Synchronization of multiple axes: printing presses, wire drawing, web making, picking and placing

- Only you can define what this means for your application.
- Application dependent.
- One size does not fit all!

Source: ARC Advisory Group

Rockwell Automation

Stance on Availability, Safety and Security

- Drivers for risk management policies and overall risk tolerance:
  - Business practices
  - Corporate / local standards
  - Application requirements
  - Applicable industry standards – e.g. NERC CIP
  - Government regulations and compliance
  - Industry Standards

Early, open and two-way OT-IT dialogue is critical!

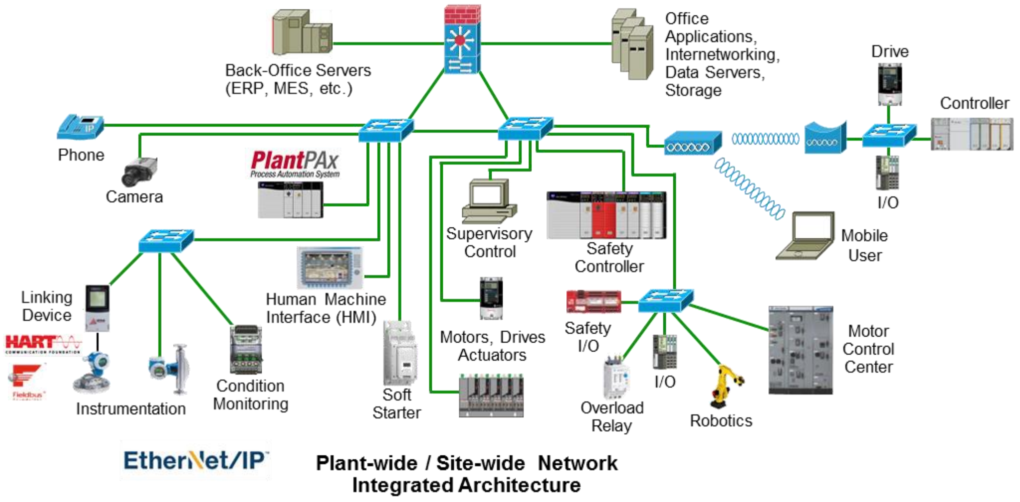
"one-size-fits-all"

- Enterprise and industrial policies and procedures (safety and security), for access control (avoidance of back doors) and network ownership
  - Alignment with industrial functional safety standards such as IEC 61508, IEC 62061 (SIL), ISO 13849 (PL)
  - Alignment with industrial security standards such as IEC-62443 (formerly ISA99), NIST 800-82 and ICS-CERT
  - Network capabilities (zone segmentation into domains of trust)

Industrial IoT (IIoT) – IACS Convergence

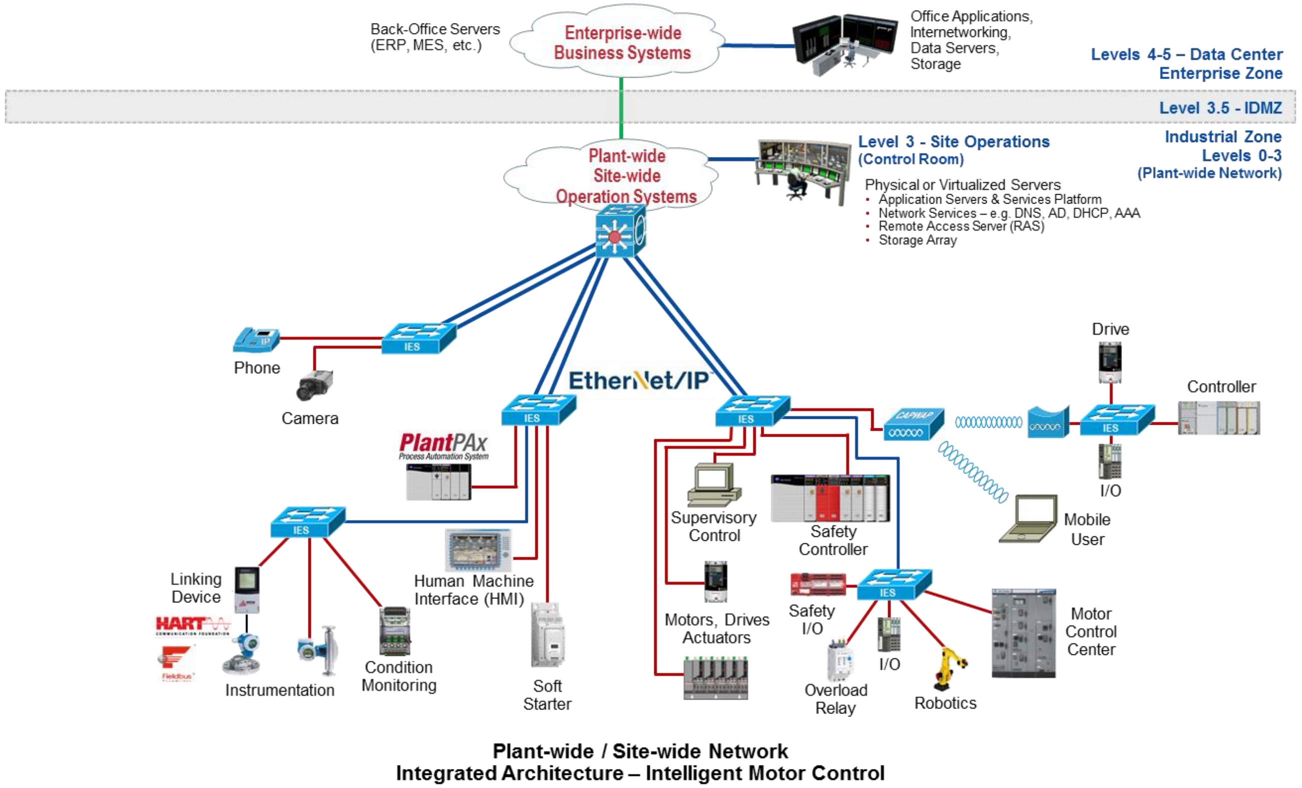
Challenges Associated with Technology Convergence

Large LAN, Lacking Natural Boundaries and Segmentation



Flat, Open and Non-Resilient IACS Network Infrastructure

Smaller Connected LANs to Create Boundaries and Segmentation

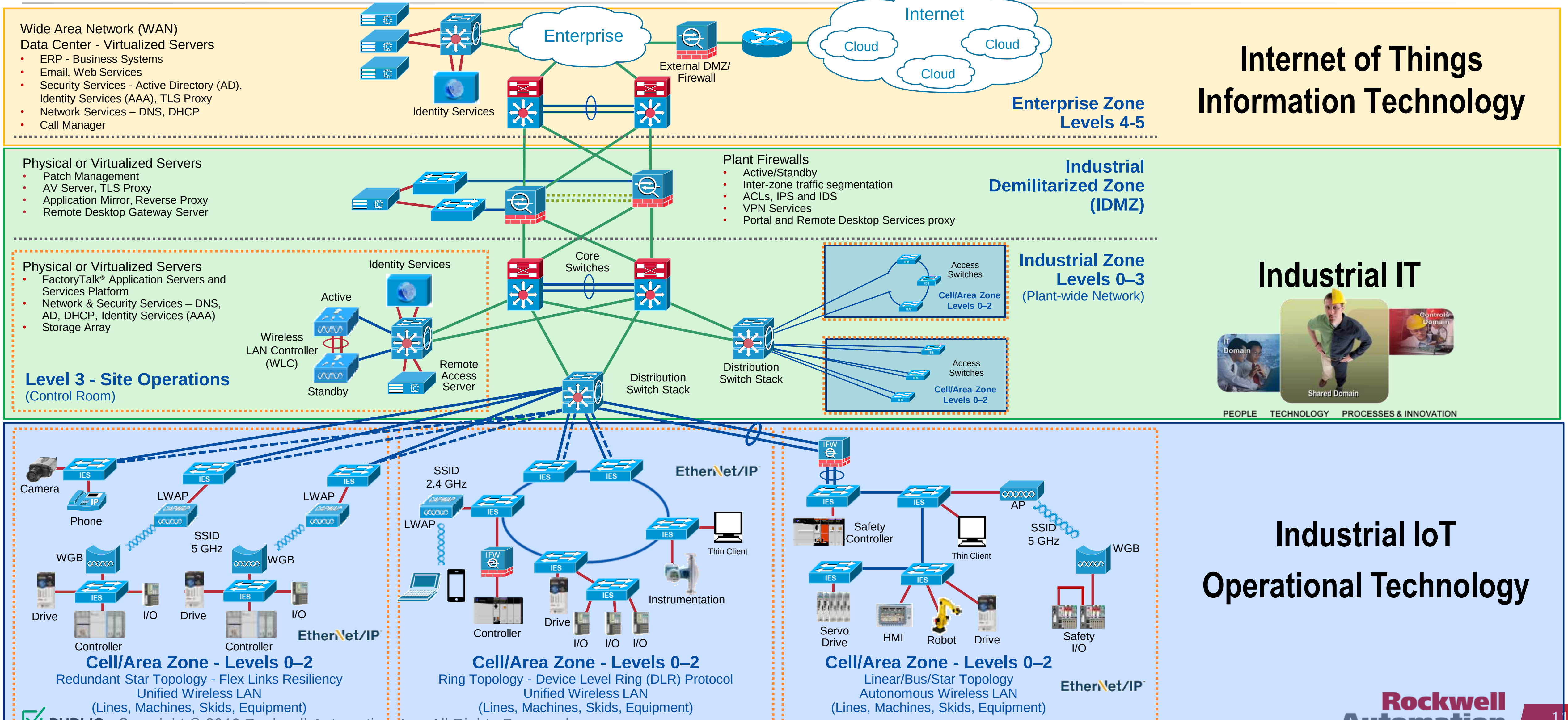


Structured and Hardened IACS Network Infrastructure

Rockwell Automation

OT-IT Collaboration / Convergence

Challenges Associated with Technology Convergence



Rockwell Automation

OT-IT Collaboration / Convergence

Challenges Associated with Technology Convergence

- Technology Differences
  - Software and hardware toolsets
  - Varying implementations of Layer 2/3 network services may create incompatibilities
    - Availability, Performance, Traffic Types, Security
- Cultural Differences
  - Availability SLA (service level agreement)
    - Minutes/Hours vs. Hours/Days
  - Policies
    - Security – CIA vs. AIC
    - QoS – prioritization of voice and video
    - NAT, Multicast
- Skill-gaps – Workforce Development
  - OT personnel with knowledge of IT skills and requirements
  - IT personnel with knowledge of OT skills and requirements
  - Lack of Industrial IT personnel
- Functional Differences and Incompatibilities between IT:
  - Technologies – e.g. resiliency
  - Products – e.g. QoS policies
  - Applications – e.g. WebEx and Skype
  - Solutions – e.g. network access control

Technology and Cultural Convergence - Similarities and Differences

Challenges Associated with Technology Convergence

Criteria	Industrial OT Network	Enterprise IT Network
Environment	• Plant-floor • Control Room • Control Panel, Industrial Distribution Frame (IDF)	• Carpeted Space, Data Center • Data Communication or Wiring Closet, Intermediate Distribution Frame (IDF)
Switches	• Managed and unmanaged • Layer 2 is predominant • DIN rail or panel mount is predominant	• Managed • Layer 2 and Layer 3 • Rack mount
Wireless	• Autonomous (locally managed) – point solutions • Mobile equipment (emerging) and personnel (prevalent)	• Unified (centrally managed) solutions • Mobile personnel – corporate provided or BYOD • Guest access
Computing	• Industrial Hardened Panel Mount Computers and Monitors • Desktop, Notebook • 19" Rack Server • Virtualization - becoming prevalent • Hardening – sporadic patching and white listing	• Desktop, Notebook • Tablets • 19" Rack Server and Blade Server • Unified Computing Systems (UCS) • Virtualization – widespread • Hardening - patching and white listing

Technology and Cultural Convergence - Similarities and Differences

Challenges Associated with Technology Convergence

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 • Sporadic use of standard Layer 2 and Layer 3 network and security services	• Standard IEEE 802.3 Ethernet • Standard IETF Internet Protocol (IPv4 and IPv6) • Pervasive use of standard Layer 2 and Layer 3 network and security services
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

Technology and Cultural Convergence - Similarities and Differences

Challenges Associated with Technology Convergence

Criteria	Industrial OT Network	Enterprise IT Network
Traffic Type	• Primarily local – traffic between local assets • Information, control, safety, motion, time synchronization, energy management • Smaller Ethernet 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 IP packets and Ethernet frames • Standard application layer protocols: HTTP, SNMP, DNS, RTP, SSH, etc.
Performance	• Low Latency, Low Jitter (1 ms, 100s ns) • Data Prioritization – QoS – Layer 2 and 3	• Low Latency, Low Jitter (100s ms, 10s ms) • Data Prioritization – QoS – Layer 3
Security	• Open by default, must secure by design, architecture and configuration • 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 best practices • Strong security policies • Line-of-sight across the Enterprise and to the Internet

Technology and Cultural Convergence - Similarities and Differences

Challenges Associated with Technology Convergence

Criteria	Industrial OT Network	Enterprise IT Network
Focus	24/7 operations, high OEE	Protecting intellectual property and company assets
Precedence of Priorities	Availability Integrity Confidentiality	Confidentiality Integrity Availability
Types of Data Traffic	Converged network of data, control, information, safety and motion	Converged network of data, voice and video
Access Control	Strict physical access Simple network device access	Strict network authentication and access policies
Implications of a Device Failure	Production is down ($$'s/hour … or worse)	Work-around or wait
Threat Protection	Isolate threat but keep operating	Shut down access to detected threat
Upgrades	Scheduled during downtime	Automatically pushed during uptime

Industrial Network Design Methodology

Structured and Hardened Network Infrastructure

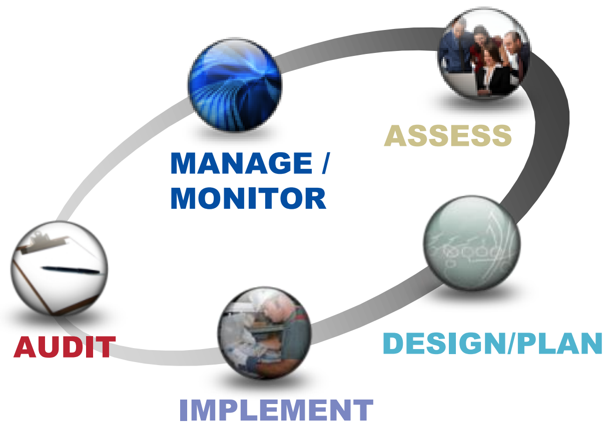
Industrial Network Design Methodology

Structured and Hardened Network Infrastructure

- Understand application and functional requirements
  - Devices to be connected – industrial and non-industrial
  - Data requirements for availability, integrity and confidentiality
  - Communication patterns, topology and resiliency requirements
  - Types of traffic – information, control, safety, time synchronization, drive control, voice, video
- Develop a logical framework (zoning)
  - Define zones and segmentation (smaller connected LANs), place applications and devices in the logical framework based on requirements
  - Migrate from flat, open and non-resilient networks to structured and hardened networks
- Develop a physical framework to align with the logical framework
- Deploy a holistic and diverse defense-in-depth security model
- Reduce risk, simplify design, and speed deployment:
  - Use information technology (IT) and operational technology (OT) standards
  - Use reference models and reference architectures

Avoiding Network Sprawl!!

Convergence-Ready OEM Solutions

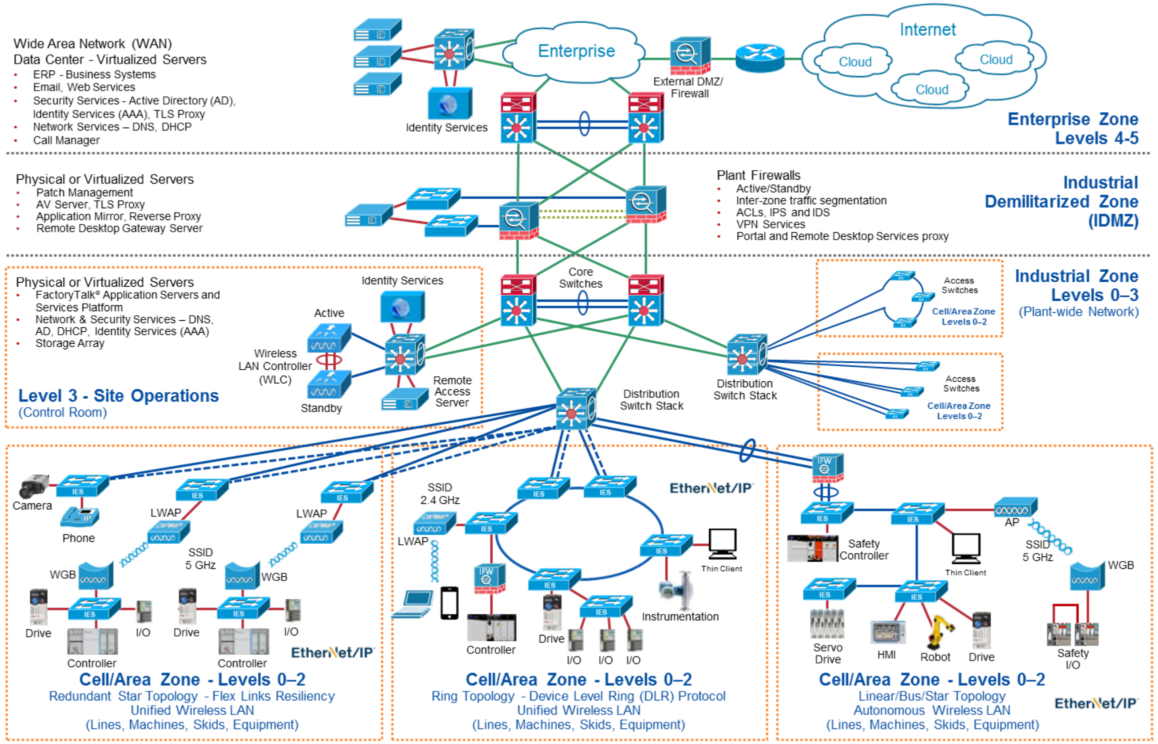


Rockwell Automation

Reference Architectures

Structured and Hardened Network Infrastructure

- What are reference architectures?
  - Baseline architectures, considerations and best practices for design and implementation.



- Reference Architectures:
  - Marketectures – high-level marketing illustrations
  - White papers and knowledgebase articles based on proof of concept (PoC) testing
  - Accelerator Toolkits:
    - Examples - Drives and Motion, Water Wastewater, Safety, Energy Management
  - System Configuration Drawings
    - Examples – Stratix®, MCC, Wi-Fi, ControlLogix®
  - Converged Plantwide Ethernet (CPwE) Architectures:
    - Cisco / Rockwell Automation Strategic Alliance
    - Tested and Validated Architectures
      - Test labs – Cisco, Rockwell Automation and Panduit
    - White papers, design guides, application guides

Cisco and Rockwell Automation®

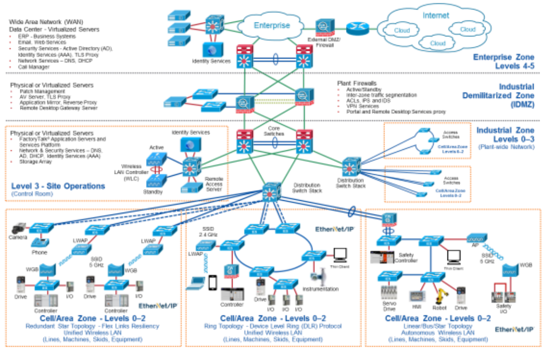
Structured and Hardened Network Infrastructure

Rockwell Automation Strategic Alliance

Plant of the Future - Common Technology View:

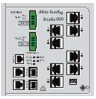
A single scalable architecture, using open and standard Ethernet, IP and Wi-Fi networking technologies, enabling the Industrial Internet of Things (IIoT) to help achieve the flexibility, visibility and efficiency required in a competitive manufacturing environment.

EtherNet/IP™ ODVA

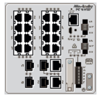


Converged Plantwide Ethernet (CPwE) Architectures:

Collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation. The content of CPwE is relevant to both operational technology (OT) and information technology (IT) disciplines. CPwE consists of documented architectures, best practices, design guidance and configuration settings to help manufacturers with development and deployment of a scalable, reliable, safe, secure and future-ready plant-wide industrial network infrastructure.






Joint Product Collaboration:

Combining the best of Rockwell Automation and Cisco - Stratix® 2500/Stratix 5000/Stratix 8000 families of managed industrial Ethernet switches, Stratix 5950 Security Appliance, and Stratix 5900 Services Router.

Workforce Development - People and Process Optimization:

Education, training, certifications and services to help facilitate OT and IT technology, network and cultural convergence.

Cisco Certified Specialist | Cisco Certified CCNA Industrial | Industrial IP Advantage | Cisco live! | Rockwell Automation TechED Inspire. Educate. Innovate. | Rockwell Automation Automation Fair

Rockwell Automation

Key Tenet

Smart IIoT Endpoints

EtherNet/IP Network Technology and Devices

Single Industrial Network Technology

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

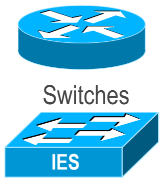
EtherNet/IP™

ISO

Open Systems Interconnection

Industrial Internet of Things (IIoT)

Layer No.		Layer Name	Function	Examples
Layer 7		Application	Network Services to User App	CIP - IEC 61158
Layer 6		Presentation	Encryption/Other processing	
Layer 5		Session	Manage Multiple Applications	
Layer 4		Transport	Reliable End-to-End Delivery Error Correction	IETF TCP/UDP
Layer 3	Routers	Network	Logical Addressing, Packet Delivery, Routing	IETF IP
Layer 2	Switches	Data Link	Framing of Data, Error Checking	IEEE 802.3/802.1/802.11
Layer 1	Cabling/RF	Physical	Signal type to transmit bits, pin-outs, cable type	IEEE : TIA-1005



5-Layer TCP/IP Model

Single Industrial Network Technology

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

EtherNet/IP™

ISO

Open Systems Interconnection

What makes EtherNet/IP industrial?

Layer No.		Layer Name	Function	Examples
Layer 7		Application	Network Services to User App	CIP - IEC 61158
Layer 6		Presentation	Encryption/Other processing	
Layer 5		Session	Manage Multiple Applications	
Layer 4		Transport	Reliable End-to-End Delivery Error Correction	IETF TCP/UDP
Layer 3	Routers	Network	Logical Addressing, Packet Delivery, Routing	IETF IP
Layer 2	Switches	Data Link	Framing of Data, Error Checking	IEEE 802.3/802.1/802.11
Layer 1	Cabling/RF	Physical	Signal type to transmit bits, pin-outs, cable type	IEEE : TIA-1005

Physical Layer Hardening

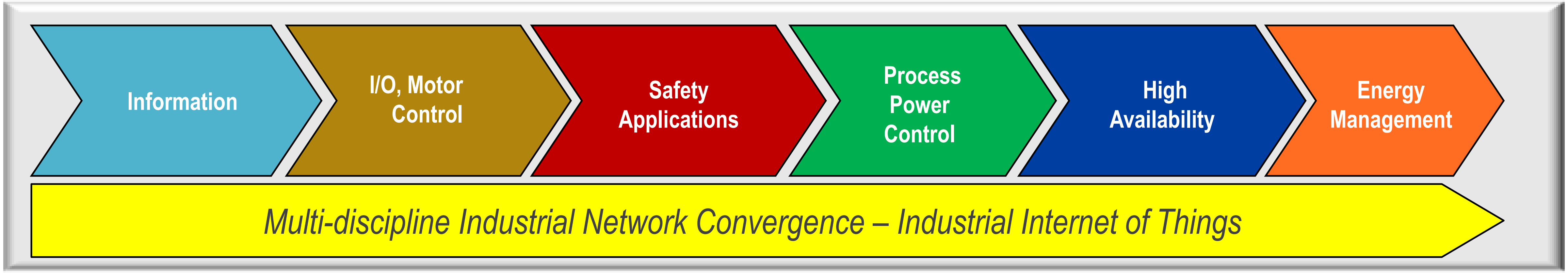
Infrastructure Device Hardening

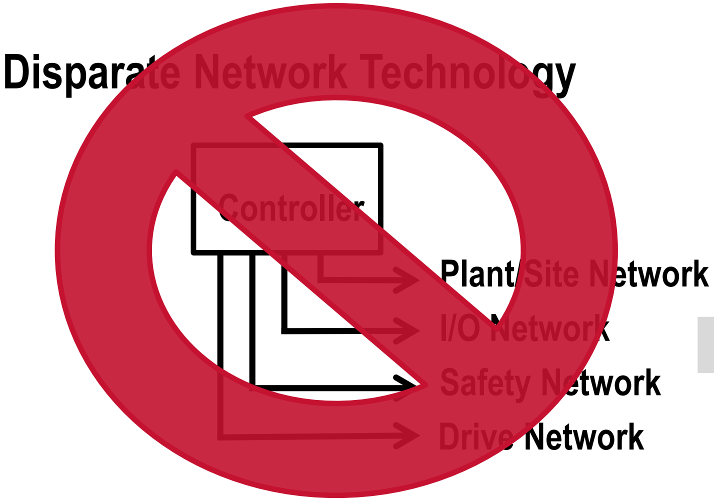
Common Application Layer Protocol

Rockwell Automation

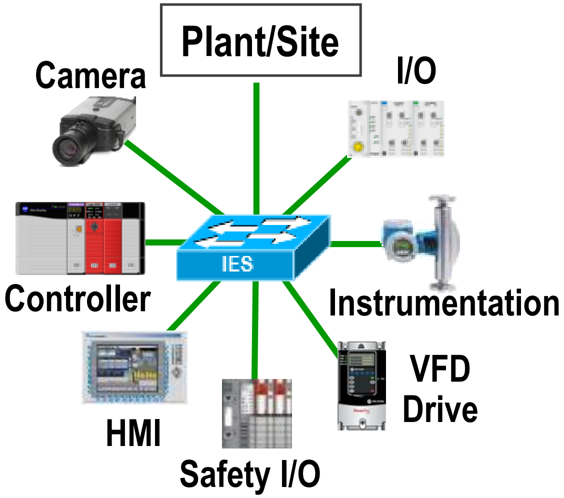
Industrial Application Convergence

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices





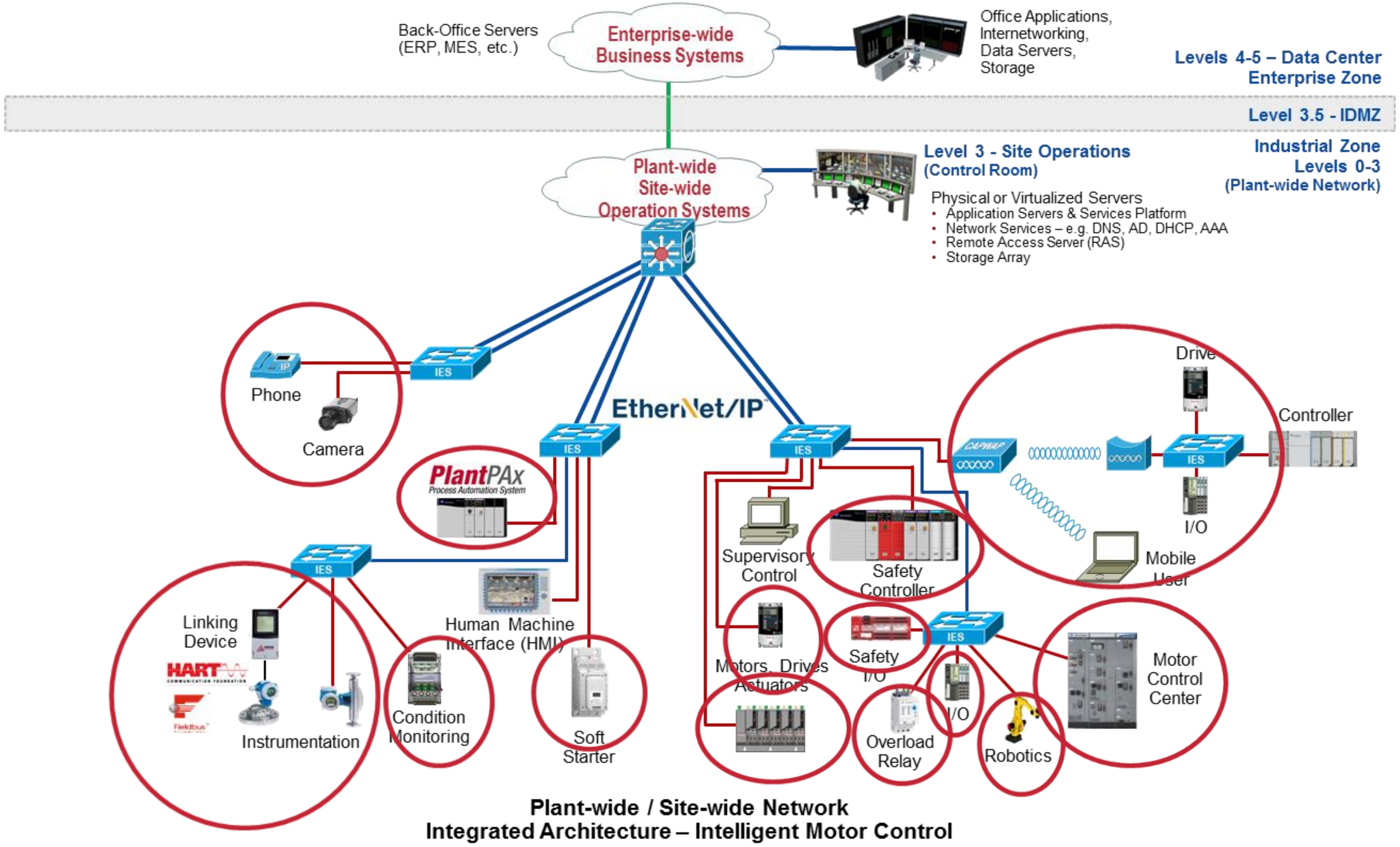
Single Industrial Network Technology



EtherNet/IP™

Industrial Application Convergence

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices



Industrial Internet of Things (IIoT)

Rockwell Automation Encompass™ Product Partner

EtherNet/IP Device Selection

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

- ODVA
  - Conformance tested, with declaration of conformity
  - PlugFest - interoperability testing in a full multi-vendor system configuration
- Selection of Controllers
  - # EtherNet/IP ports, types, topology
  - Environment: on-machine / in-panel
  - Communication speed
  - Maximum # of nodes
  - Minimum requested packet interval (RPI)
  - Maximum I/O data size per RPI
- Selection of Sensor / Actuators
  - Application Requirements
  - Environment: on-machine / in-panel
  - # EtherNet/IP ports, types, topology
  - Communication speed
  - Minimum RPI (how fast)
  - Maximum I/O Data Size per RPI
- Selection Tools
  - Integrated Architecture Builder (IAB)
  - EtherNet/IP Capacity Tool
  - System Configuration Drawings (PCDs)

EtherNet/IP Advantage

Smart IIoT Endpoints – EtherNet/IP: Network Technology and Devices

- Single industrial network technology for:
  - Multi-discipline Network Convergence - Discrete, Continuous Process, Batch, Motor, Safety, Motion, Power, Time Synchronization, Supervisory Information, Asset Configuration/Diagnostics
- Established
  - Risk reduction – broad availability of products, applications and vendor support
  - ODVA: Cisco Systems®, Endress+Hauser, Rockwell Automation® are principal members
  - Supported – Conformance testing, defined QoS priority values for EtherNet/IP devices
- Standard – IEEE 802.3 Ethernet and IETF TCP/IP Protocol Suite
  - Enables convergence of OT and IT – common toolsets (assets for design, deployment and troubleshooting) and skills/training (human assets)
  - Topology and media independence – flexibility and choice
  - Device-level and switch-level topologies; copper - fiber - wireless
- Portability and routability – seamless plant-wide / site-wide information sharing
  - No data mapping – simplifies design, speeds deployment and reduces risk

Key Tenet

Zoning (Segmentation)

Structured and Hardened Network Infrastructure

Zoning (Segmentation)

- Smaller Connected LANs to help:
  - Minimize network sprawl
  - Modular building block approach for scalable, reliable, safe, secure and future-ready network infrastructure
  - Segment Industrial IoT Technologies
  - Smaller Layer 2 broadcast domains
    - Restrict Layer 2 broadcast traffic
    - Smaller fault domains (e.g. Layer 2 loops)
    - Smaller domains of trust (security)

- Multiple techniques to create smaller network building blocks (Layer 2 domains)
  - Logical zoning – geographical and functional organization of IACS devices
  - Multiple network interface cards (NICs) – e.g. CIP bridge
  - Campus network model - multi-tier switch hierarchy – Layer 2 and Layer 3
  - Virtual Local Area Networks (VLANs) with Access Control Lists (ACLs), Firewalls
  - Network Address Translation (NAT)
  - Software-Defined Segmentation via Security Group Tagging (SGT)

Key Tenet

Logical Zoning (Segmentation)

CPwE Logical Model - Built on Technology and Industry Standards

Logical Zoning (Segmentation)

OT Standards

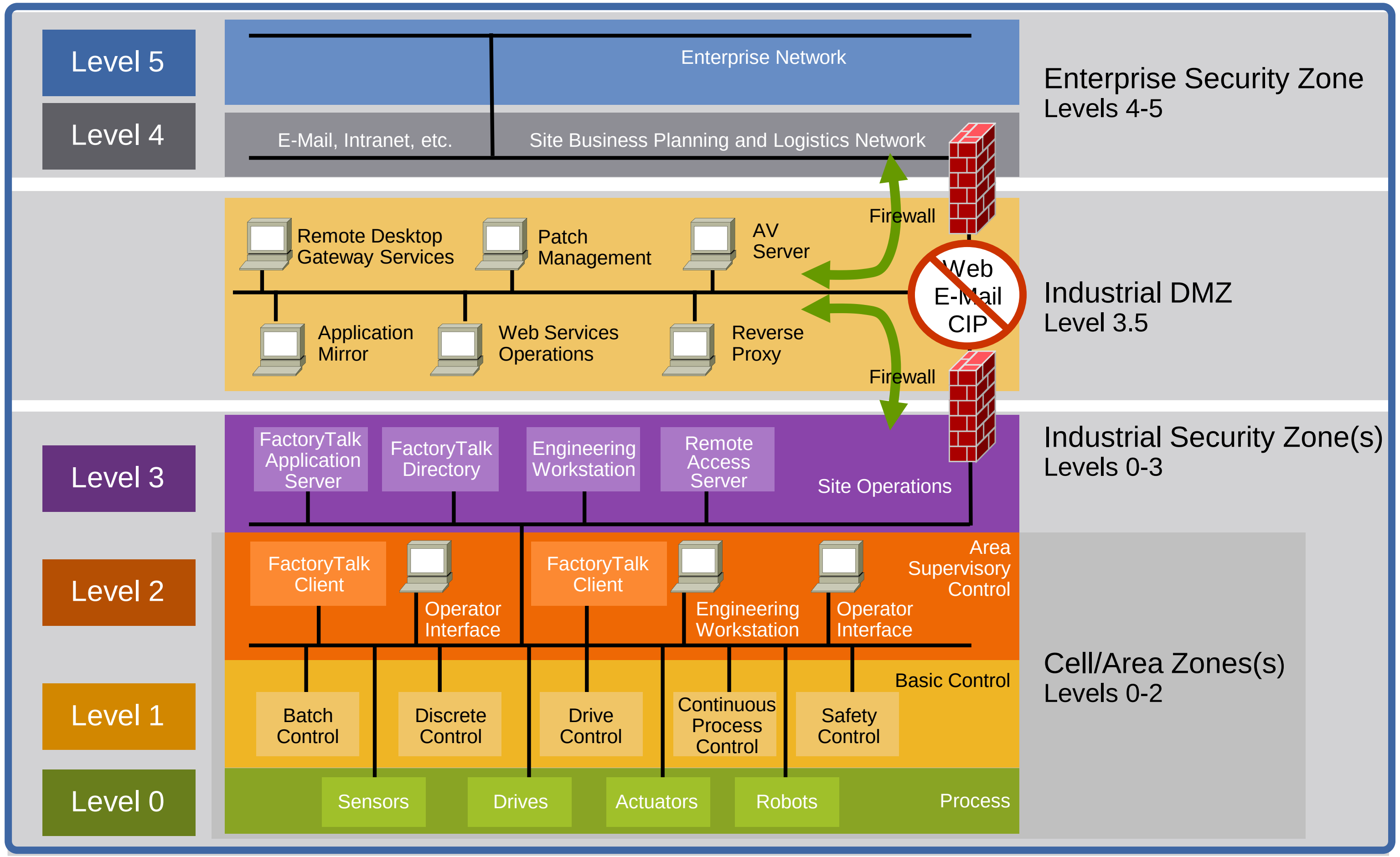
- Operational Levels
  - ISA 95, Purdue – Levels 0-5
    - Level 0 Sensor/Actuators
    - Level 1 Controller
    - Level 2 Local Supervisor
    - Level 3 Site Operations
    - Levels 4-5 Enterprise
- Functional / Security Zones
  - IEC-62443, NIST 800-82, DHS/INL/ICS-CERT
    - Enterprise, Industrial, IDMZ
    - Industrial Subzones – Cell/Area, Site Operations

IT Standards

- Network Technology
  - OSI Reference Model – 7 Layers
  - IEEE 802.1, 802.3, 802.11
  - IETF TCP, UDP, IP
- Network Switch Hierarchy
  - Campus Network Model
    - Layer 2 Access
    - Layer 3 Distribution/Aggregation
    - Layer 3 Core

CPwE Logical Model - Operational Levels - Functional / Security Zones

Logical Zoning (Segmentation)



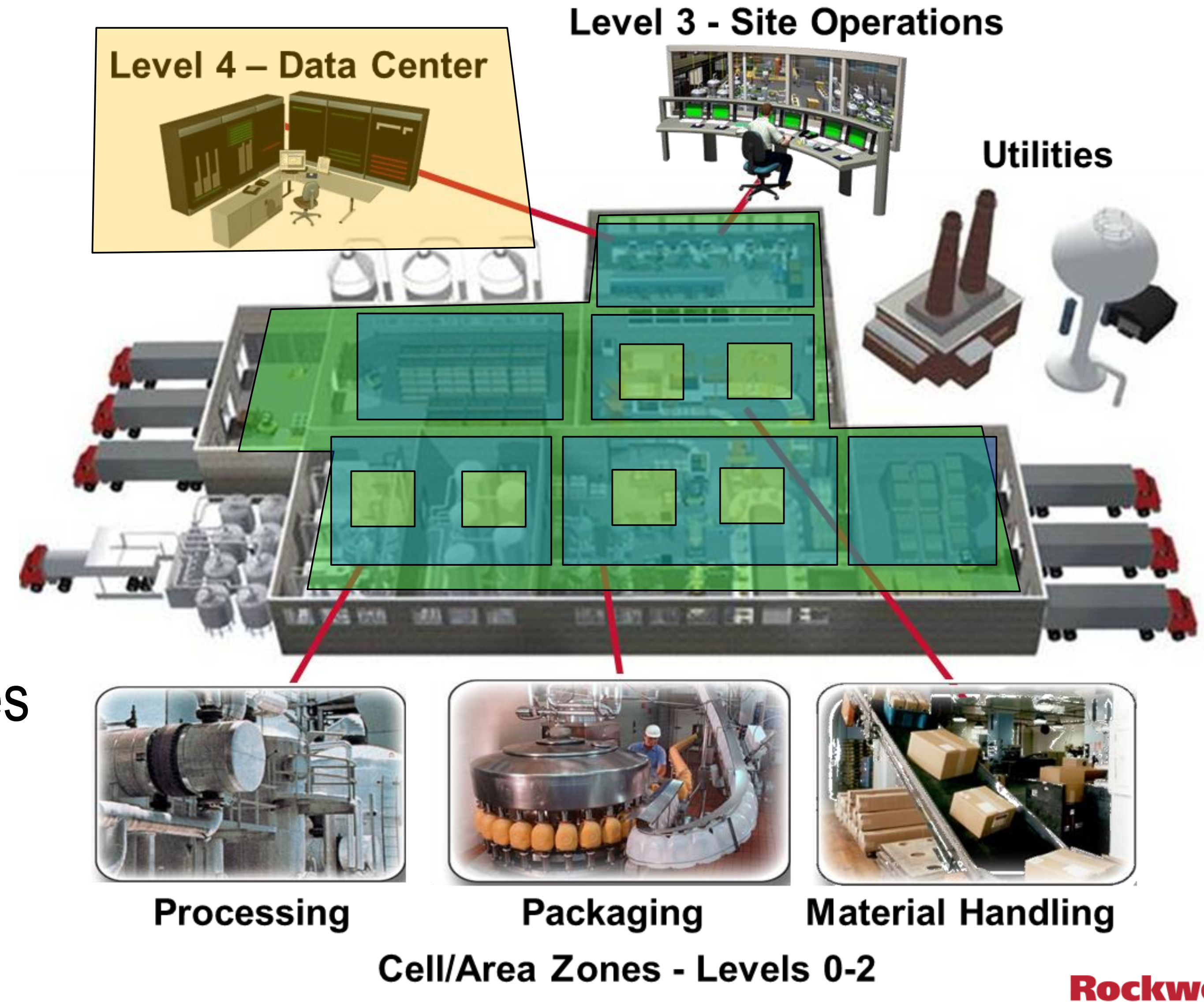
- Levels – ISA 95, Purdue Reference Model
- Zones – IEC 62443, NIST 800-82, DHS/INL/ICS-CERT Recommended Practices

Plant-wide Functional / Security Zoning

Logical Zoning (Segmentation)

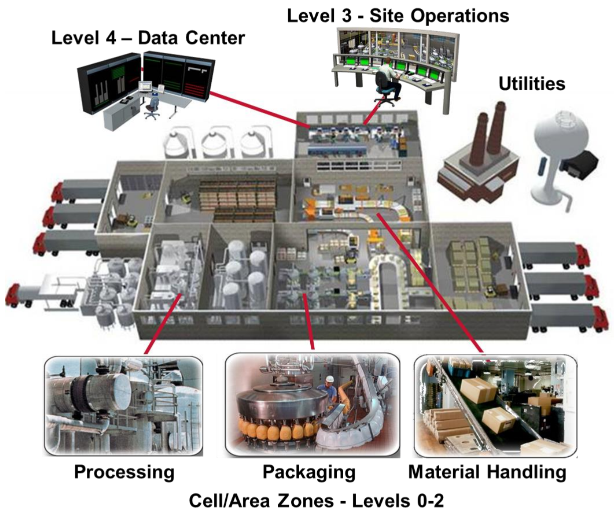
Plant-wide Zoning

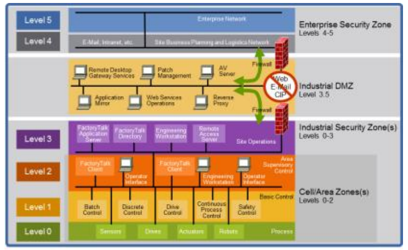
- Functional / Security Areas
- Smaller Connected LANs
  - Smaller Broadcast Domains
  - Smaller Fault Domains
  - Smaller Domains of Trust
- IEC 62443-3-2 Security Zones and Secure Conduits Model
- DHS/INL/ICS-CERT Best Practices
- Industrial IoT Technology
- Building Block Approach for Scalability

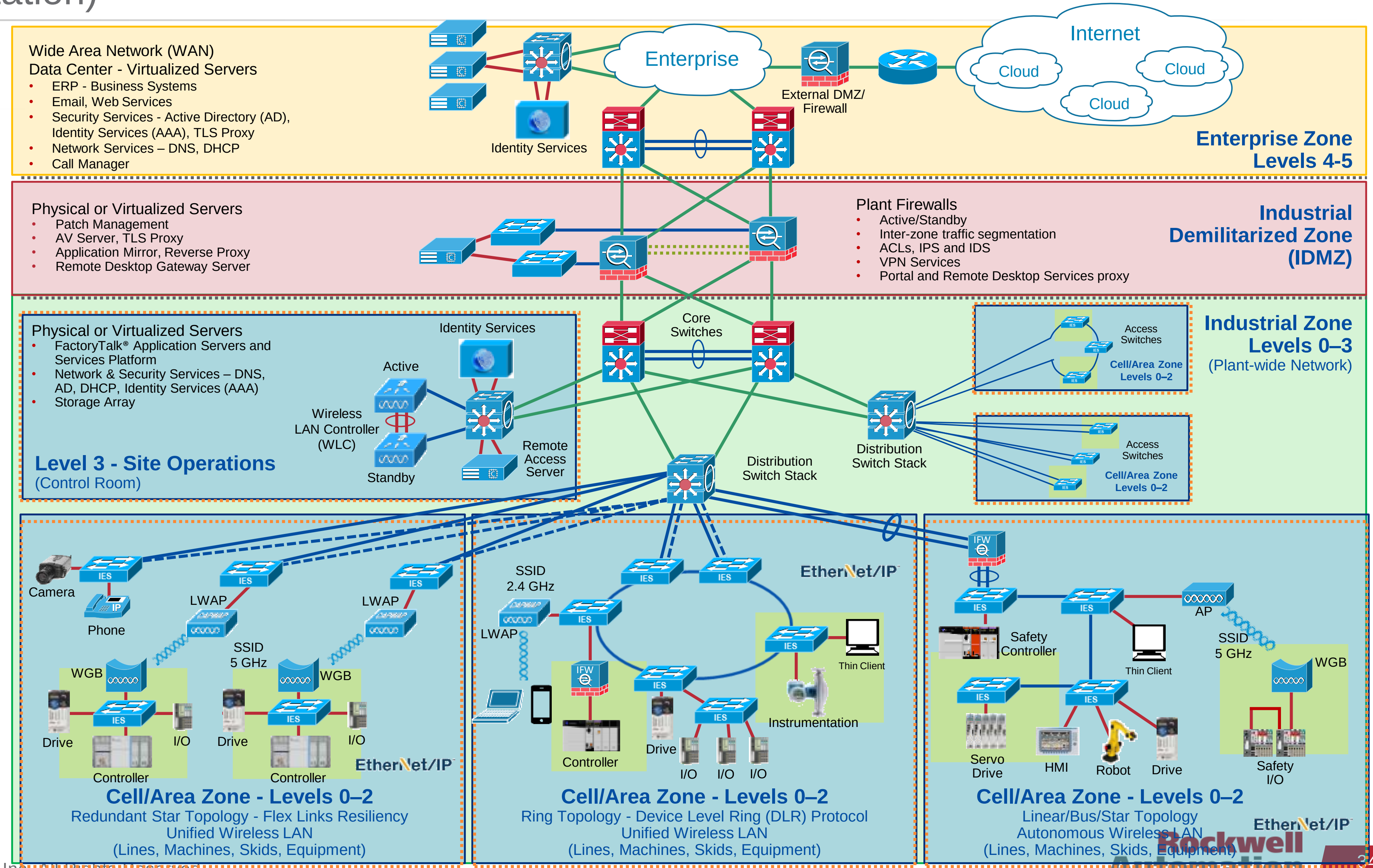


Plant-wide Functional / Security Zoning

Logical Zoning (Segmentation)





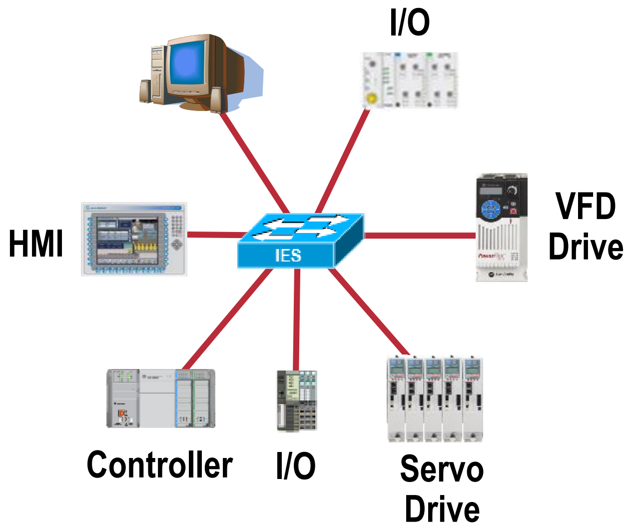


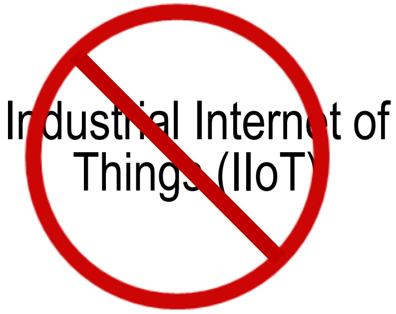
Key Tenet

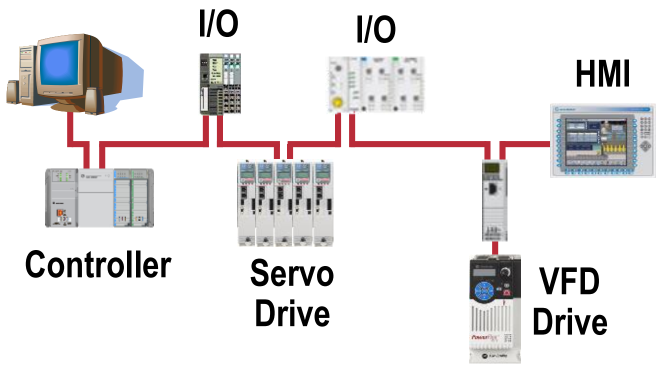
Segmentation – Network Services

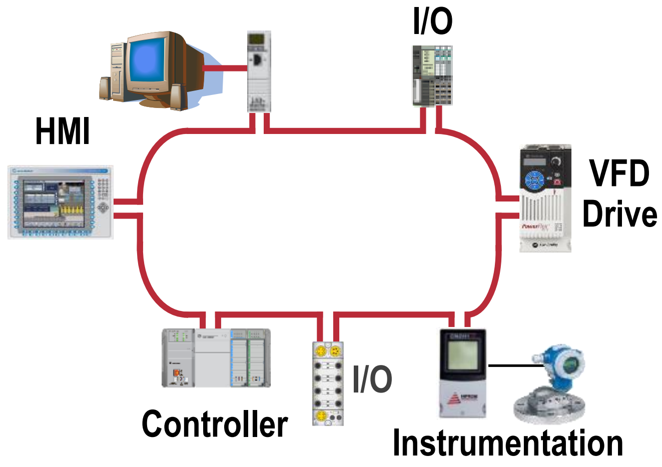
Islands of Automation with Isolated Local Area Networks (LANs)

Segmentation – Network Services



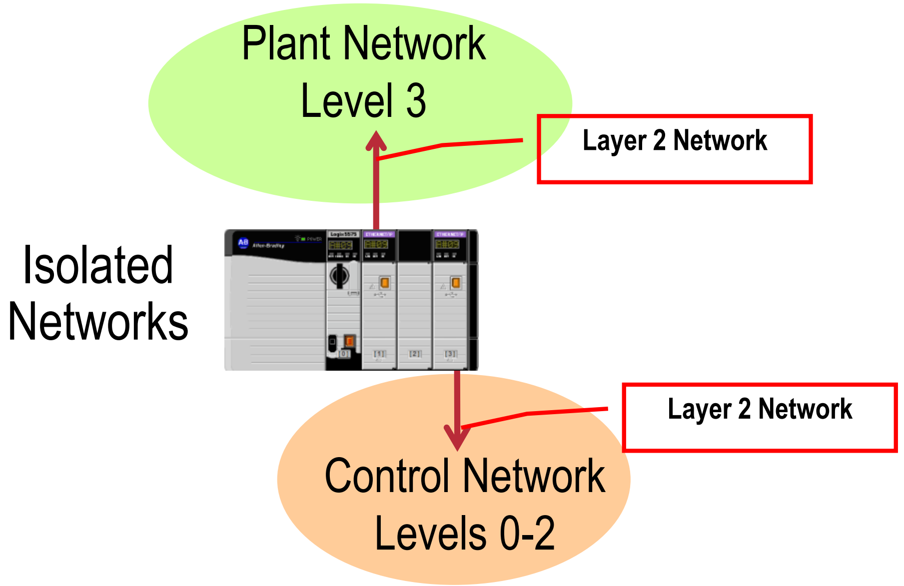


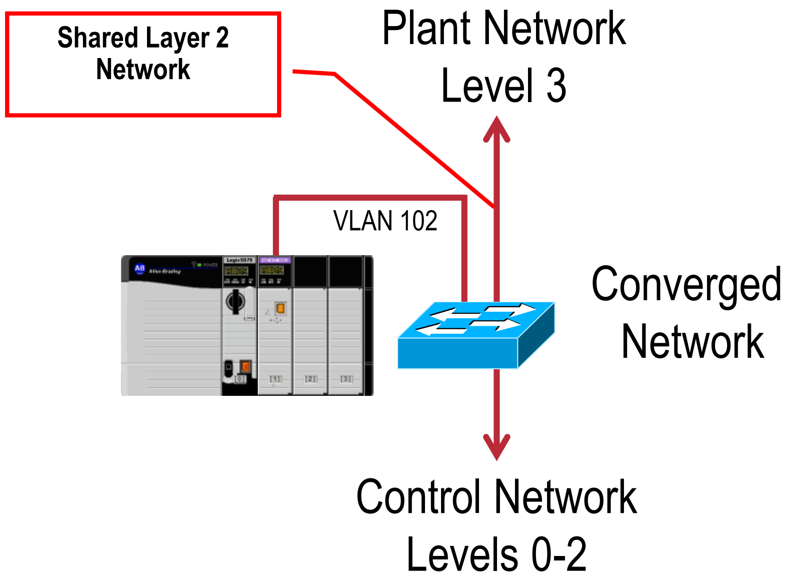




Multiple Network Interface Cards (NICs) - CIP™ Bridge

Segmentation – Network Services



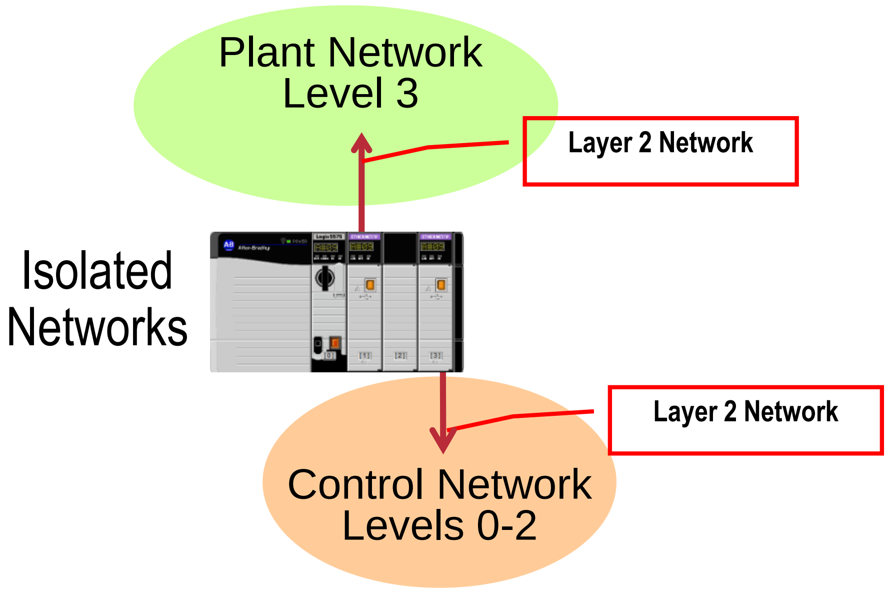


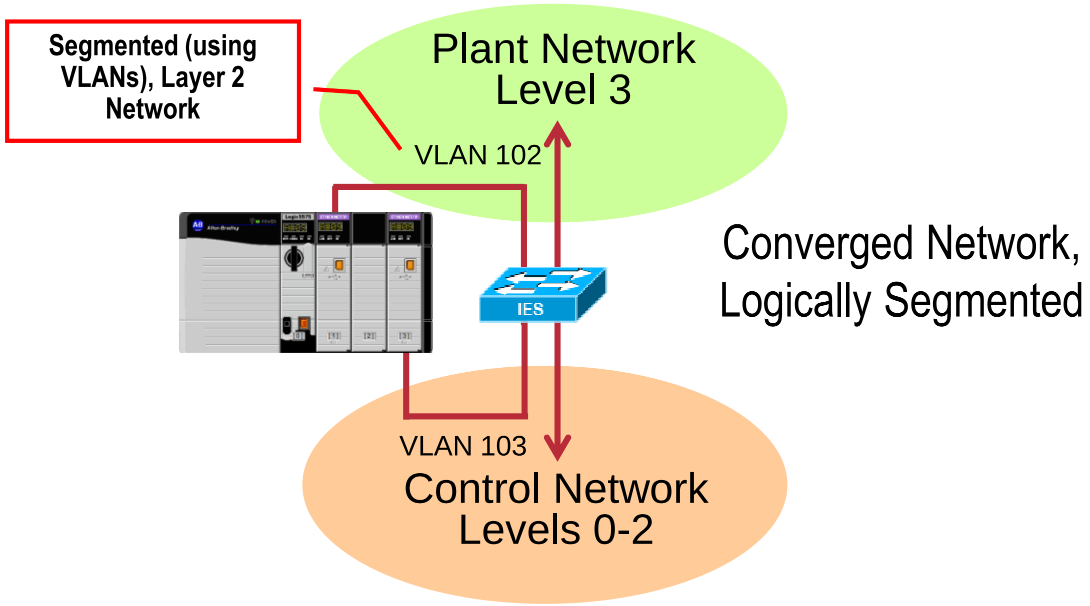
- Benefits
  - Clear network ownership demarcation line
- Challenges
  - Limited visibility to control network devices for asset management
  - Limited future-ready capability
  - Smaller PACs may not support

- Benefits
  - Plant-wide information sharing for data collection and asset management
  - Future-ready
- Challenges
  - Blurred network ownership demarcation line

Multiple Network Interface Cards (NICs) - CIP™ Bridge

Segmentation – Network Services



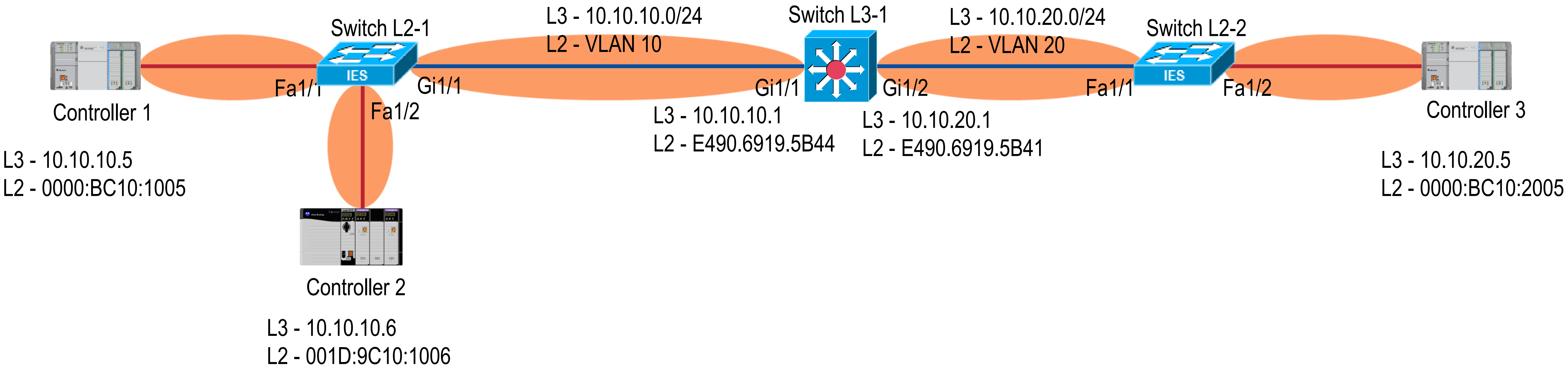


- Benefits
  - Clear network ownership demarcation line
- Challenges
  - Limited visibility to control network devices for asset management
  - Limited future-ready capability
  - Smaller PACs may not support

- Benefits
  - Plant-wide information sharing for data collection and asset management
  - Future-ready
- Challenges
  - Blurred network ownership demarcation line

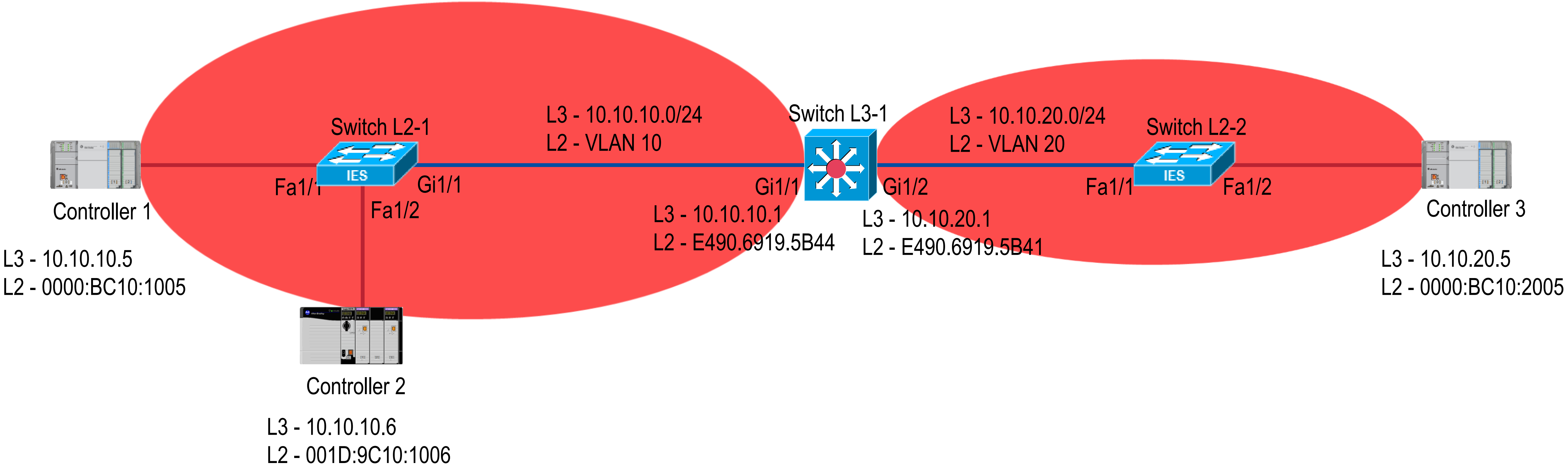
Layer 2 Collision Domains

Segmentation – Network Services



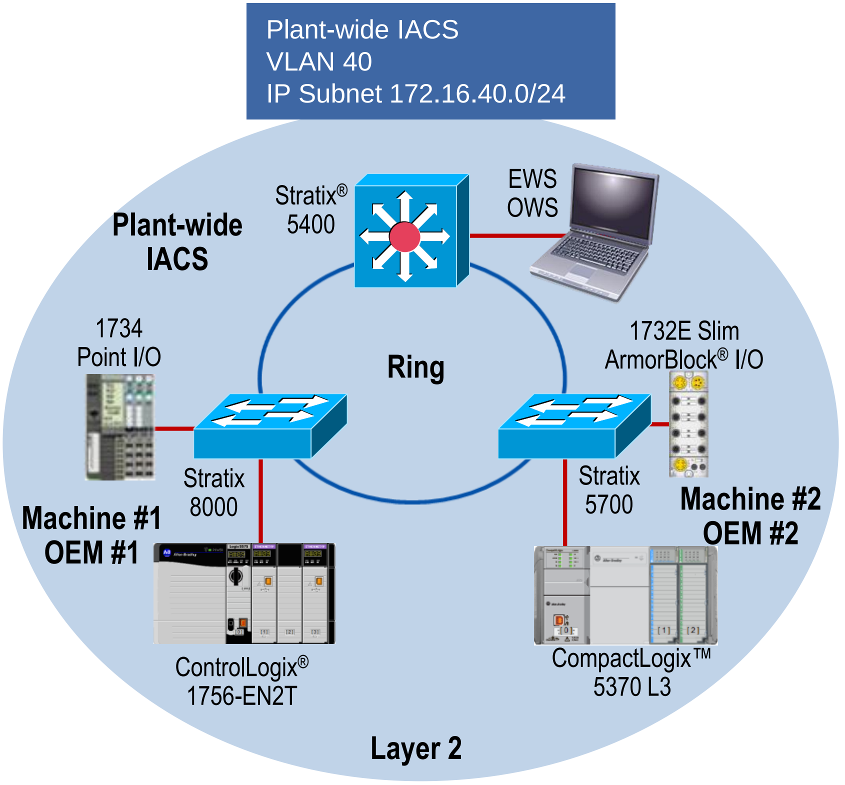
Layer 2 Broadcast Domains - Switch Hierarchy

Segmentation – Network Services

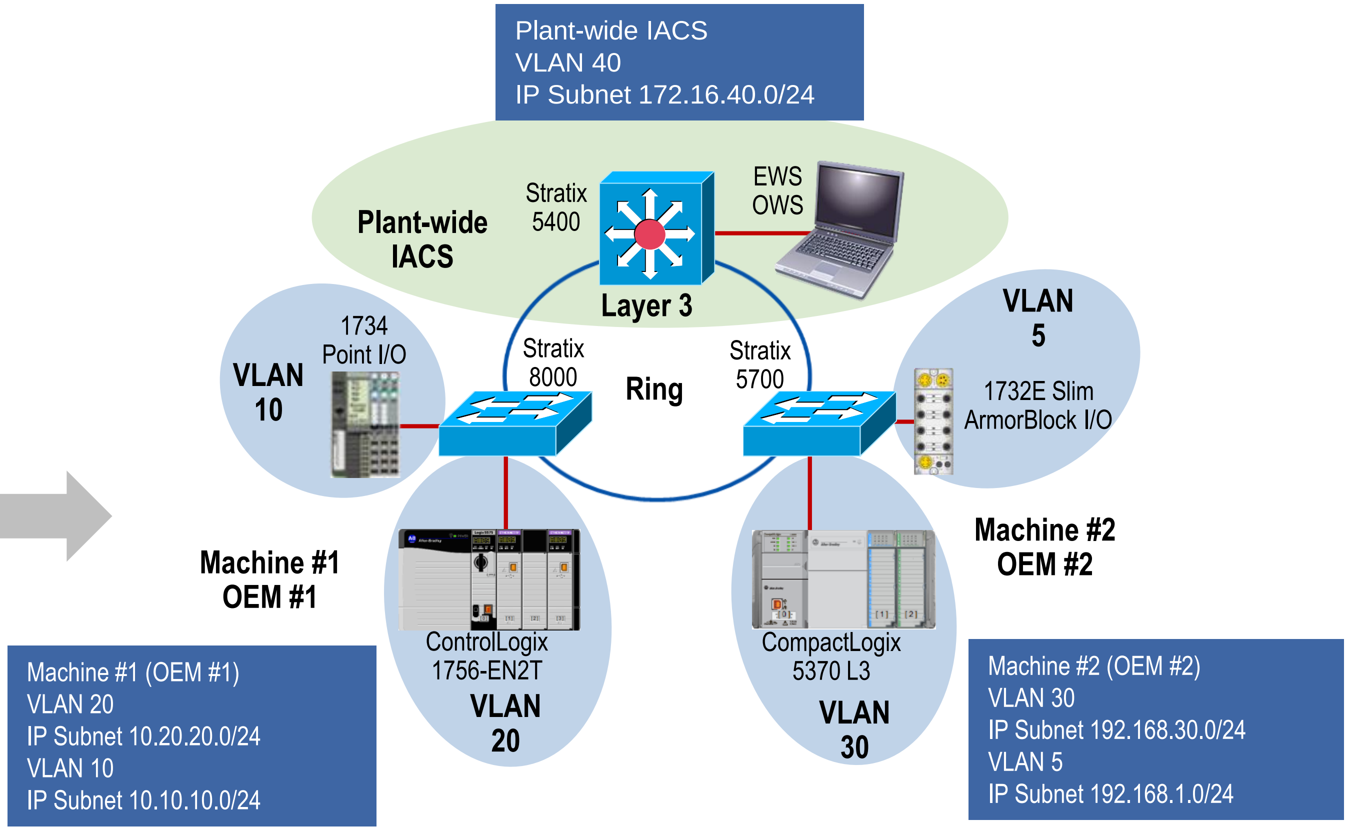


Switch Hierarchy, Virtual LANs (VLANs)

Segmentation – Network Services



Large Flat LAN
Larger Layer 2 Broadcast Domain

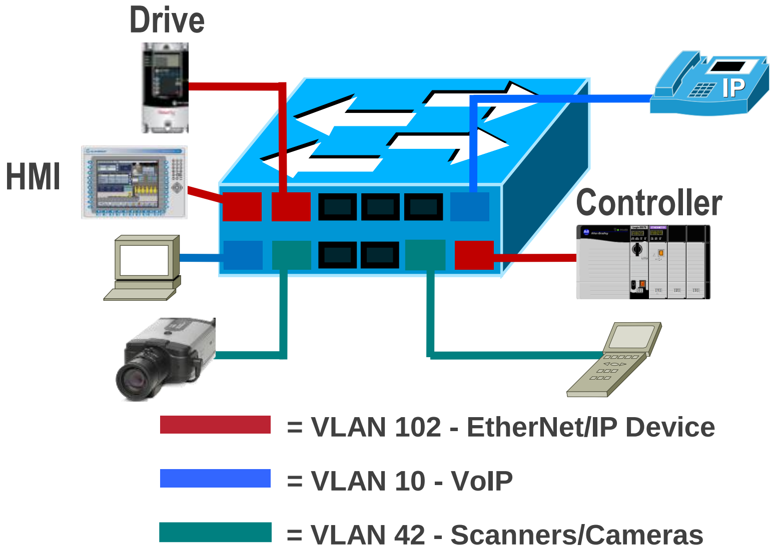


Small Connected LANs
Smaller Layer 2 Broadcast Domains

Virtual Local Area Networks (VLANs)

Segmentation – Network Services

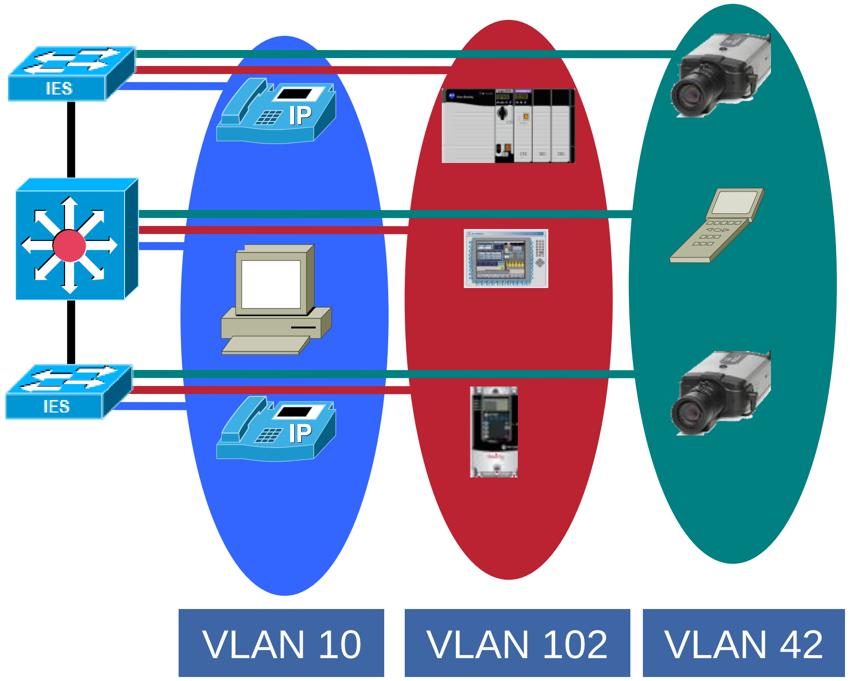
- Layer 2 network service, VLANs segment a network logically without being restricted by physical connections
  - VLAN established within or across switches
- Data is only forwarded to ports within the same VLAN
  - Devices within each VLAN can only communicate with other devices on the same VLAN
- Segments traffic to restrict unwanted broadcast and multicast traffic
- Software configurable using managed switches
- Benefits
  - Ease network changes – minimize network cabling
  - Simplifies network security management - domains of trust
  - Increase efficiency



Virtual Local Area Networks (VLANs)

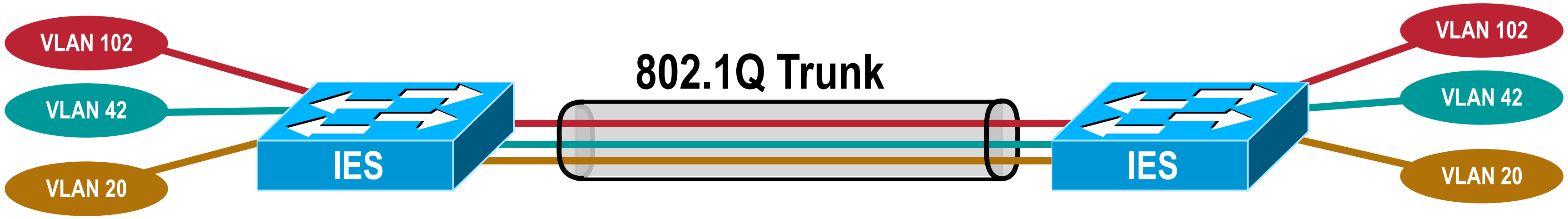
Segmentation – Network Services

- Layer 2 VLAN Trunking
  - Independent of physical switch location
  - Logically group assets by type, role, logical area, physical area or a hybrid of these
  - Devices communicate as if they are on the same physical segment – no re-cabling required
- Software configurable using managed switches
- A Layer 3 device (Router or Layer 3 switch) is required to forward traffic between different VLANs
  - Inter-VLAN routing



Virtual Local Area Networks (VLANs)

Segmentation – Network Services



Pre	SFD	DA	SA	Type/Len	Data (Payload)	FCS

Original Ethernet Frame

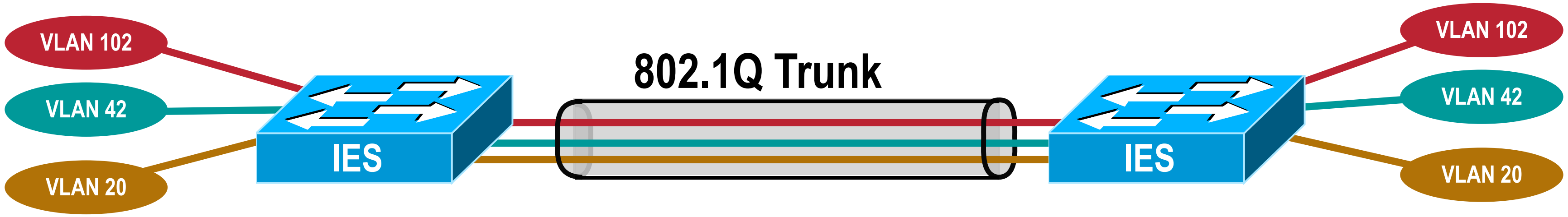
Pre	SFD	DA	SA	Tag	Type/Len	Data (Payload)	FCS

Tagged Ethernet Frame

- Trunking Methods
  - IEEE 802.1Q, generally referred to as “dot1q”

Virtual Local Area Networks (VLANs)

Segmentation – Network Services

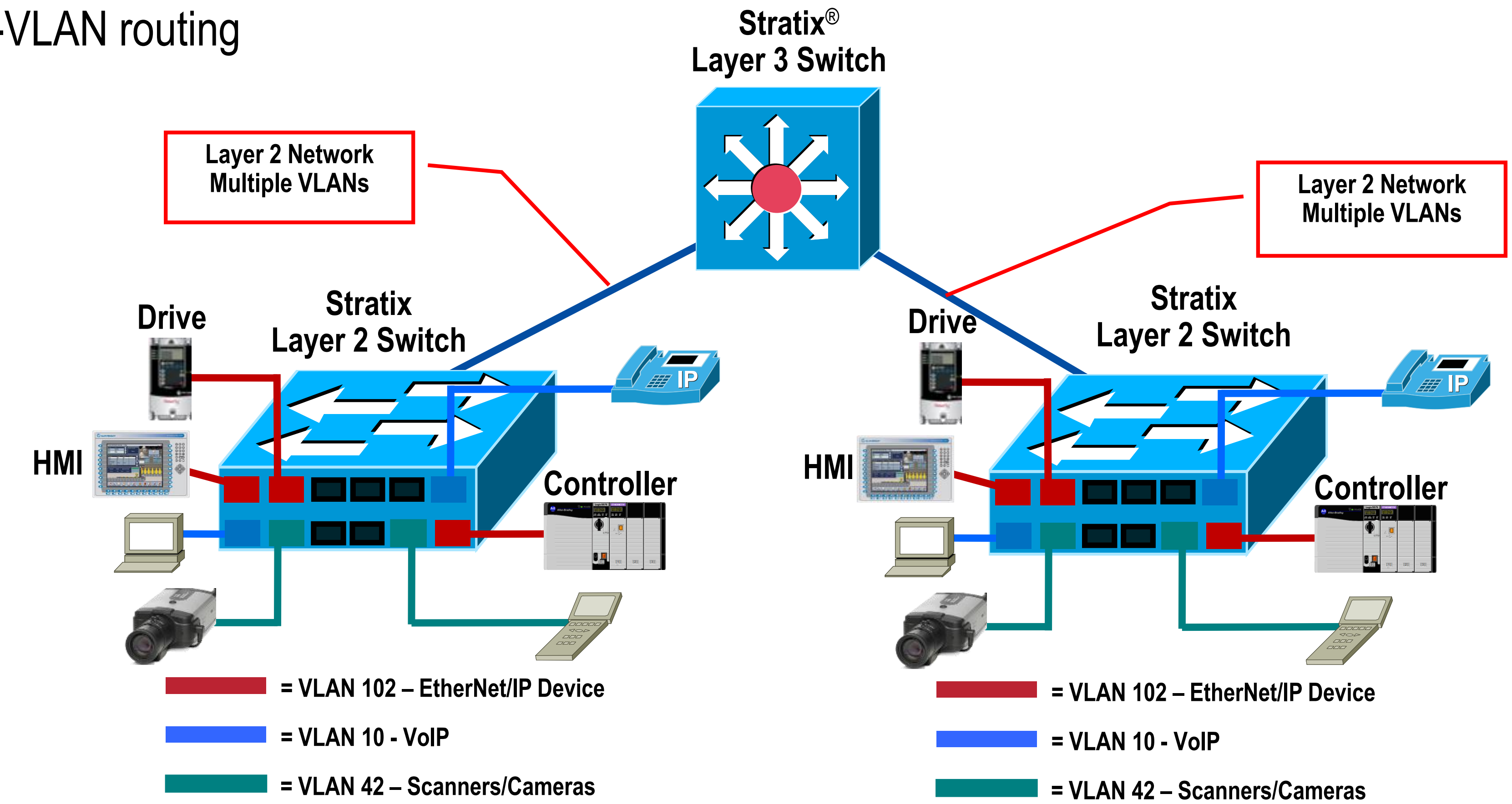


- VLAN Trunking Protocol (VTP)
  - Provides centralized VLAN management, runs only on trunks
  - Three modes:
    - Server: updates clients and servers
    - Client: receive updates - cannot make changes
    - Transparent: allow updates to pass through
- Use VTP transparent mode to decrease potential for operational error
  - Define VLANs at each switch, no centralized management

Switch Hierarchy, Virtual LANs (VLANs)

Segmentation – Network Services

- Multi-Layer Switch
  - Layer 2 VLAN Trunking
  - Layer 3 Inter-VLAN routing



Design and Implementation Considerations

Segmentation – Network Services

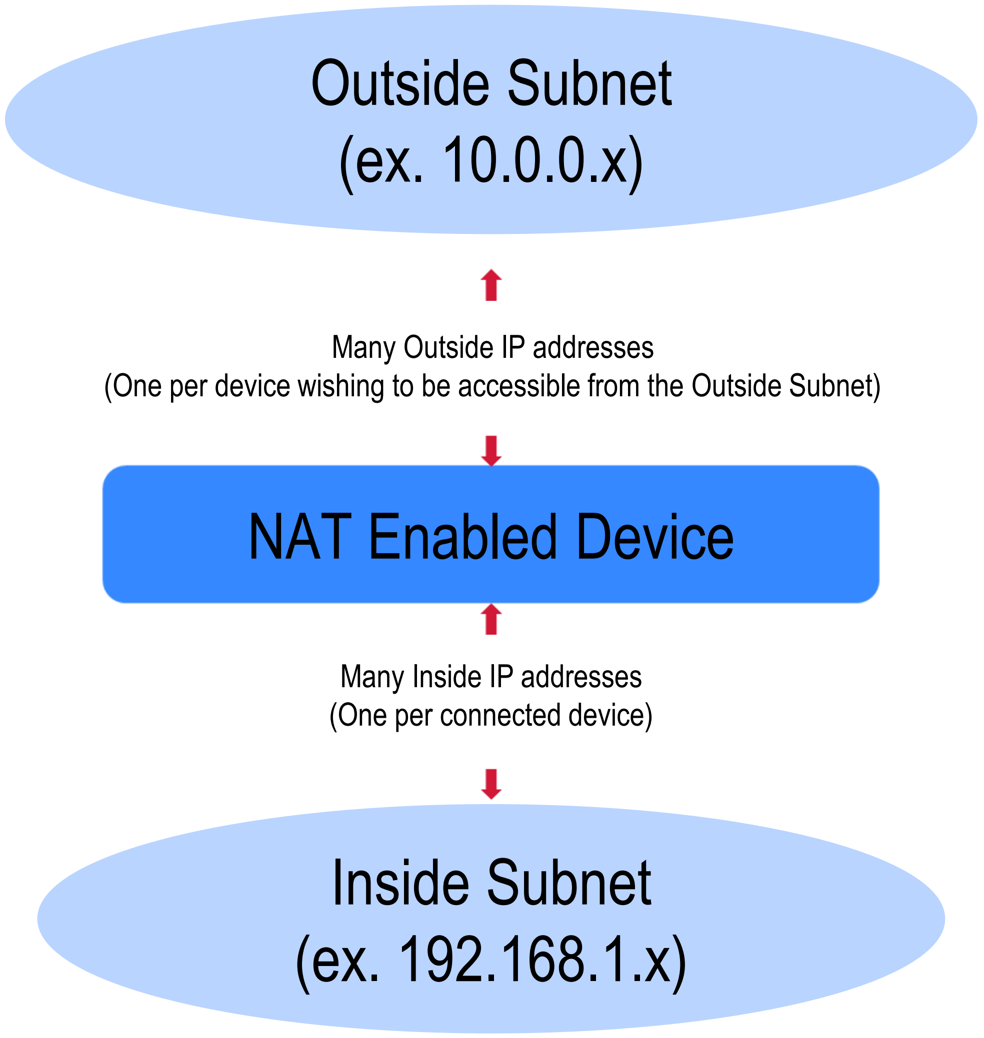
VLANs

- Segment different traffic types into separate VLANs (Control & Information, VoIP, HTTP)
- Create smaller IP Subnet (/24 prefix) per VLAN
- Within the Cell/Area Zone
  - Use Layer 2 VLAN trunking between switches with similar traffic types
  - When trunking, use 802.1Q, VTP in transparent mode
- Use Layer 3 Inter-VLAN routing/switching
  - Between VLANs within the same Cell/Area zone
  - Between zones
- Assign different traffic types to a unique VLAN, other than VLAN 1

IP Subnets - Network Address Translation (NAT)

Segmentation – Network Services

- Network Address Translation is a service which can translate a packet from one IP address to another IP address
- Can be a Layer 2 or Layer 3 device
- Has two forms:
  - One to One (1:1) – Allows for the assignment of a unique outside IP address to a specific inside IP address
  - One to Many (1:n) – a.k.a. TCP/UDP Port Address Translation (PAT). Allows Multiple devices to share one "Outside" address

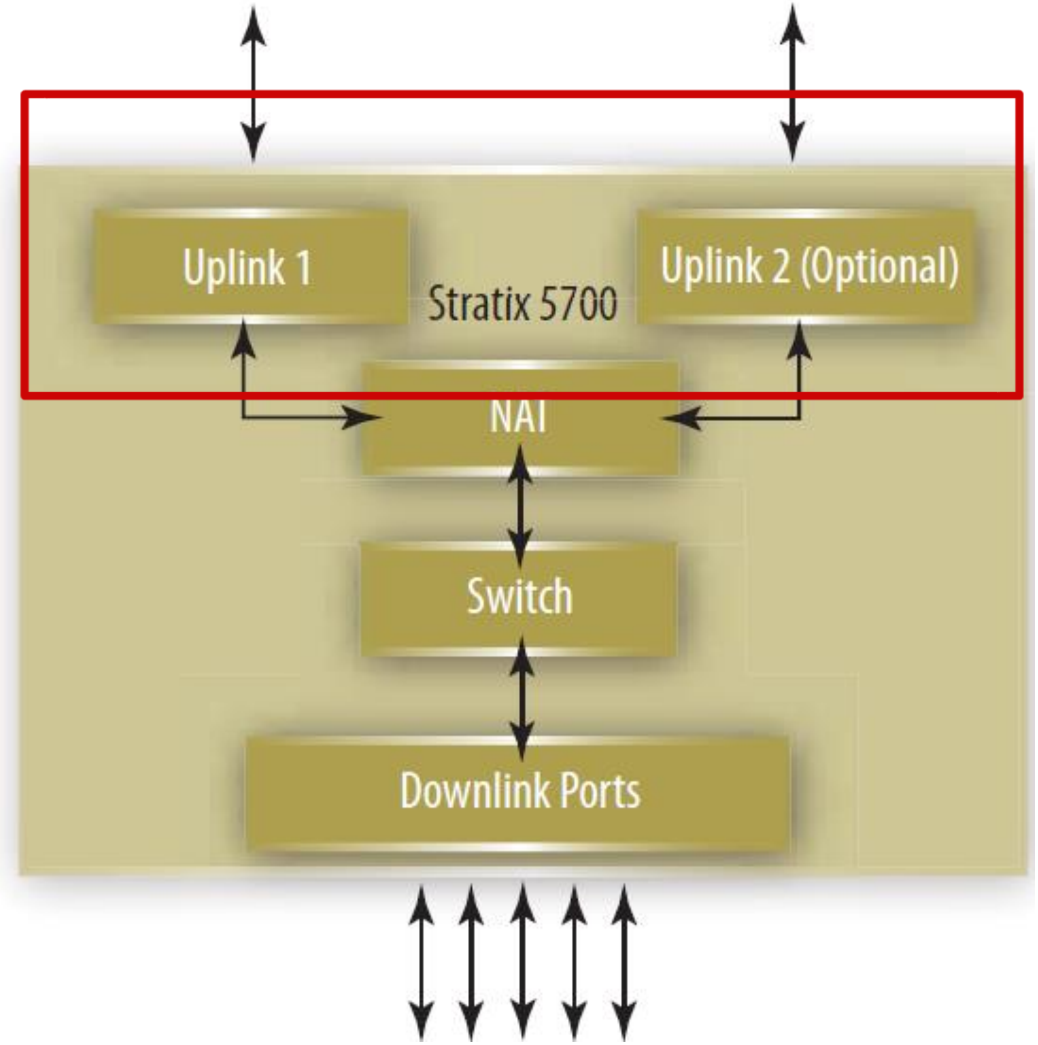


Network Address Translation (NAT) - Layer 3 Address Segmentation

Segmentation – Network Services

IPv4 Header

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			Padding



Why use Network Address Translation (NAT) ?

Segmentation – Network Services

Allows a single device to act as an agent between the Plant (Outside) network and the Equipment/Skid/Machine (Inside) network.

- Helps simplify integration of IP address mapping from a equipment/skid/machine level IP addresses to the plant network.
- Allows OEMs to develop standard equipment/skids/machines and eliminate the need for unique IP addressing and code modifications.
- Allows End Users to more easily integrate equipment/skids/machines into their larger plant network without extensive coordination with OEMs.
- Provides better maintainability at the equipment/skids/machines as they remain standard.
- Allows for reuse of IP addresses allowing for more connected devices in a limited address pool.

Layer 3 vs Layer 2 NAT Devices

Segmentation – Network Services

Layer 2 NAT Device Key Points

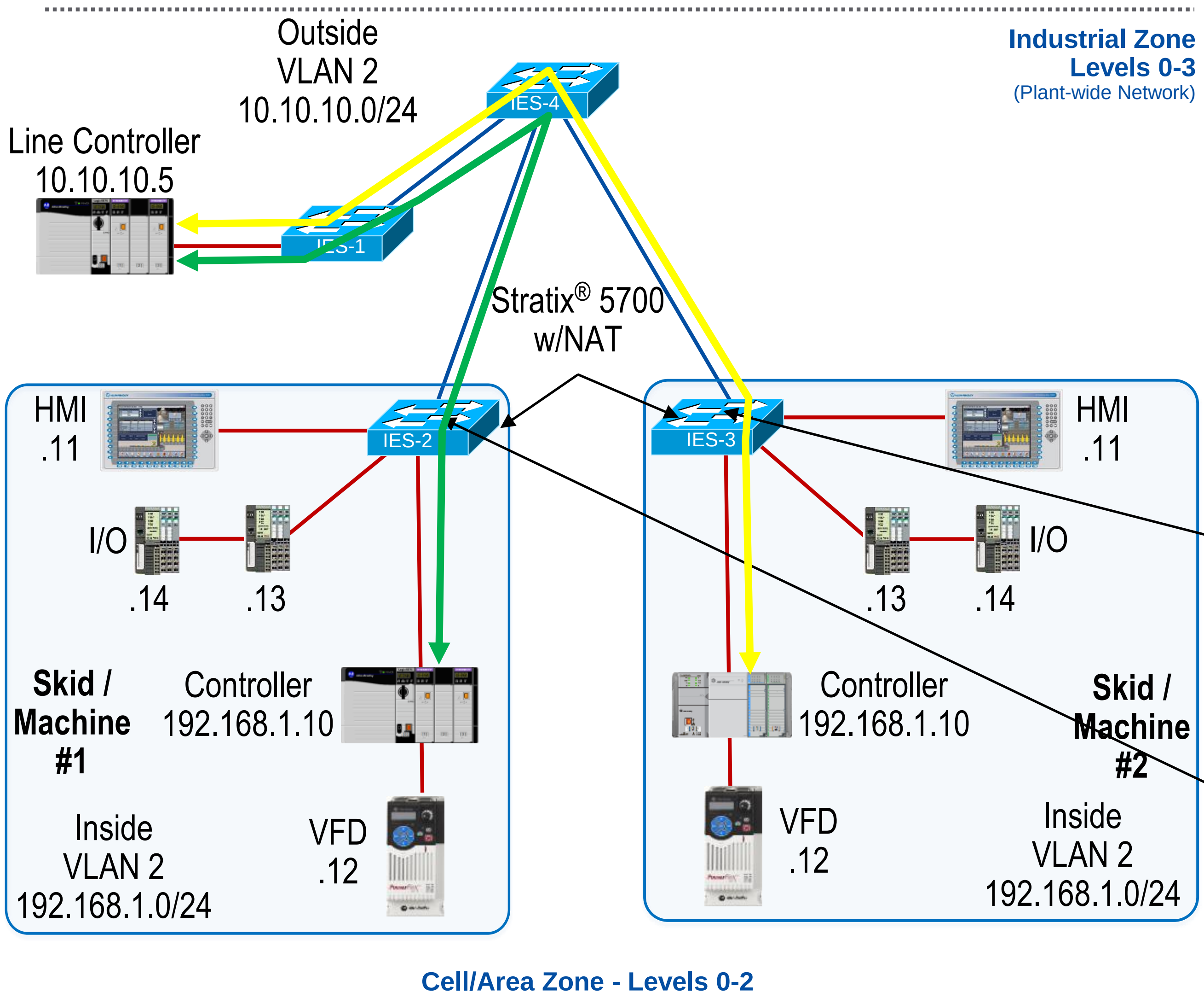
- Hardware based implementation, performance is at wire speed throughout switch loading
- NAT device does not act as a router and utilizes 2 translations tables – inside to outside & outside to inside
  - Supports multiple VLANs through NAT boundary enhancing segmentation flexibility (communication between VLANS requires a separate layer 3 device)
- Broadcast traffic in a VLAN can propagate through the NAT boundary
- Untranslated traffic, including multicast, can be permitted through the NAT boundary

Layer 3 NAT Device Key Points

- Typically a software implementation, performance of translation directly tied to the loading of the NAT CPU
- NAT device acts as the default gateway (router) for the devices on the inside network
  - NAT device will intercept traffic, perform translation, and route traffic
- Broadcast traffic is stopped at the NAT boundary
- Untranslated traffic is not permitted through the NAT device

Network Address Translation (NAT)

Segmentation – Network Services



- Multiple Skids/Machines
  - Each Skid/Machine Aggregated by One Stratix® 5700 Layer 2 NAT Switch
  - Single VLAN Architecture

IES-3 Stratix 5700 w/ NAT

Inside to Outside NAT Table	Inside	Outside
	192.168.1.10	10.10.10.20
Outside to inside NAT Table	Outside	Inside
	10.10.10.5	192.168.1.5

IES-2 Stratix 5700 w/ NAT

Inside to Outside NAT Table	Inside	Outside
	192.168.1.10	10.10.10.10
Outside to inside NAT Table	Outside	Inside
	10.10.10.5	192.168.1.5

Network Address Translation (NAT) Limitations

Segmentation – Network Services

These applications are not supported, which is typical for all NAT devices:

- Traffic encryption and integrity checking protocols generally incompatible with NAT (for example, IPsec transport mode)
- Applications that use dynamic session initiations, such as NetMeeting
- File Transfer Protocol (FTP)
- Microsoft® Distributed Component Object Model (DCOM), which is used in Open Platform Communication (OPC)
- Multicast I/O and Multicast Produced Consumed traffic
- IEEE 1588 PTP unless the NAT-enabled switch is in boundary mode

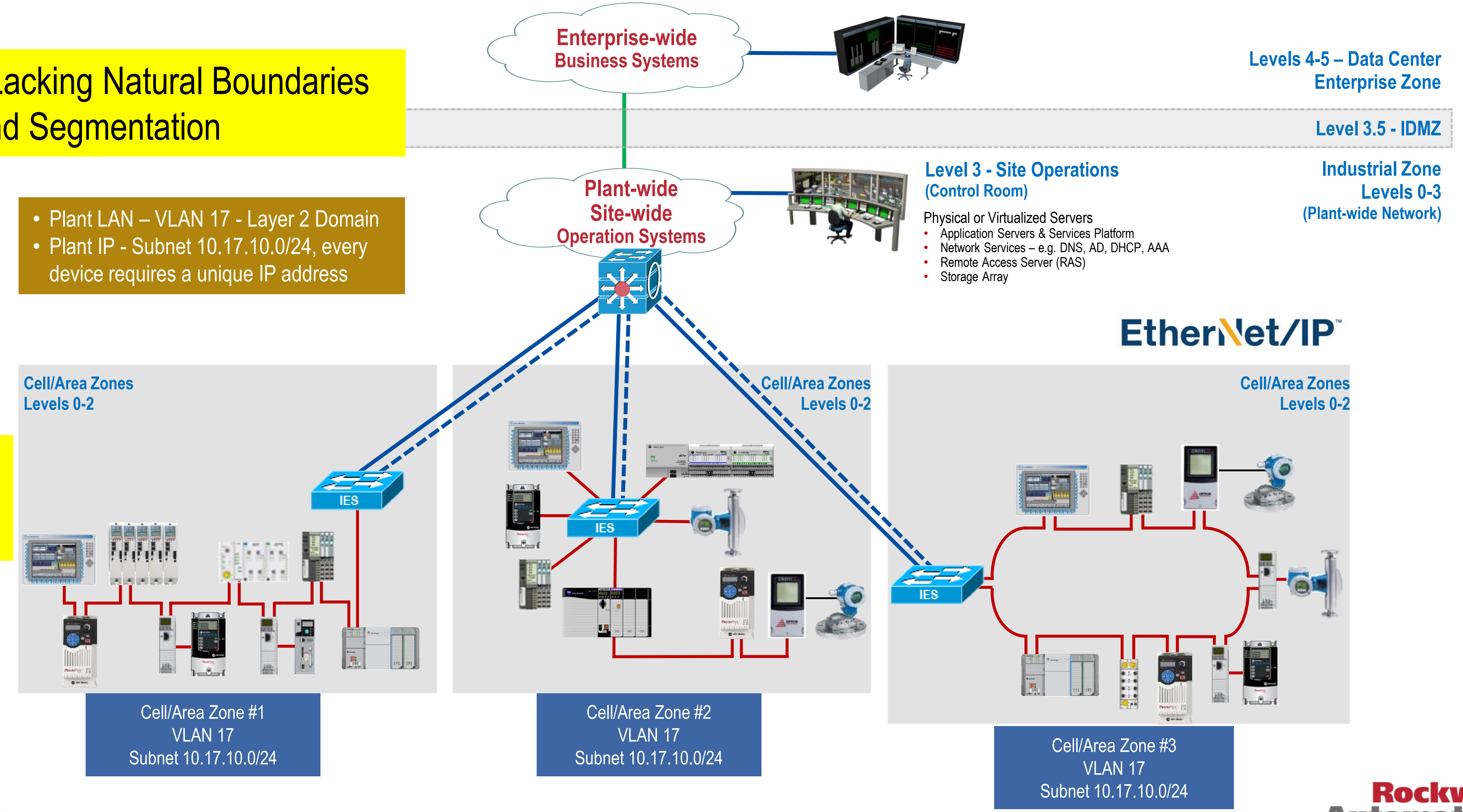
No Segmentation (not recommended)

Segmentation – Network Services

Large LAN, Lacking Natural Boundaries and Segmentation

- Plant LAN – VLAN 17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24, every device requires a unique IP address

- Same Layer 2 Broadcast Domain
- Same IP Address Space



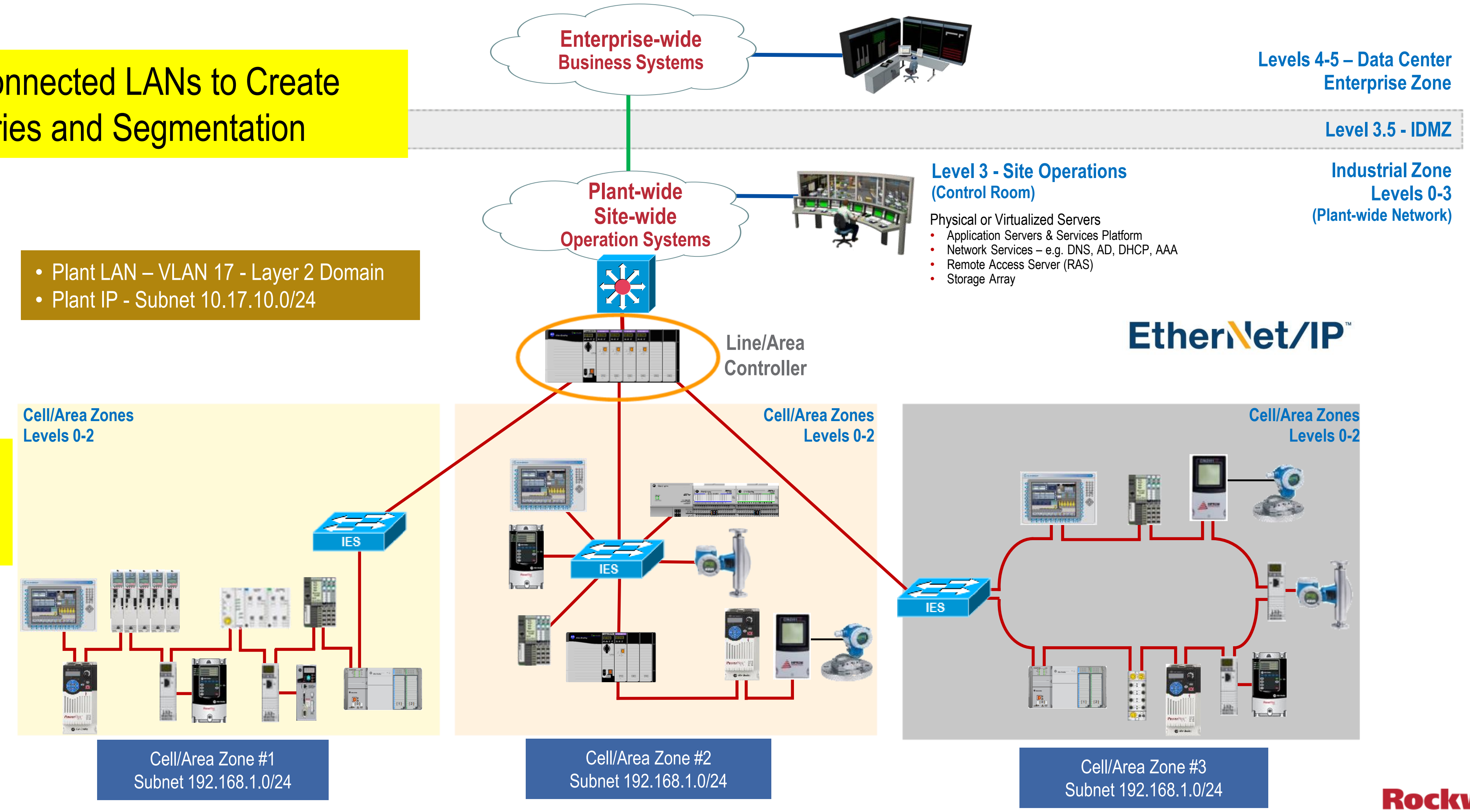
Multiple Network Interface Cards (NICs) - CIP Bridge Segmentation

Segmentation – Network Services

Smaller Connected LANs to Create Boundaries and Segmentation

- Plant LAN – VLAN 17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

- Unique Layer 2 Broadcast Domains
- Reused IP Address Space



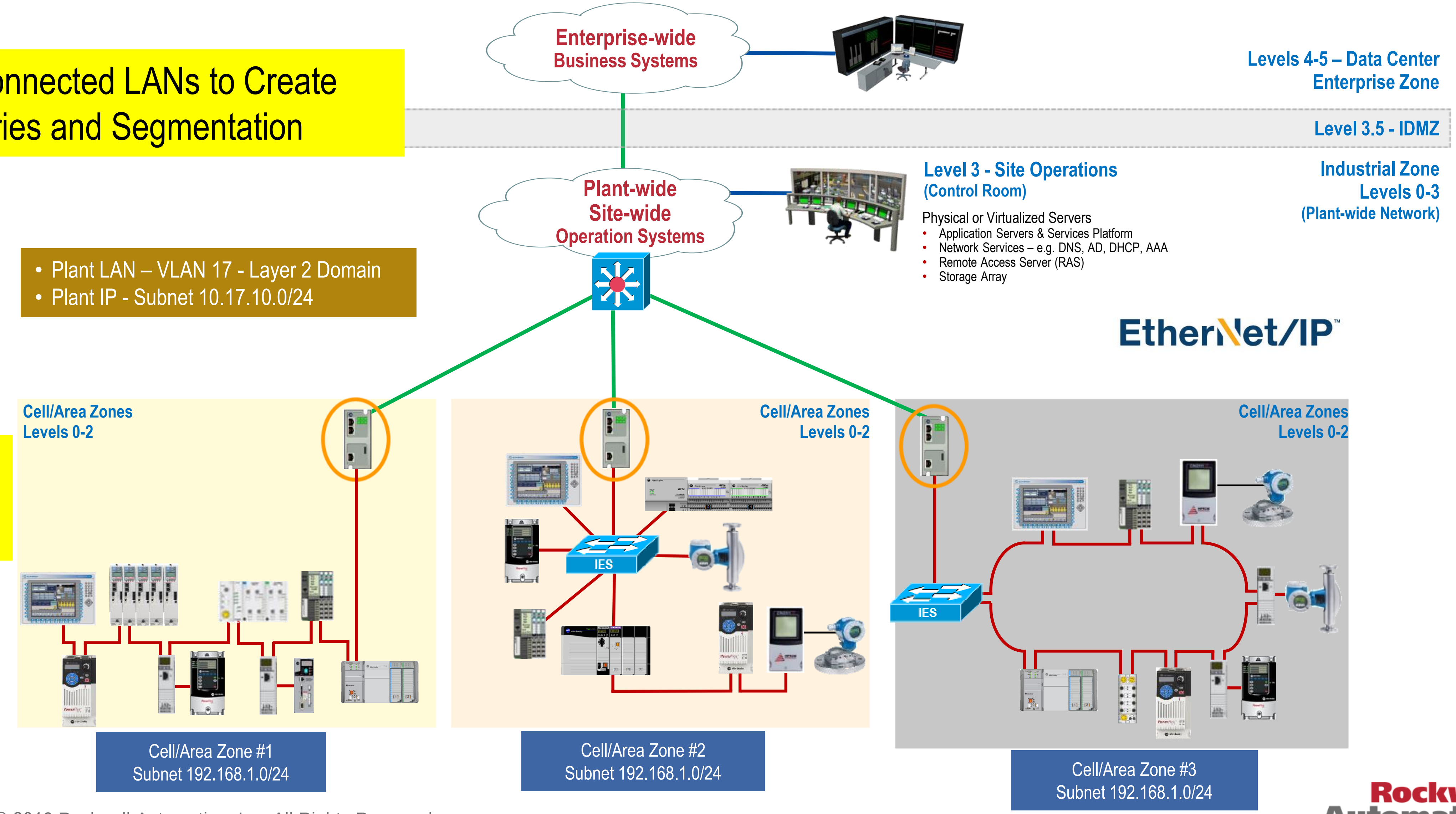
Layer 3 NAT Appliance Segmentation

Segmentation – Network Services

Smaller Connected LANs to Create Boundaries and Segmentation

- Plant LAN – VLAN 17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

- Unique Layer 2 Broadcast Domains
- Reused IP Address Space

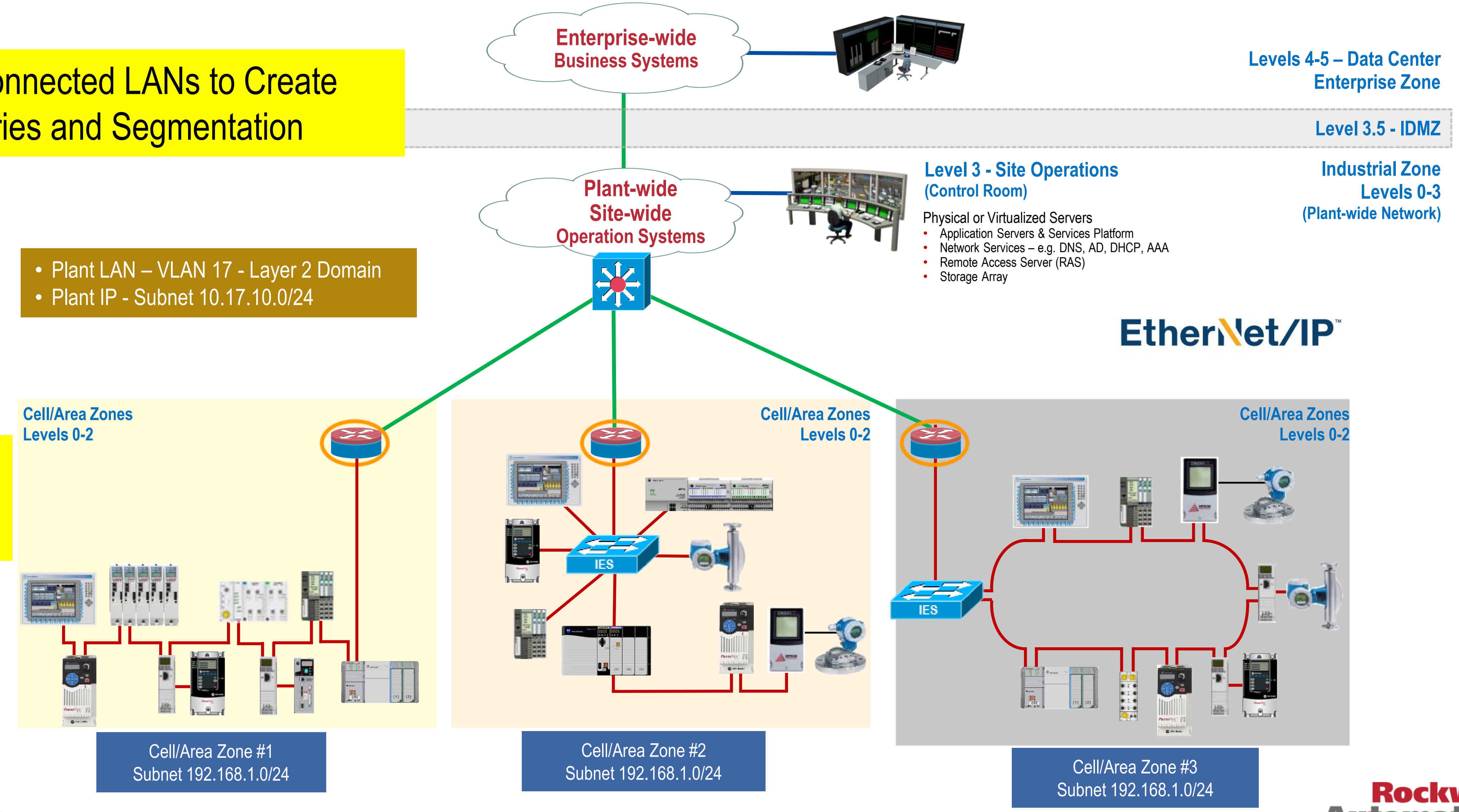


Layer 3 NAT - Integrated Services Router Segmentation

Segmentation – Network Services

Smaller Connected LANs to Create Boundaries and Segmentation

- Unique Layer 2 Broadcast Domains
- Reused IP Address Space



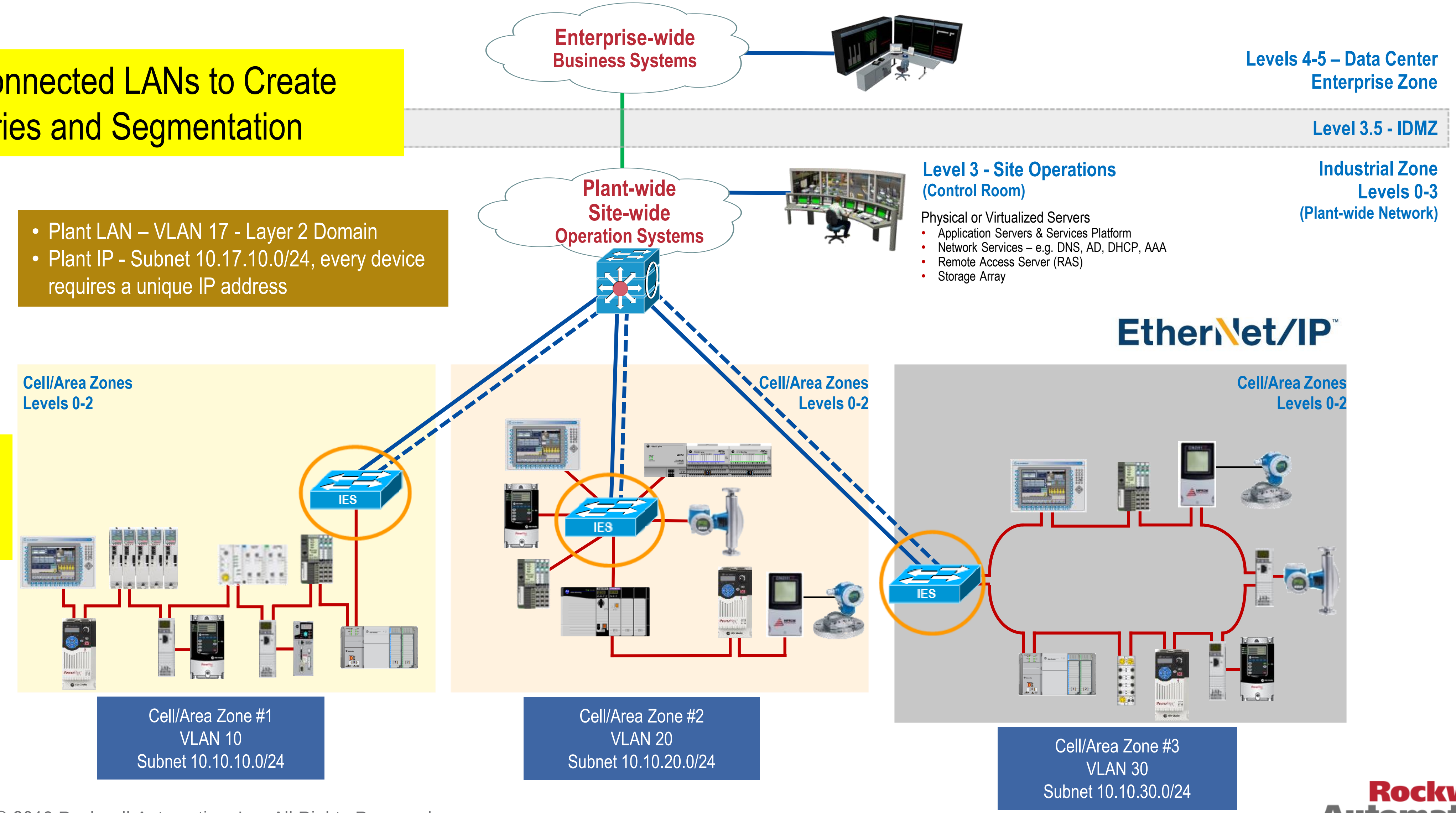
Rockwell Automation

VLAN Segmentation without NAT

Segmentation – Network Services

Smaller Connected LANs to Create Boundaries and Segmentation

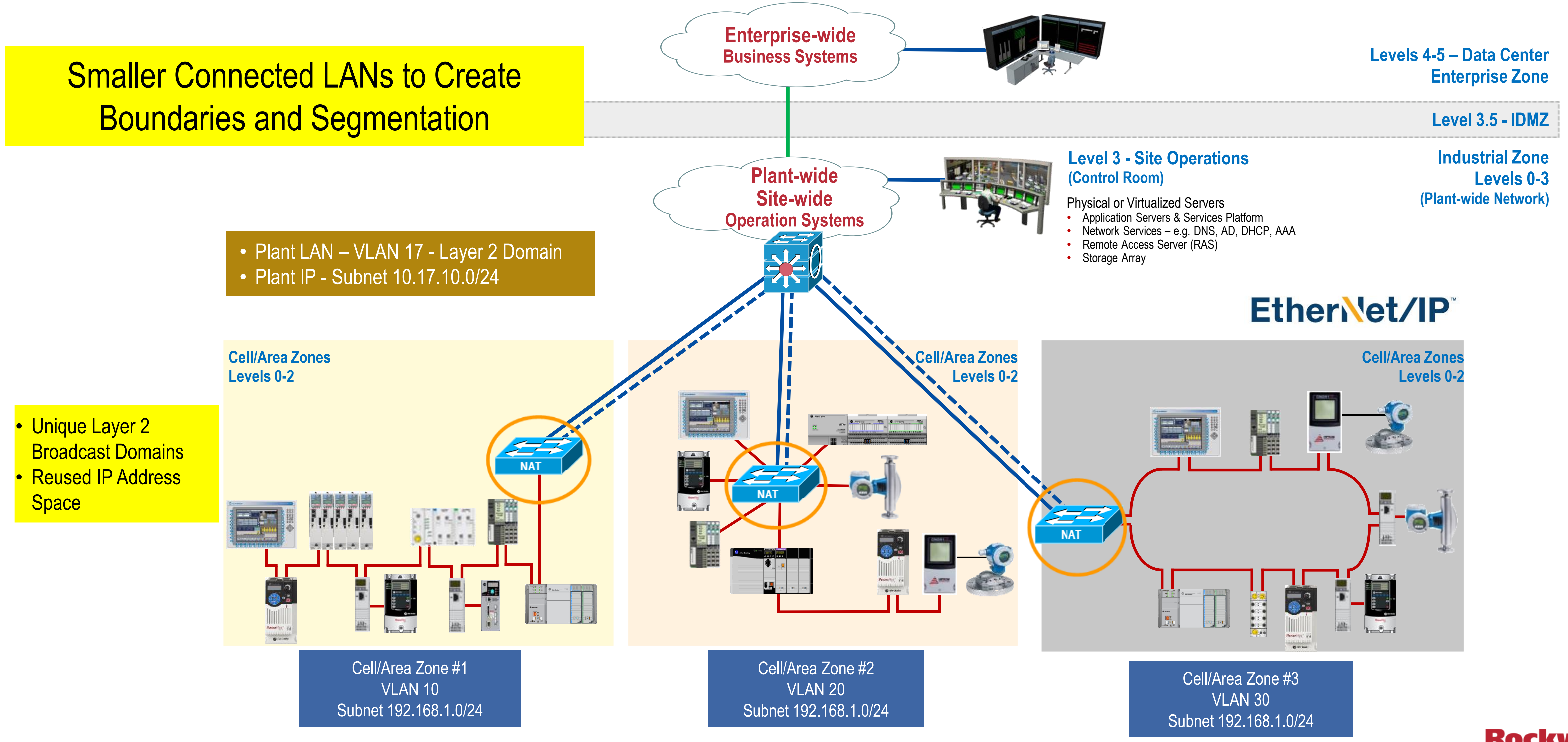
- Unique Layer 2 Broadcast Domains
- Unique IP Address Space



Rockwell Automation

VLAN Segmentation with Layer 2 NAT

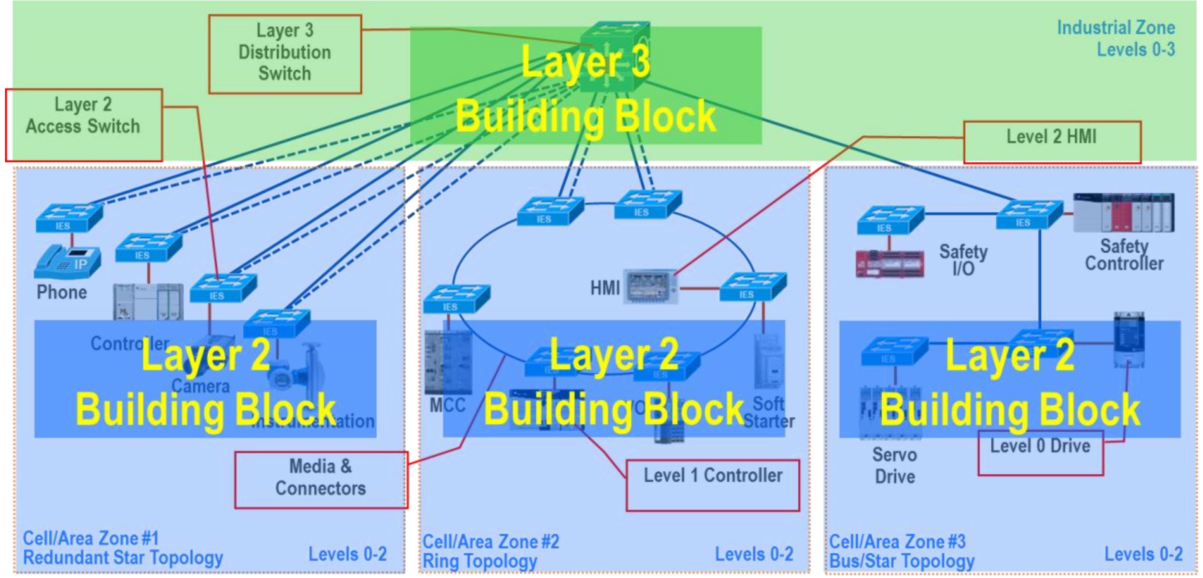
Segmentation – Network Services



Design and Implementation Considerations

Segmentation – Network Services

- Design smaller modular building blocks to help create functional / security zones
  - Minimize network sprawl
  - Build scalable, robust and future-ready network infrastructure
  - Smaller Connected LANs
    - Smaller fault domains (e.g. Layer 2 loops)
    - Smaller broadcast domains
    - Smaller domains of trust (security)
  - Segment Industrial IoT Technologies
- Multiple techniques to create smaller network building blocks (Layer 2 domains)
  - Logical zoning, Multiple NICs
  - Campus network model - multi-tier switch hierarchy – Layer 2 and Layer 3
  - Virtual Local Area Networks (VLANs), Network Address Translation (NAT)
  - Firewalls



Rockwell Automation

Key Tenet

Managed Infrastructure

Industrial Ethernet Switch Type Selection

Managed Infrastructure

	Advantages	Disadvantages
Managed Switches	▪ Loop prevention and resiliency ▪ Security services ▪ Management services (Multicast, DHCP per port and DLR) ▪ Diagnostic information ▪ Segmentation services (VLANs) ▪ Prioritization services (QoS)	▪ More expensive ▪ Requires some level of support and configuration to start up
Unmanaged Switches	▪ Inexpensive ▪ Simple to set up	▪ No loop prevention or resiliency ▪ No security services ▪ No diagnostic information ▪ No segmentation or prioritization services ▪ Difficult to troubleshoot, no management services
ODVA Embedded Switch Technology	▪ Cable simplification with reduced cost ▪ Ring loop prevention and resiliency ▪ Prioritization services (QoS) ▪ Time Sync Services (IEEE 1588 PTP Transparent Clock) ▪ Diagnostic information	▪ Limited management capabilities ▪ May require minimal configuration

Managed Infrastructure Selection

Managed Infrastructure

Managed Switches

- Access switching or distribution routing
- Diagnostic information
- Network Address Translation (NAT)
- Segmentation / VLAN capabilities
- Prioritization services (QoS)
- Network resiliency

Security Appliances

- Secure real-time control communication
- Routing and firewall capabilities
- Intrusion protection
- Access control lists

- Manageability by OT and IT tools
  - Topologies - Switch-level and device-level
  - Switching – network services
  - Routing – connected, static, dynamic
  - Wireless Access Points - Autonomous and Unified Architectures
  - Security Appliances - Industrial firewalls with inspection profiles for EtherNet/IP – deep packet inspection (DPI)

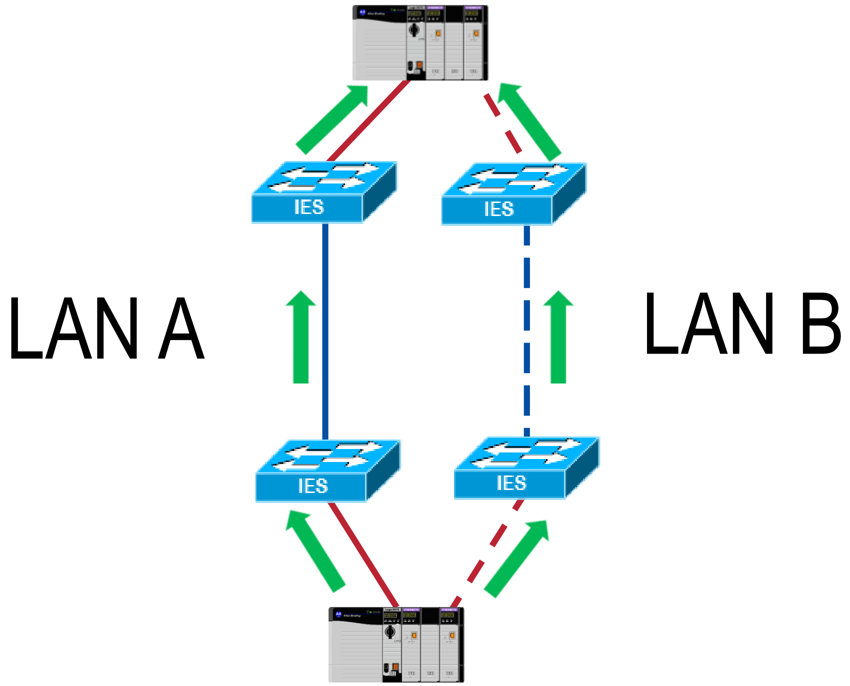
Key Tenet

Resiliency

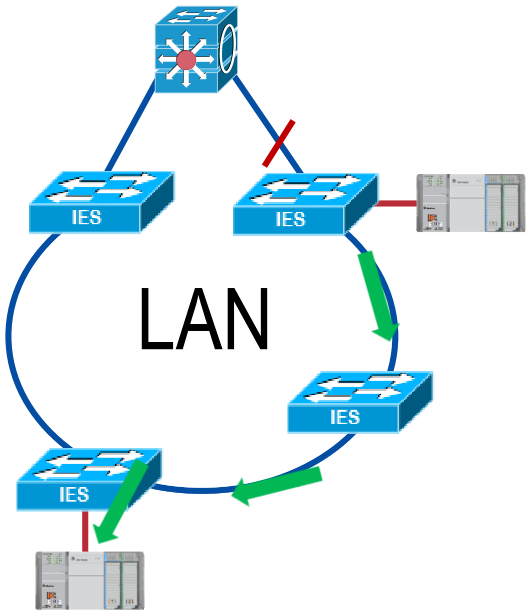
Networking Design Considerations

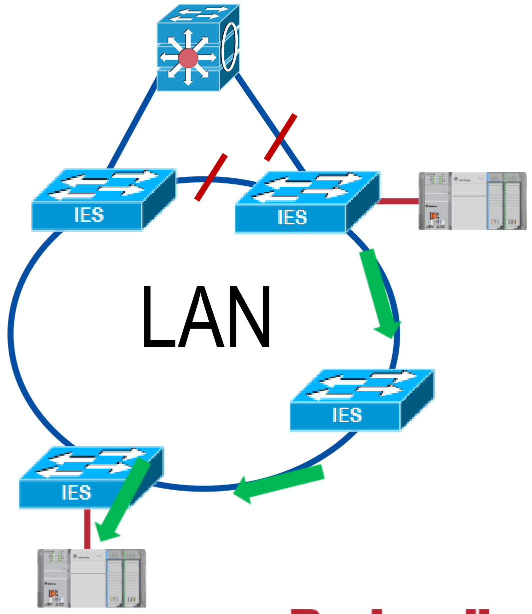
Resiliency

- Redundant Ethernet Networks
  - Independent LANs
  - Independent Paths



- Resilient Path Ethernet Network
  - Common LAN
  - Redundant Paths
  - Resiliency Protocol

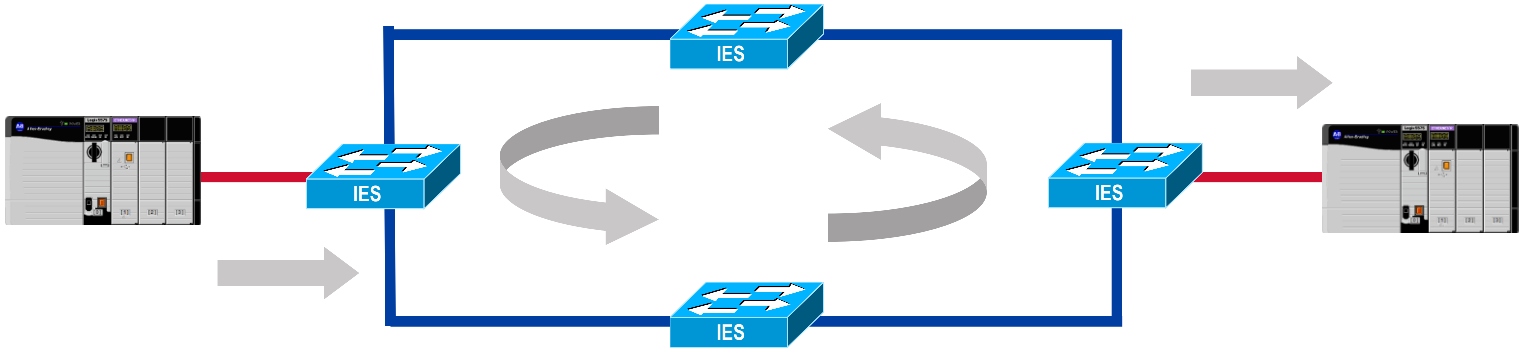




Rockwell Automation

Layer 2 – Loop Avoidance

Resiliency



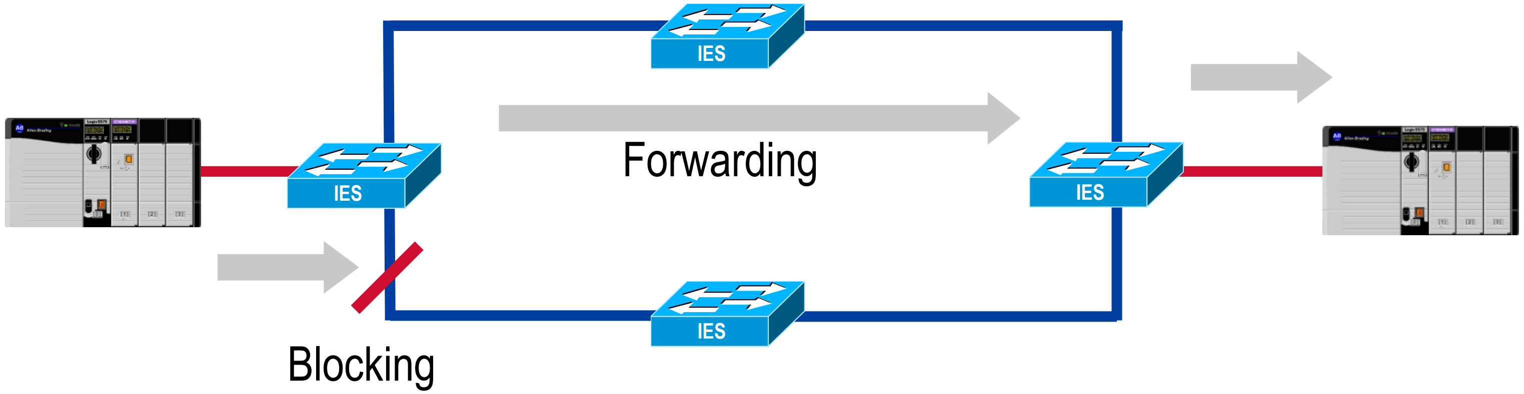
- Redundant paths create a switching (bridging) loop
  - Without proper configuration, a loop will lead to a broadcast storm, flooding the network, which will consume available bandwidth, and take down a Layer 2 switched (bridged) network
    - Layer 2 Ethernet frames do not have a time-to-live (TTL)
    - A Layer 2 frame can loop forever

Pre	SFD	DA	SA	Type/Len	Data (Payload)	FCS

Ethernet Frame

Layer 2 – Loop Avoidance

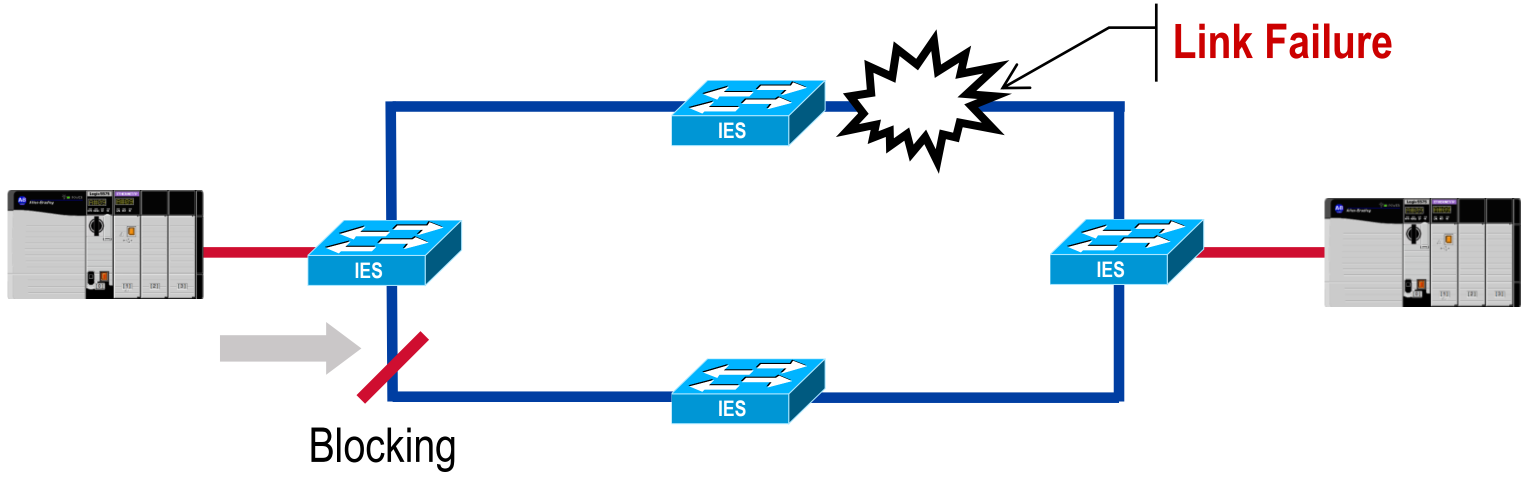
Resiliency



- A Layer 2 resiliency protocol maintains redundant paths while avoiding switching (bridging) loop

Layer 2 – Loop Avoidance

Resiliency



- Network convergence (healing, recovery, etc.) must occur before the Industrial Automation and Control System (IACS) application is impacted

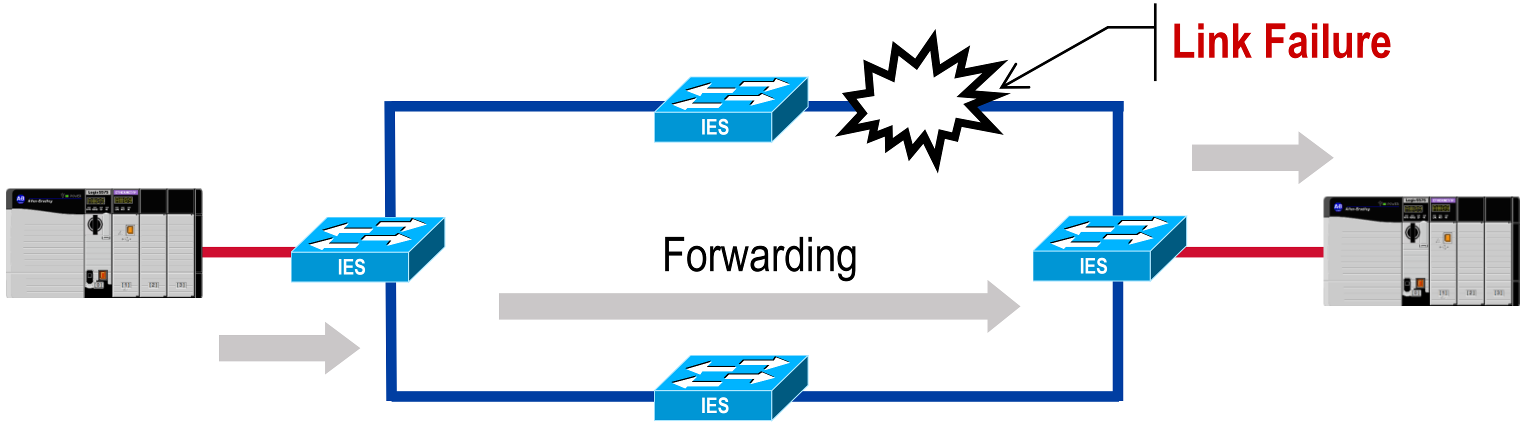
Network Convergence

Resiliency

- Network convergence (healing, recovery, etc.) time – is a measure of how long it takes to detect a fault, find an alternate path, then start forwarding network traffic across that alternate path.
  - MAC tables must be relearned
  - Multicast on uplinks must be relearned
- During the network convergence time, some portion of the traffic is dropped by the network because interconnectivity does not exist.
- If the convergence time is longer than the Logix controller connection timeout, the IACS devices on the affected portion of the network may stop operating and may affect the IACS application.

Layer 2 – Loop Avoidance

Resiliency

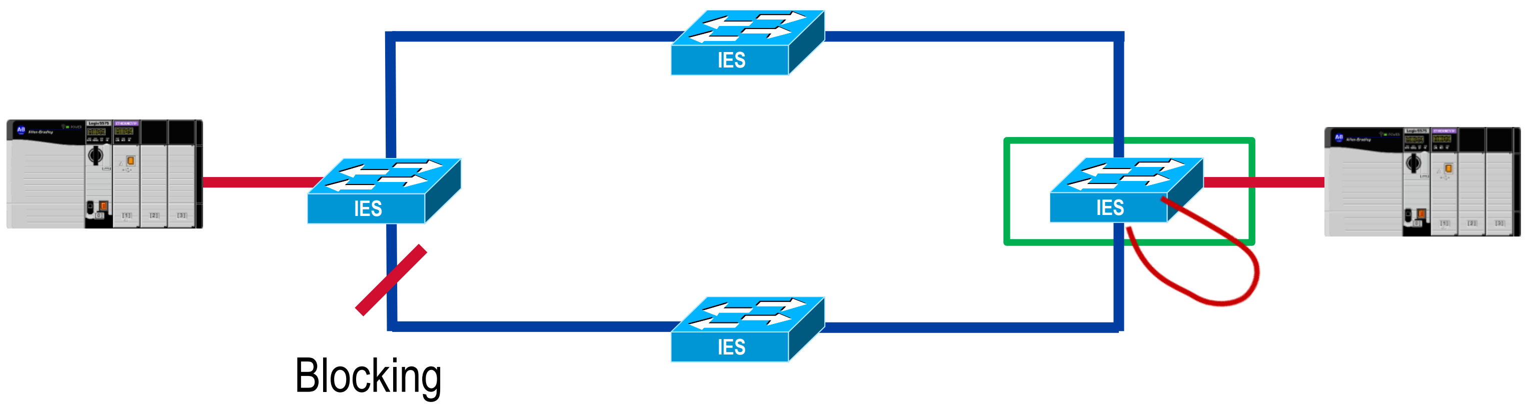


- Network convergence must occur quickly enough to avoid a IACS connection timeout:
  - Message (MSG) instruction
    - Instruction timeout - 30 second default
  - I/O and Producer/Consumer
    - Connection timeout - 4 x RPI, with a minimum of 100 ms
  - Safety I/O
    - Connection timeout - 4 x RPI by default

Layer 2 – Loop Avoidance

Resiliency

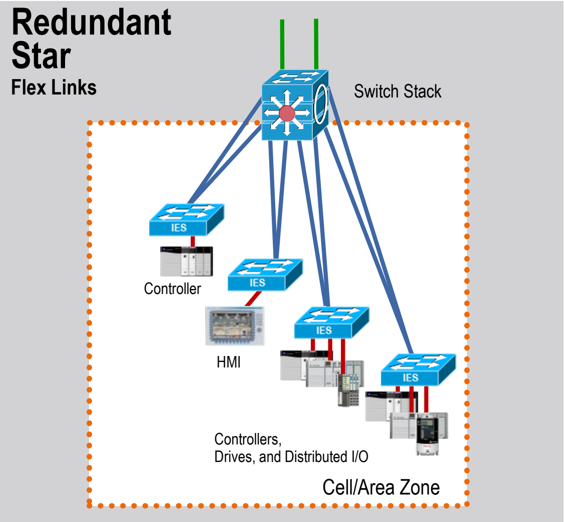
- Don’t forget about potential loops on the switch itself

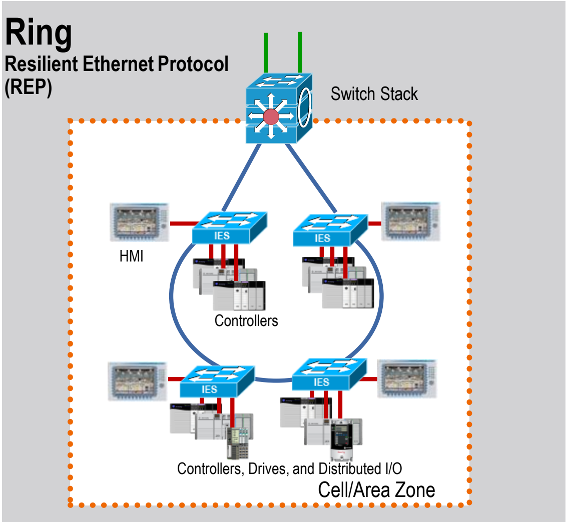


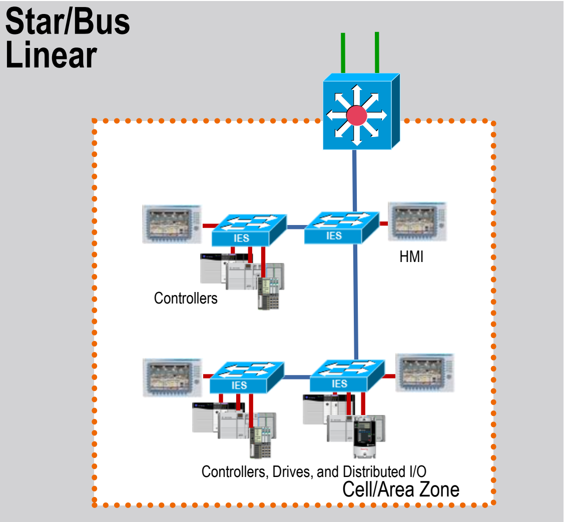
Redundant Path Topologies with Resiliency Protocols

Resiliency

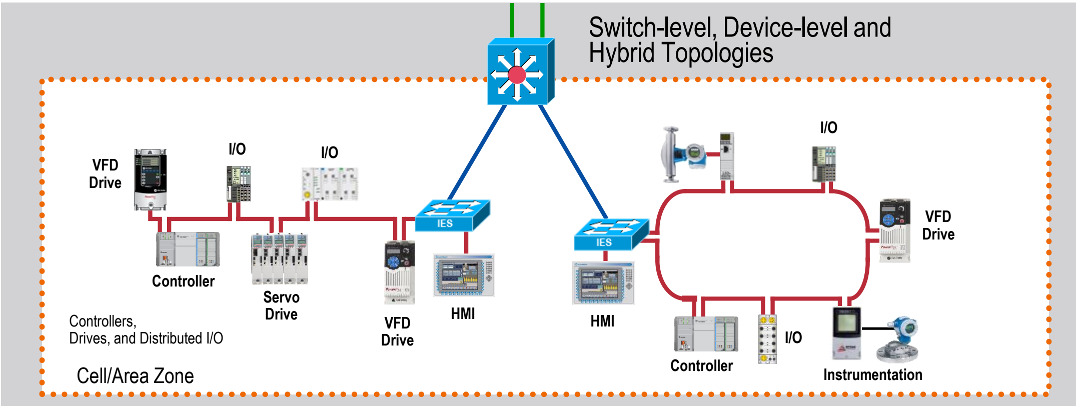
Switch-level Topologies







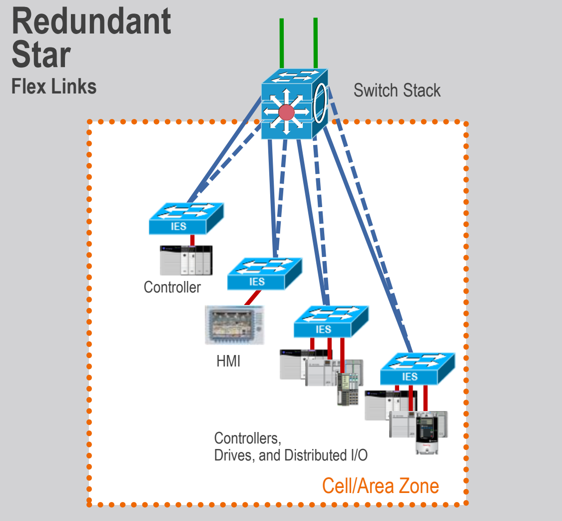
Device-level Topologies

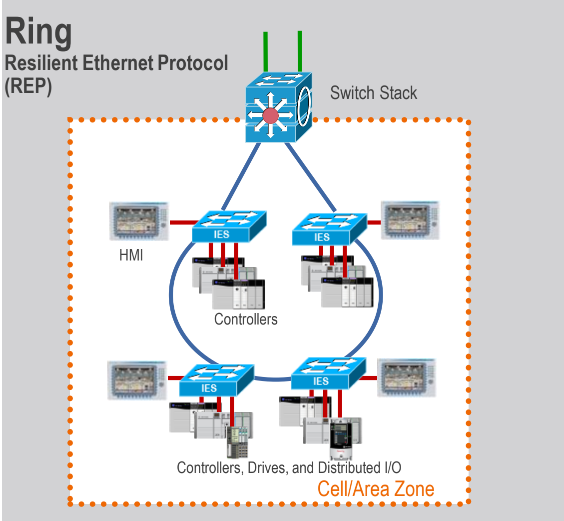


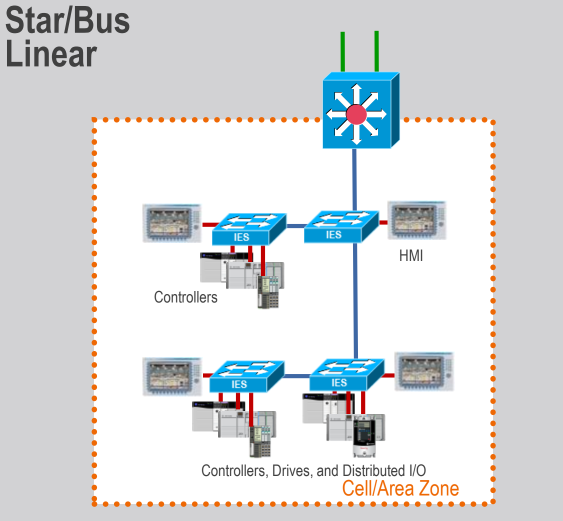
Rockwell Automation

Networking Design Considerations - Topology Choice

Resiliency







	Redundant Star	Ring	Linear
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	**Best**	**OK**	**Worst**

Networking Design Considerations – Topology / Technology Choice

Resiliency

Resiliency Protocol	Mixed Vendor	Ring	Redundant Star	Network Convergence > 250 ms	Network Convergence 60 - 100 ms	Network Convergence 1 - 3 ms	Layer 3	Layer 2
STP (802.1D)	X	X	X					X
RSTP (802.1w)	X	X	X	X				X
MSTP (802.1s)	X	X	X	X				X
rPVST+		X	X	X				X
REP		X			X			X
EtherChannel (LACP 802.3ad)	X		X		X			X
Flex Links			X		X			X
DLR (IEC & ODVA)	X	X				X		
StackWise		X	X			X	X	X
HSRP		X	X	X			X	
GLBP		X	X	X			X	
VRRP (IETF RFC 3768)	X	X	X	X			X	

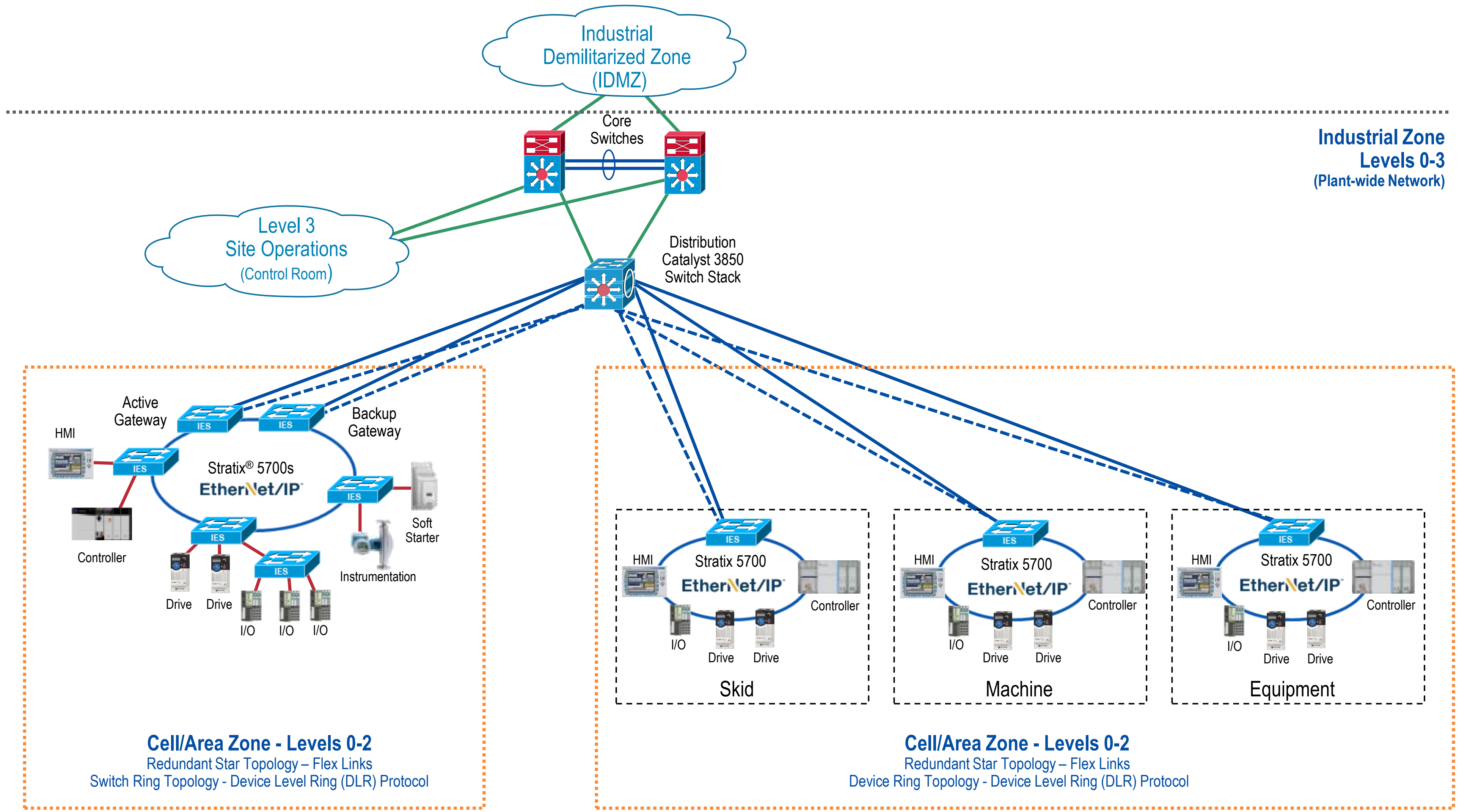
Process and Information

Time Critical

Loss Critical

Networking Design Considerations – Topology / Technology Choice

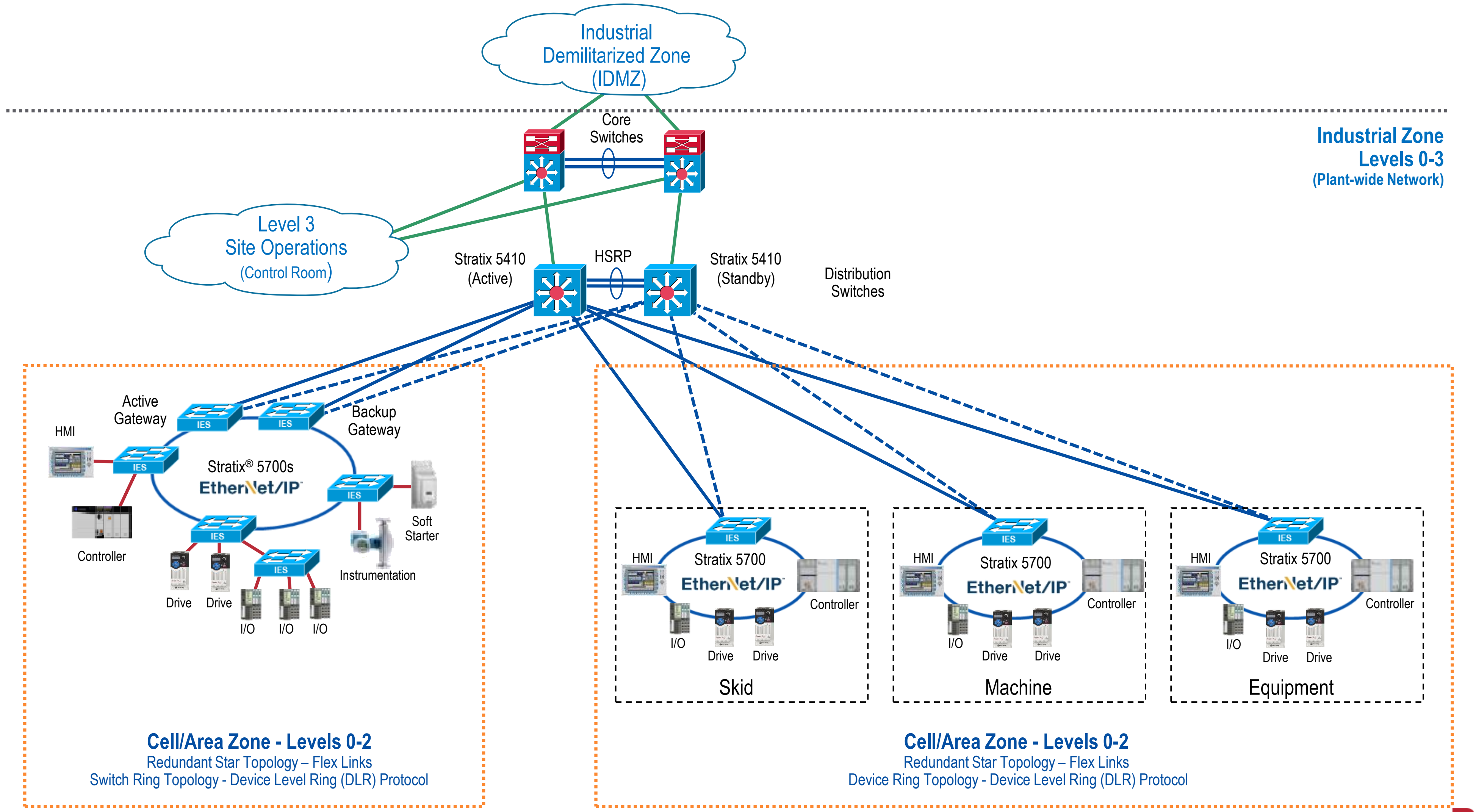
Resiliency



Rockwell Automation

Networking Design Considerations – Topology / Technology Choice

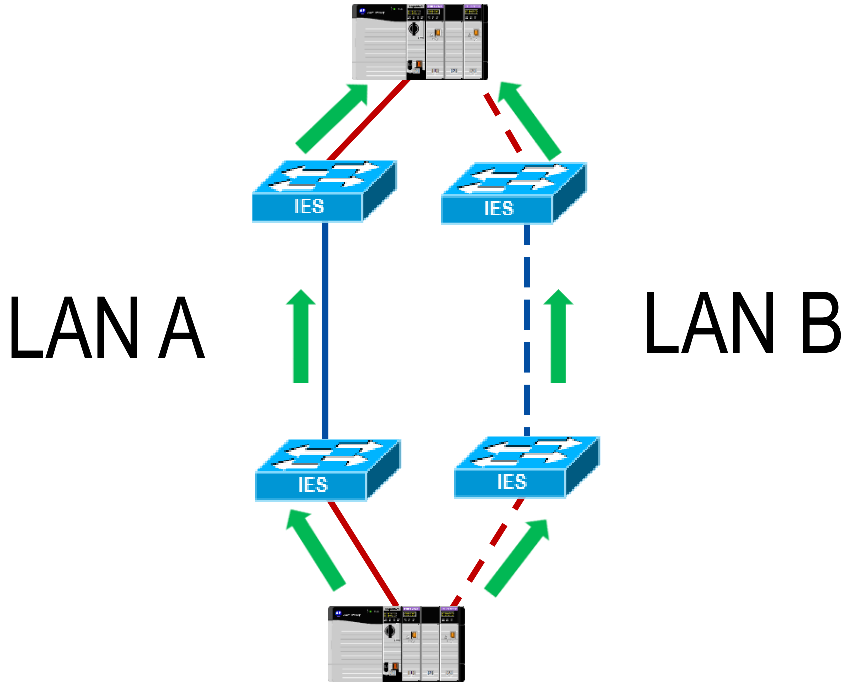
Resiliency



Parallel Redundancy Protocol

Resiliency

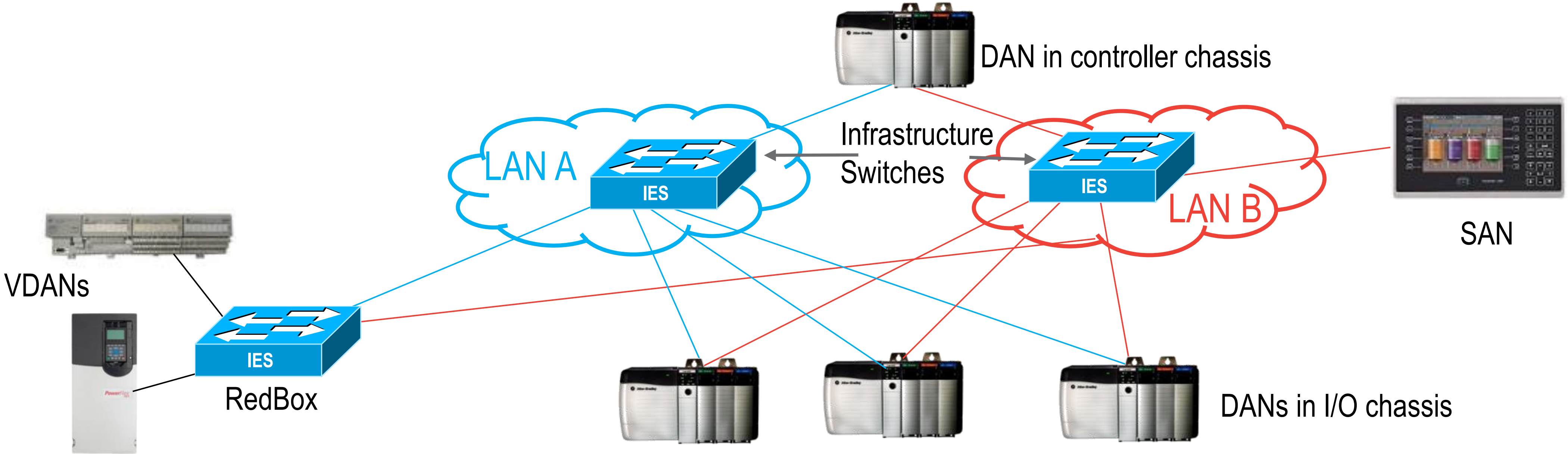
- What is PRP?
  - PRP, Parallel Redundancy Protocol, IEC standard 62439-3
  - Fault tolerant, fully redundant Ethernet infrastructure
  - Same frame is sent (replicated) on both LANs
  - Zero network healing time for a single fault
- What are some typical applications for PRP?
  - Where redundant network infrastructure, independent LANs, independent Paths, are desired
  - Process applications – heavy industries



PRP General

Resiliency

- DAN, Dually Attached Node, has PRP protocol built in and attaches to both LANs
  - One IP address, one MAC ID
- SAN, Singly Attached Node, is a node that does not have PRP built, attaches to one LAN
- RedBox: connects non-PRP devices to the PRP networks
- VDANs: non-PRP devices connected to both LANs through a RedBox
- Standard switch – must support the baby jumbo frame size of 1506 bytes



Design and Implementation Considerations

Resiliency

- Choice is Application Dependent
  - Switch-level vs. Device-level topologies
  - Ring vs. Redundant Star Topology
  - Mixed switch vendor environment - Legacy Migration
  - Geographic dispersion of IACS devices
  - Location within the hierarchal architecture - Layer 2 vs. Layer 3
  - Performance
    - Tolerance to: Network Convergence time, Packet loss, Latency & Jitter
- Redundant Path Topologies Require a Resiliency Protocol
  - Switch-level Topologies - Redundant Star, Ring
  - Device-level Topology - Ring
- Use fiber media and SFPs for all inter-switch links – ring and redundant star switch-level topologies

Design and Implement a Robust Physical Layer

Resiliency

- Environment Classification - MICE
- More than cable
  - Connectors
  - Patch panels
  - Cable management
  - Noise mitigation
    - Bonding, Shielding and Grounding
- Standard Physical Media
  - Wired vs. Wireless
  - Copper vs. Fiber
  - UTP vs. STP
  - Single-mode vs. Multi-mode
  - SFP – LC vs. SC
- Standard Topology Choices
  - Switch-Level, Device-Level and Hybrid

1585 Media

Rockwell Automation Encompass™ Product Partner

3 - Copper Media
2 - Fiber Media
1 - Fiber Solutions

Cable Selection
ENET-WP007

PANDUIT

Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide

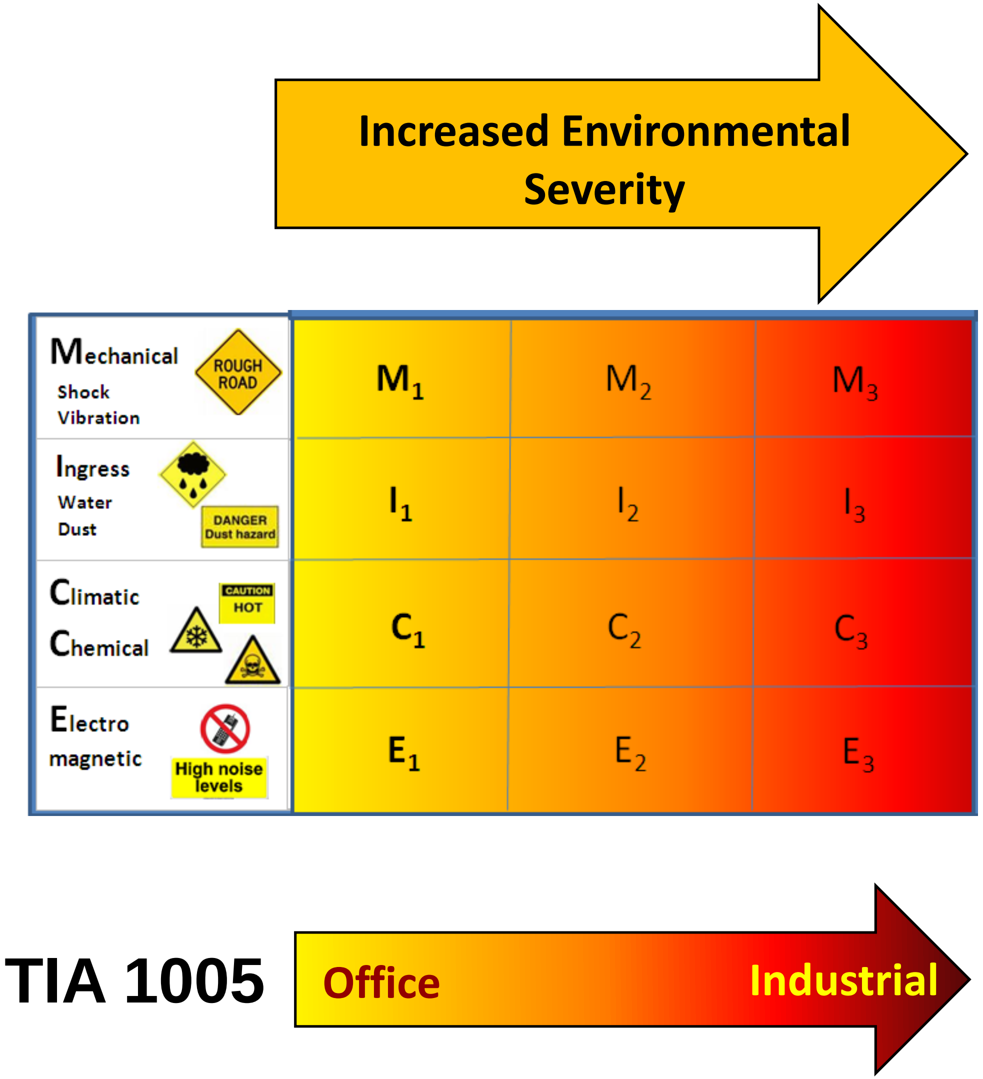
ODVA

ODVA Guide

Fiber Guide
ENET-TD003

Environmental Focus – M.I.C.E.

Resiliency



- M.I.C.E. provides a method of categorizing the environmental classes for each plant Cell/Area Zone.
- The MICE environmental classification is a measure of product robustness:
  - Specified in ISO/IEC 24702
  - Part of TIA-1005 and ANSI/TIA-568-C.0 standards
- This provides for determination of the level of “hardening” required for the network media, connectors, pathways, devices and enclosures.
- Examples of rating:
  - 1585 Industrial Ethernet Media : $M_3I_3C_3E_3$
  - M12: $M_3I_3C_3E_3$
  - RJ-45: $M_1I_1C_2E_2$

Rockwell Automation

Select best media for your needs

Resiliency

UTP vs. STP	**Unshielded Twisted Pair (UTP)**	**Shielded Twisted Pair (STP)**
	Costs less	Excellent immunity from EMI and RFI noise
	Installs faster	Can locate cable close to source of noise
	Smaller diameter, more flexible	Well suited for more rigorous environments
CAT5e vs. CAT6a	**CAT5e**	**CAT6a**
	Costs Less	Higher signal to noise ration; performance margins
	Suitable for speeds of less than a Gbps	Designed to deliver Gbps performance
Copper vs. Fiber	**Copper**	**Fiber**
	Termination and installation is faster	Cost of fiber transceivers is higher
	Less fragile	Use when excessive EMI noise is present
	Distances of less than 100m	Use when distance is a factor (over 100m)
Multi-mode vs. Single-mode Fiber	**Multi-mode**	**Single-mode**
	For distances of up to 550m @ 1Gbps and 2km @ 100 Mbps	Longer distances (up to 40km)
	Lower cost transceivers, connectors and installation	High bandwidth capabilities
	Higher fiber cost, but lower total system cost	Lower fiber cost, but higher total system cost

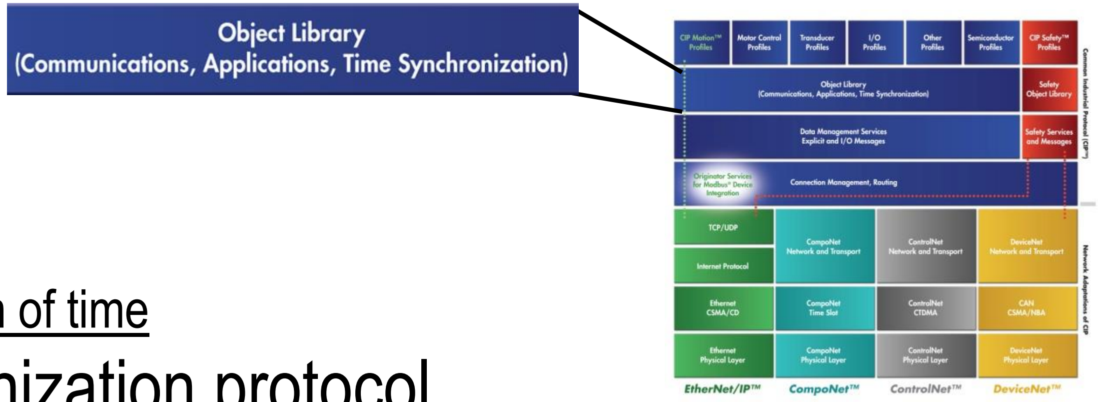
Key Tenet

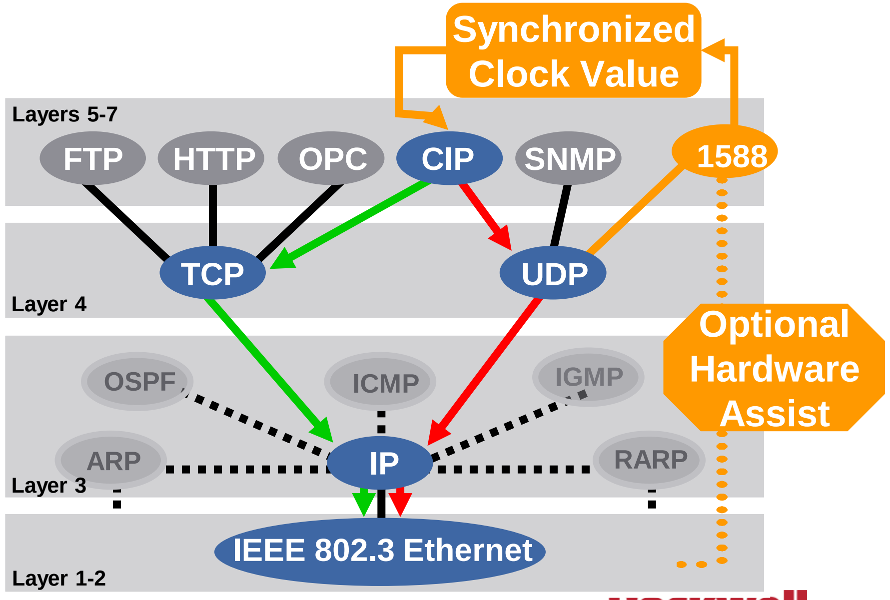
Time-critical Data - Time Synchronization and Data Prioritization

Time Synchronization – CIP Sync

Time-critical Data - Time Synchronization

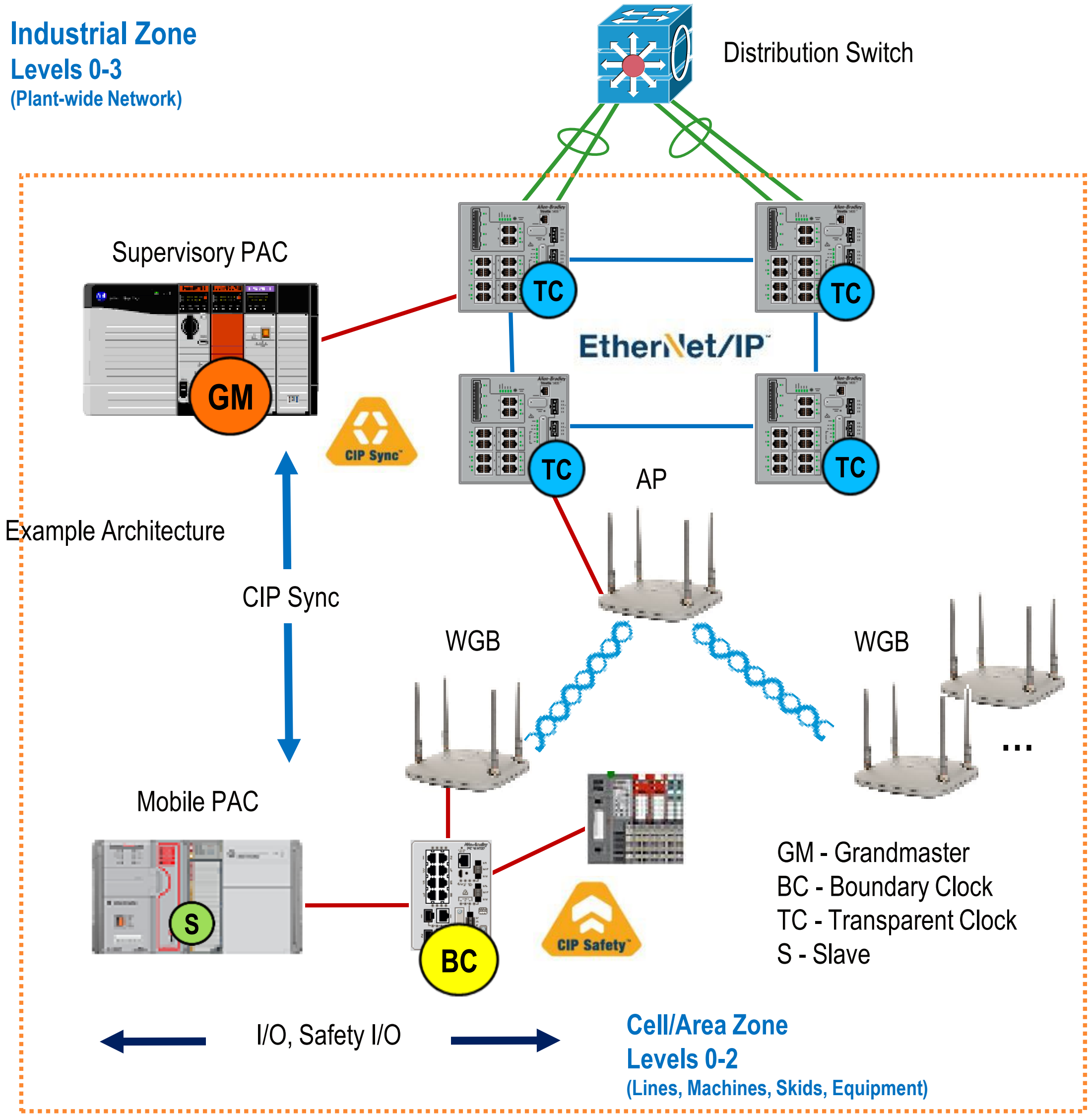
- CIP™ Extension
- Defines time synchronization services and object for CIP Networks
  - Allows distributed control components to share a common notion of time
- Implements IEEE-1588 precision clock synchronization protocol
  - Referred to as precision time protocol (PTP)
  - Provides +/- 100 ns synchronization (hardware-assisted clock)
  - Provides +/- 100 µs synchronization (software clock)
- Time Synchronized Applications such as:
  - Input time stamping
    - Alarms and Events
    - Sequence of Events (SOE)
    - First fault detection
  - Scheduled outputs, synchronized actuation
  - Coordinated Motion





Time Synchronization – CIP Sync, IEEE 1588 Precision Time Protocol

Time-critical Data - Time Synchronization

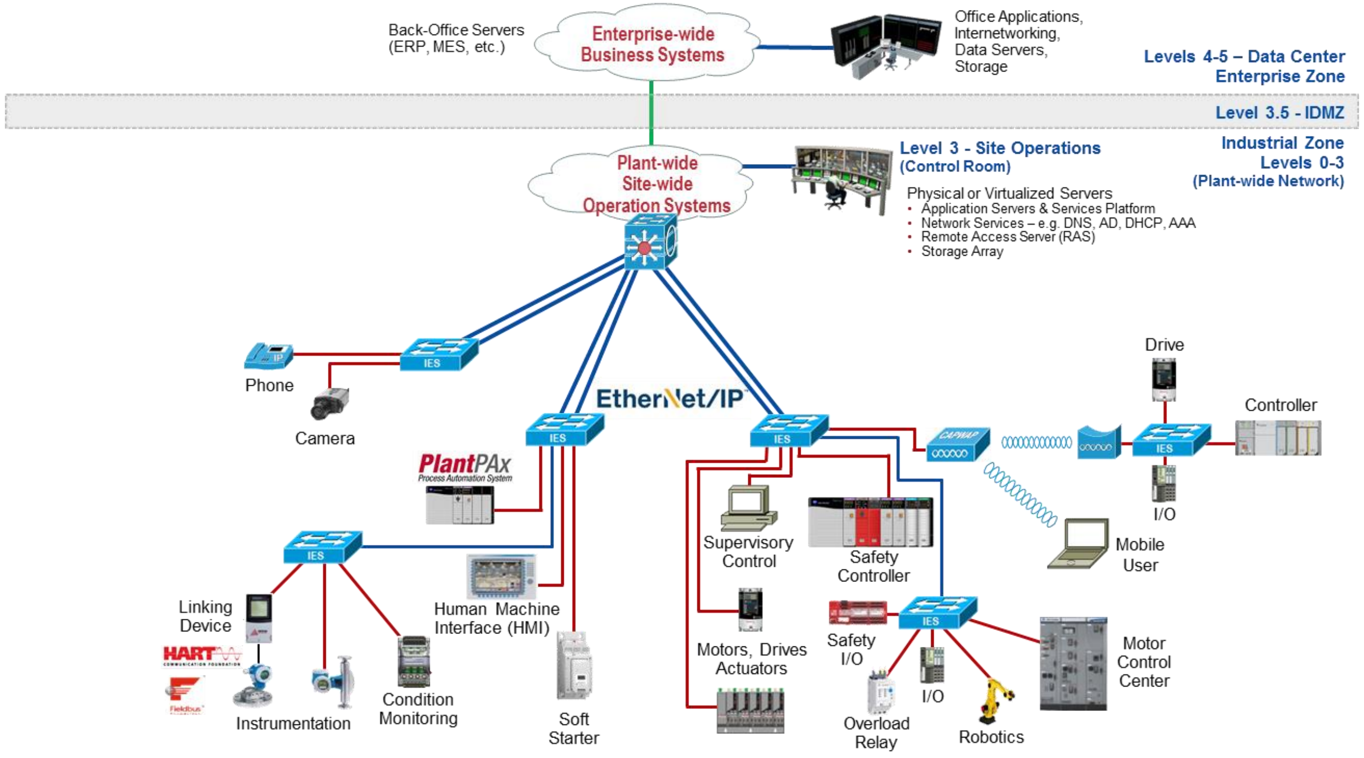


- CIP Sync Defines
  - System Time data representation
  - Clock Model for each node
  - Timestamp Step Compensation Algorithm
  - Time Sync Object for CIP
- PTP Clock Types
  - Ordinary
  - Grandmaster (GM)
  - Boundary Clock
  - Transparent Clock

Data Prioritization – Quality of Service (QoS)

Time-critical Data - Data Prioritization

- QoS helps mitigate the following network issues:
  - End-to-end delay
    - Fixed delay – latency
    - Variable delay – jitter
  - Bandwidth capacity issues
  - Packet loss
- QoS design considerations:
  - Provides preferential forwarding treatment to some data traffic, at the expense of others
  - QoS prioritizes traffic into different service levels
  - Allows for more predictable service for different applications and traffic types

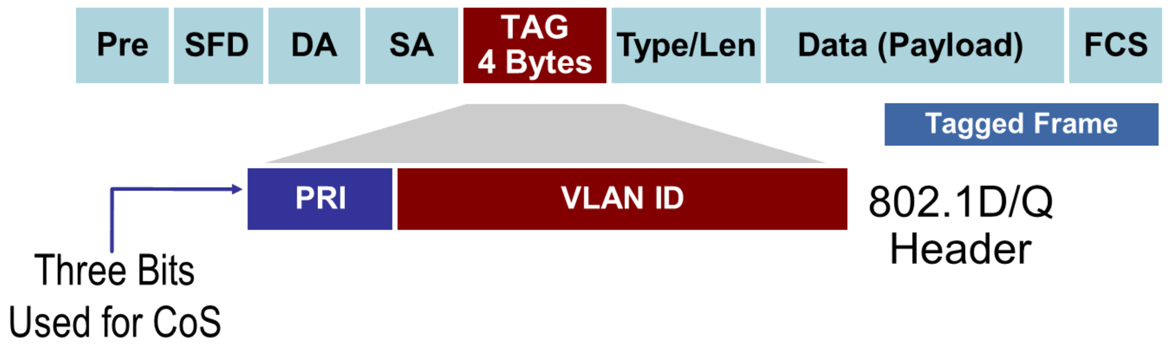


Plant-wide / Site-wide Network
Integrated Architecture – Intelligent Motor Control

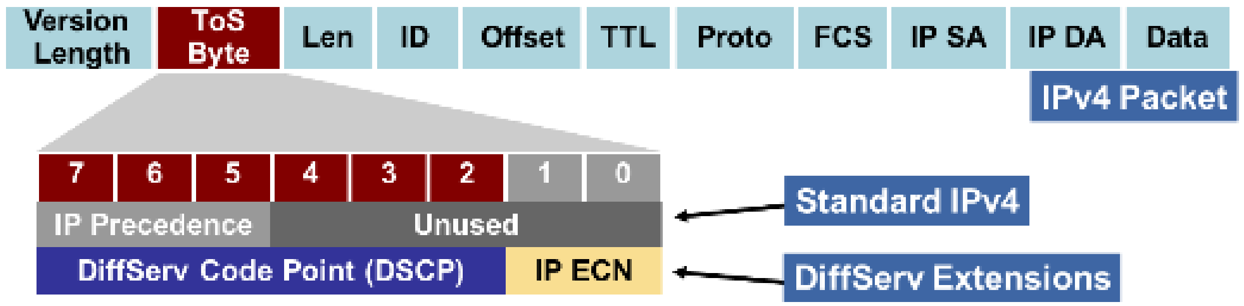
Data Prioritization – Quality of Service (QoS) Markings

Time-critical Data - Data Prioritization

Layer 2 CoS Class of Service



Layer 3 ToS Type of Service Differentiated Server Code Point

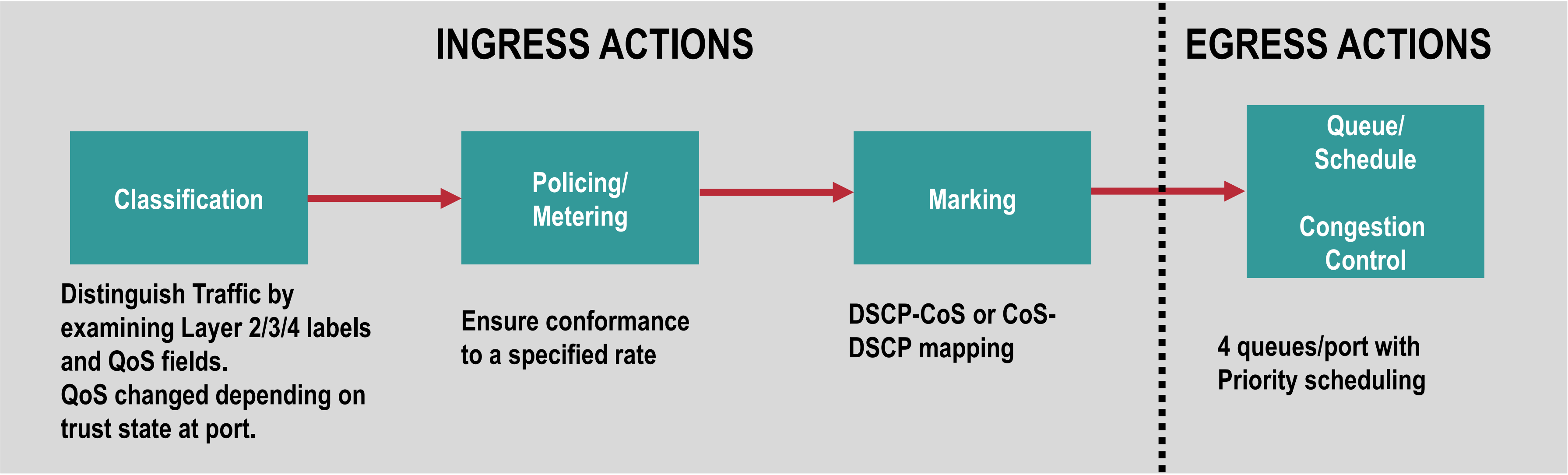


Rockwell Automation

Data Prioritization –Quality of Service (QoS) Policies

Time-critical Data - Data Prioritization

- QoS classification based on Layer attributes:
  - Layer 2 Destination MAC Address, Layer 2 EtherType
  - Layer 3 Source / Destination IP Address
  - Layer 4 TCP / UDP Source or Destination Port Number – e.g. UDP 2222 and TCP 44818
- ODVA EtherNet/IP QoS Specification
  - Layer 2 … Class of Service (CoS) … 802.1D/Q
  - Layer 3 … type of service (ToS) … DiffServ Code Point (DSCP)



Data Prioritization – ODVA Quality of Service (QoS) Policies

Time-critical Data - Data Prioritization

Traffic Type	CIP Priority	DSCP Layer 3	CoS Layer 2	CIP Traffic Usage
PTP event (IEEE 1588)	n/a	59	7	n/a
PTP General (IEEE 1588)	n/a	47	5	n/a
CIP class 0/1	Urgent (3)	55	6	CIP Motion
	Scheduled (2)	47	5	Safety I/O I/O
	High (1)	43	5	I/O
	Low (0)	31	3	No recommendation at present
CIP UCMM CIP class 2/3	All	27	3	CIP messaging

THE CIP NETWORKS LIBRARY
Volume 2
EtherNet/IP Adaptation of CIP
Edition 1.22, November 2016

Data Prioritization – ODVA Quality of Service (QoS) Policies

Time-critical Data - Data Prioritization

- Embedded Switch Technology – Linear and Ring Topologies
- ODVA has specified QoS markings for CIP and PTP traffic

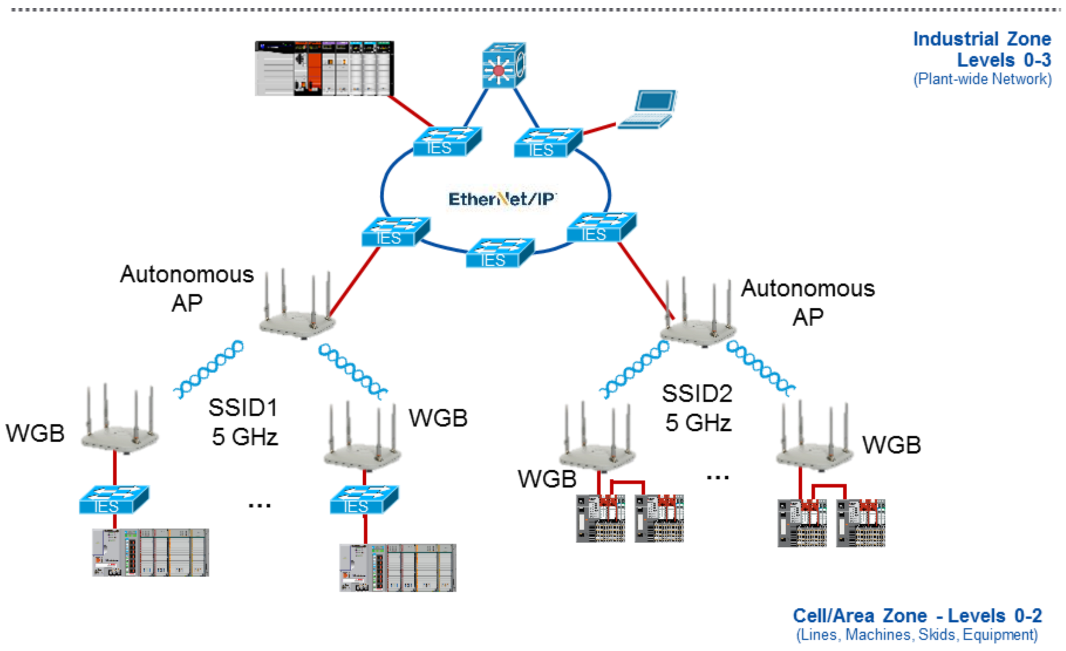
CIP Priority	DSCP Layer 3	CoS Layer 2	CIP Traffic Usage
Highest	59	7	Beacon, PTP Event
High	55		CIP Motion
Low	43, 47		I/O, Safety I/O, PTP General
Lowest	0-42, 44-46, 48-54, 56-58, 60-63	1, 2, 3, 4, 5, 6	Best effort

Key Tenet

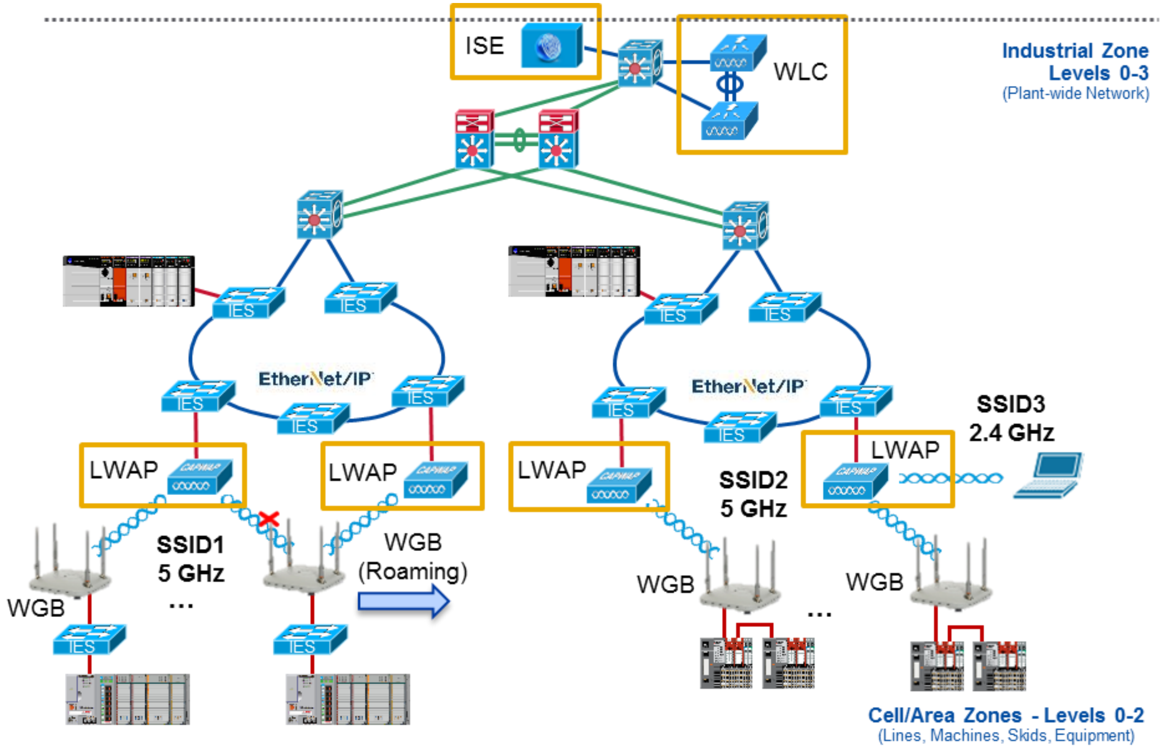
Wireless - Mobility

CPwE WLAN

Wireless - Mobility



Autonomous WLAN Architecture



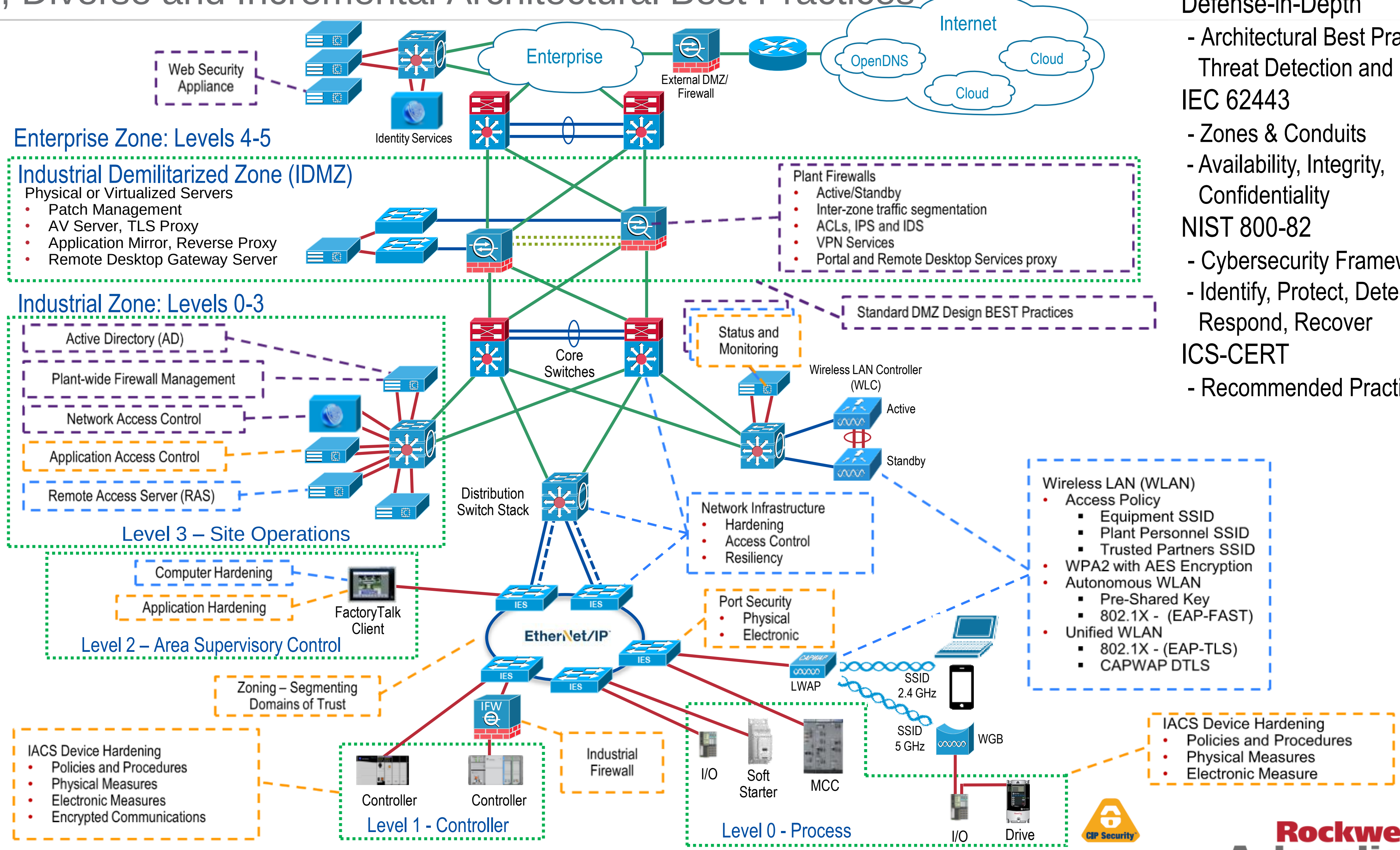
Unified WLAN Architecture

Key Tenet

Holistic & Diverse Defense-in-Depth Security

CPwE Industrial Security Framework

Holistic, Scalable, Diverse and Incremental Architectural Best Practices



Defense-in-Depth
- Architectural Best Practices for Threat Detection and Protection

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

NIST 800-82
- Cybersecurity Framework
- Identify, Protect, Detect, Respond, Recover

ICS-CERT
- Recommended Practices

Personas

Control System Engineers (OT)

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

IT Security Architects in Collaboration with Control Systems Engineers

Rockwell Automation

Key Tenet

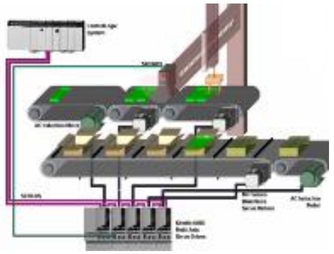
Convergence-Ready Network Solutions

Design and Implementation Considerations

Convergence-Ready Network Solutions

Early, open and two-way OT-IT dialogue is critical!

Partner Solution(s)
e.g. Machine



Plant-wide Industrial
Automation & Control System

Partner Solution(s)
e.g. Process Skid

Plant-wide Industrial
Automation & Control System

Design and deployment considerations that a partner (e.g. OEM, SI, Contractor) has to take into account to achieve seamless integration of their solution (e.g. equipment, skid, machine) into their customers' plant-wide/site-wide network infrastructure.

Alignment with End User - Network Services:

Convergence-Ready Network Solutions

- Use of a common industrial network technology that fully uses standard Ethernet and IP networking technology as the multi-discipline industrial network infrastructure.
- IP addressing schema
  - Who manages? End User (OT/IT) or OEM?
  - Address range (class), subnet, default gateway (routability)
  - Implementation conventions – static/dynamic, hardware/software configurable, NAT/DNS
- Use Common Layer 2 and Layer 3 Network Services
  - Switches - managed vs. unmanaged, industrial vs. COTS, system vs. component approach
  - Segmentation, data prioritization
  - Topologies - switch-level, device-level, hybrid
  - Availability – loop prevention, redundant path topologies with resiliency protocols
  - Time Synchronization Services
    - IEEE 1588 Precision Time Protocol (PTP w/E2E) – first fault, SOE, Motion

The OEM Guide to Networking
ENET-RM001_-EN-P

Additional Material

Additional Material

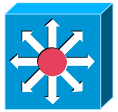
Network Architecture Icon Key

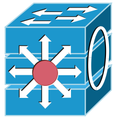

Layer 2 Access Switch, Catalyst 2960

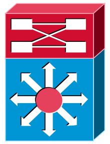
Layer 2 Access, Industrial Ethernet Switch (IES),
Stratix® 2500, Stratix 5700, Stratix 5400, Stratix 8000

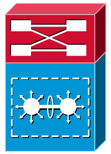
Layer 2 IES with NAT, Stratix 5700, Stratix 5400

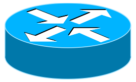
Layer 2 IES with NAT and Connected Routing,
Stratix 5700, Stratix 5400

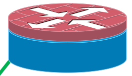

Multi-Layer Switch - Layer 2 and Layer 3,
Stratix 8300, Stratix 5700, Stratix 5400, Stratix 5410

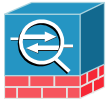

Layer 3 Distribution Switch Stack,
Catalyst 3750-X, Catalyst 3850

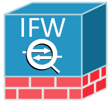

Layer 3 Core Switch,
Catalyst 4500, 4500-X, 6500, 6800


Layer 3 Core Switch with Virtual Switching System (VSS)
Catalyst 4500-X, 6500, 6800

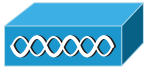

Layer 3 Router, Stratix 5900

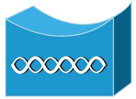

Layer 3 Router with Zone-based Firewall, Stratix 5900


Firewall, Adaptive Security Appliance (ASA) 55xx



Industrial Firewall, Stratix 5950


Autonomous Wireless Access Point (AP)


Wireless workgroup bridge (WGB)

Unified Wireless Lightweight Access Point (LWAP),
Catalyst 3602E LWAP


Unified Wireless LAN Controller (WLC), Cisco 5508 WLC


Unified Computing System (UCS), UCS-C series


Identity Services Engine (ISE) for Authentication,
ISE - PAN/PSN/MnT

Layer 2 Access Link (EtherNet/IP Device Connectivity)

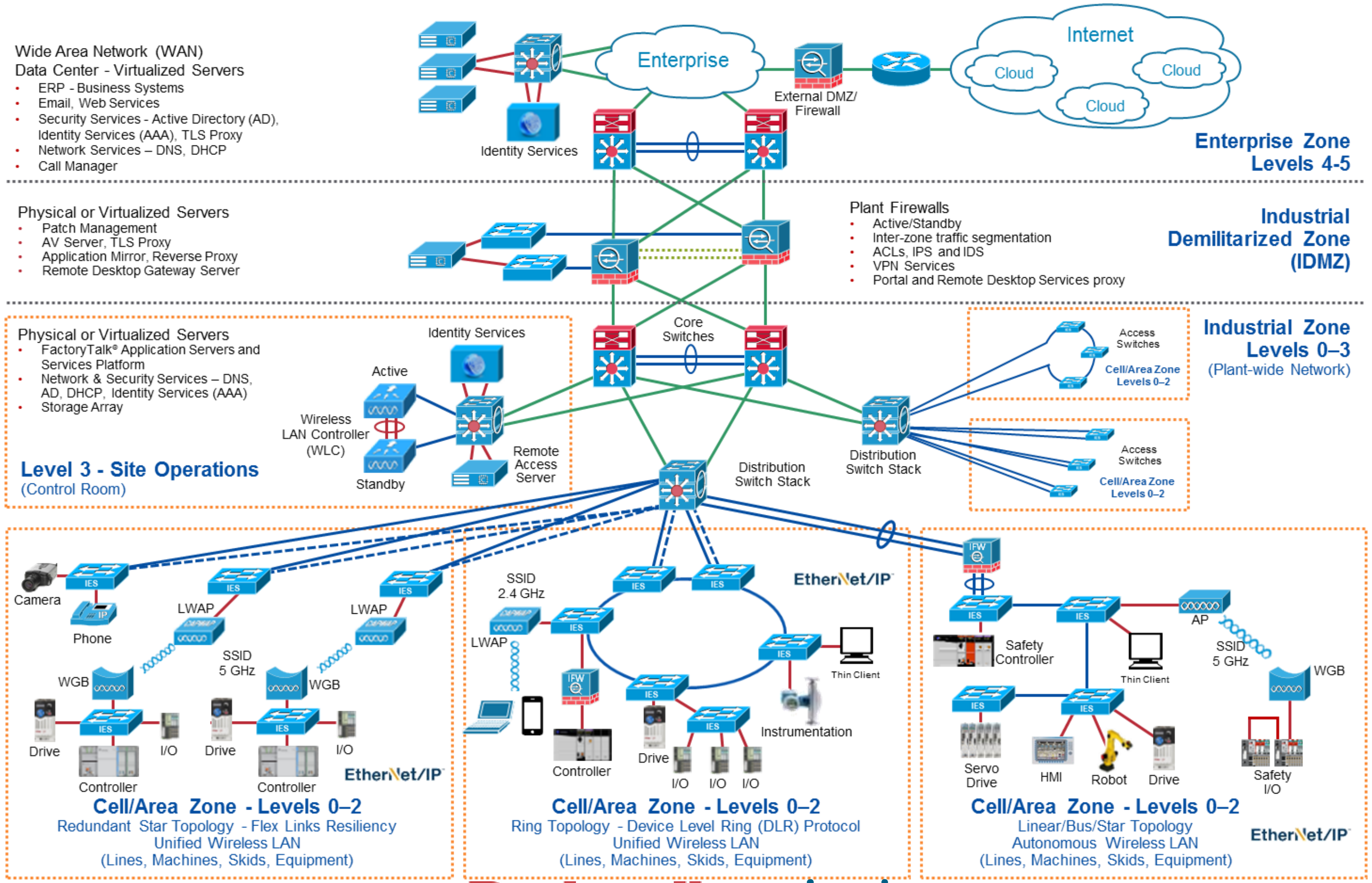
Layer 2 Interswitch Link/802.1Q Trunk

Layer 3 Link

Additional Material

CPwE Architectures - Cisco and Rockwell Automation®

- CPwE website
- Overview Documents
  - Alliance Profile
  - Top 10 Recommendations for Plant-wide EtherNet/IP Deployments
  - Design Considerations for Securing Industrial Automation and Control System Networks



Additional Material

CPwE Architectures - Cisco and Rockwell Automation®

Topic	Design Guide	Whitepaper
Design Considerations for Securing IACS Networks	N/A	ENET-WP031A-EN-P
Converged Plantwide Ethernet – Baseline Document	ENET-TD001E-EN-P	N/A
Deploying 802.11 Wireless LAN Technology within a CPwE Architecture	ENET-TD006A-EN-P	ENET-WP034A-EN-P
Deploying Identity and Mobility Services within a CPwE 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 CPwE Architecture	ENET-TD007A-EN-P	ENET-WP036A-EN-P
Migrating Legacy IACS Networks to a CPwE Architecture	ENET-TD011A-EN-P	ENET-WP040A-EN-P
Deploying A Resilient Converged Plantwide Ethernet Architecture	ENET-TD010B-EN-P	ENET-WP039D-EN-P
Site-to-site VPN to a CPwE Architecture	ENET-TD012A-EN-P	N/A
Deploying Industrial Firewalls within a CPwE Architecture	ENET-TD002A-EN-P	ENET-WP011B-EN-P
Deploying Device Level Ring within a CPwE Architecture	ENET-TD015A-EN-P	ENET-WP016C-EN-P
OEM Networking within a CPwE 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 CPwE Architecture	ENET-TD014A-EN-P	ENET-WP013A-EN-P
Scalable Time Distribution within a Converged Plantwide Ethernet Architecture	ENET-TD016A-EN-P	ENET-WP017A-EN-P
Network Security within a Converged Plantwide Ethernet Architecture	ENET-TD019A-EN-P	ENET-WP023A-EN-P

Additional Material

Rockwell Automation® Reference Documents

- Ethernet Design Considerations Reference Manual
  - ENET-RM002C-EN-P
  - EtherNet/IP Overview, Ethernet Infrastructure Components, EtherNet/IP Protocol, Predict System Performance
- EtherNet/IP IntelliCENTER® Reference Manual (MCC-RM001)

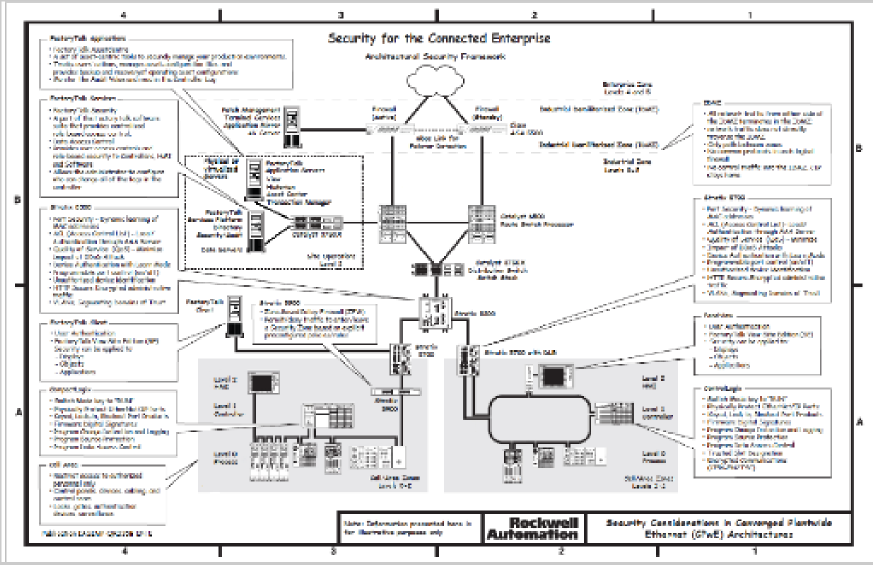
- The OEM Guide to Networking
  - ENET-RM001A-EN-P
  - This guide is intended to help OEMs understand relevant technologies, networking capabilities and other considerations that could impact them as they develop EtherNet/IP solutions for the machines, skids or equipment they build
- Segmentation Methods Within the Cell/Area Zone ENET-AT004B-EN-E

Additional Material

Rockwell Automation® Tools

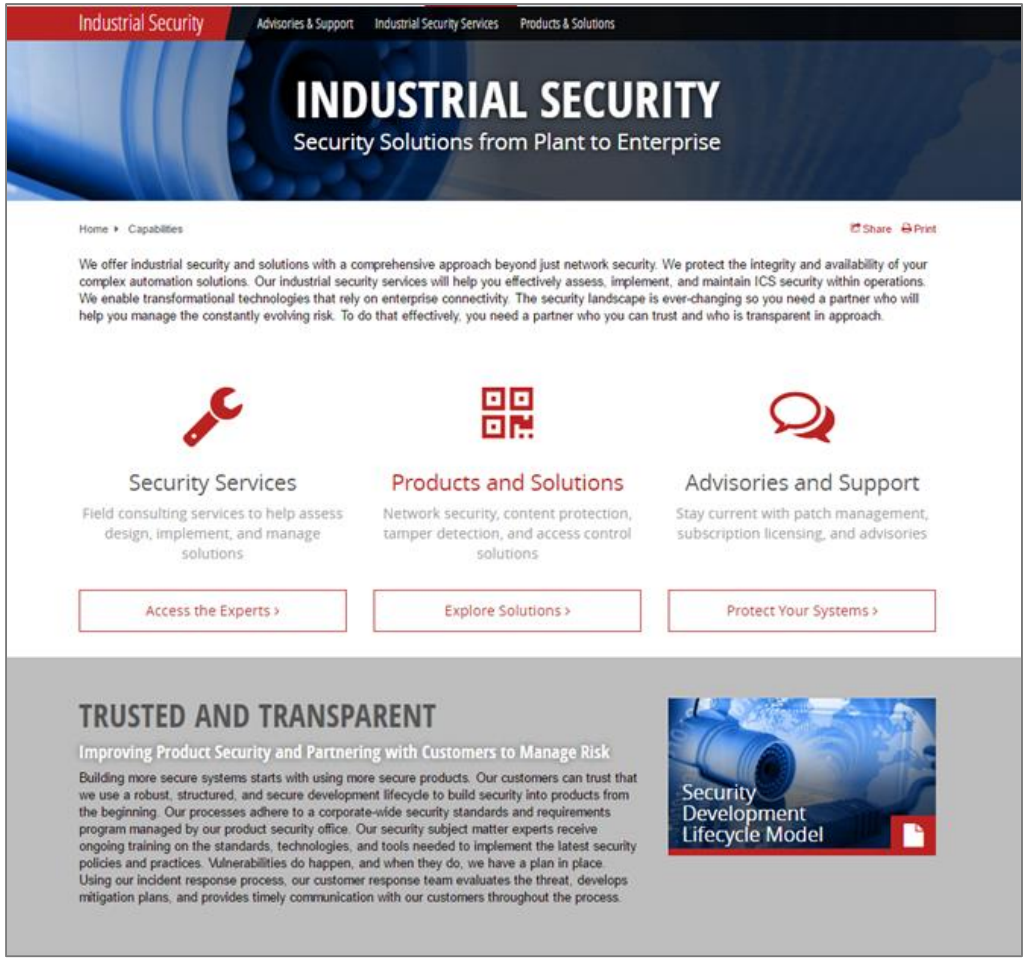
- [Integrated Architecture Builder (IAB)]
  - Updates and additions to better-reflect CPwE structure, hierarchy and best practices
  - Improved Switch Wizard for distribution (e.g. Stratix® 5410) and access (e.g. Stratix 5700)
  - Easier to create a large EtherNet/IP network with many topologies
  - CIP traffic is measured per segment, not just controller scanner and adapter centric

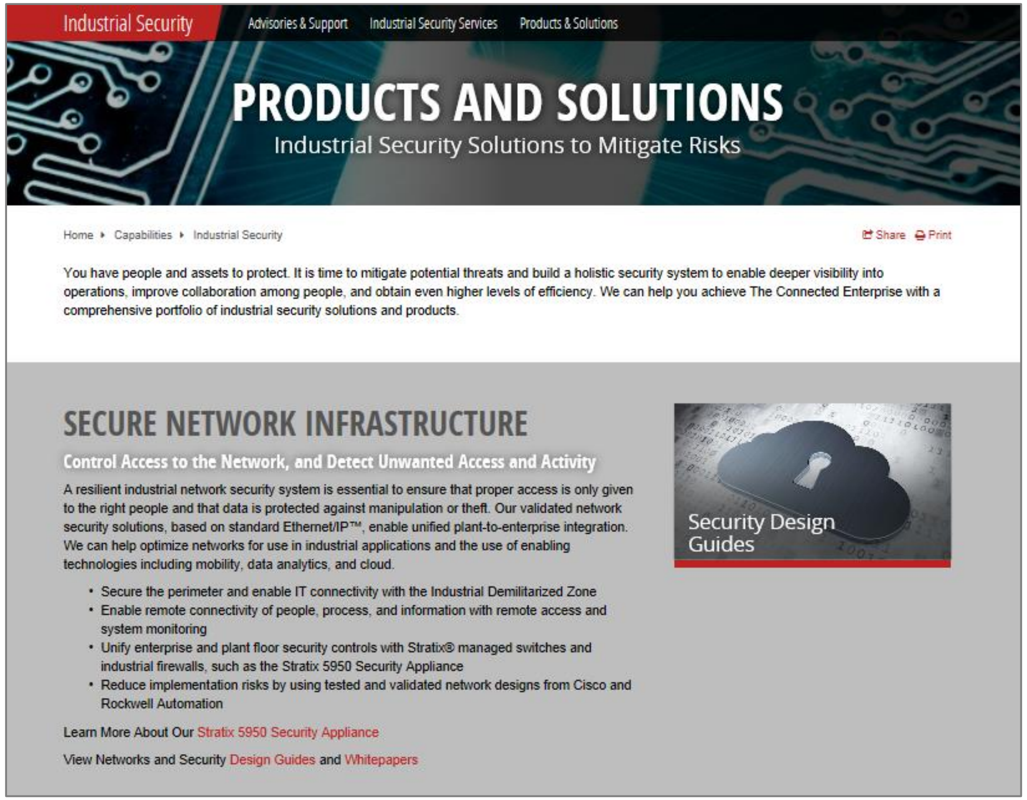
- [EtherNet/IP Capacity Tool]
- [System Configuration Drawings]
  - Updates and additions to better reflect CPwE recent enhancements



Additional Material

Rockwell Automation® Industrial Security Website





Additional Material

ODVA

- Website:
  - http://www.odva.org/
- EtherNet/IP
  - https://www.odva.org/Technology-Standards/EtherNet-IP/OverviewSecuring EtherNet/IP™ Networks
- EtherNet/IP Network Infrastructure Guide
  - https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf
- Common Industrial Protocol (CIP™)
  - https://www.odva.org/Technology-Standards/Common-Industrial-Protocol-CIP/Overview
- The Family of CIP Networks
  - https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00123R1_Common-Industrial_Protocol_and_Family_of_CIP_Networks.pdf
- CIP Security
  - https://www.odva.org/Technology-Standards/Common-Industrial-Protocol-CIP/CIP-Security