LISTEN.
THINK.
SOLVE.

Summer Days 2018

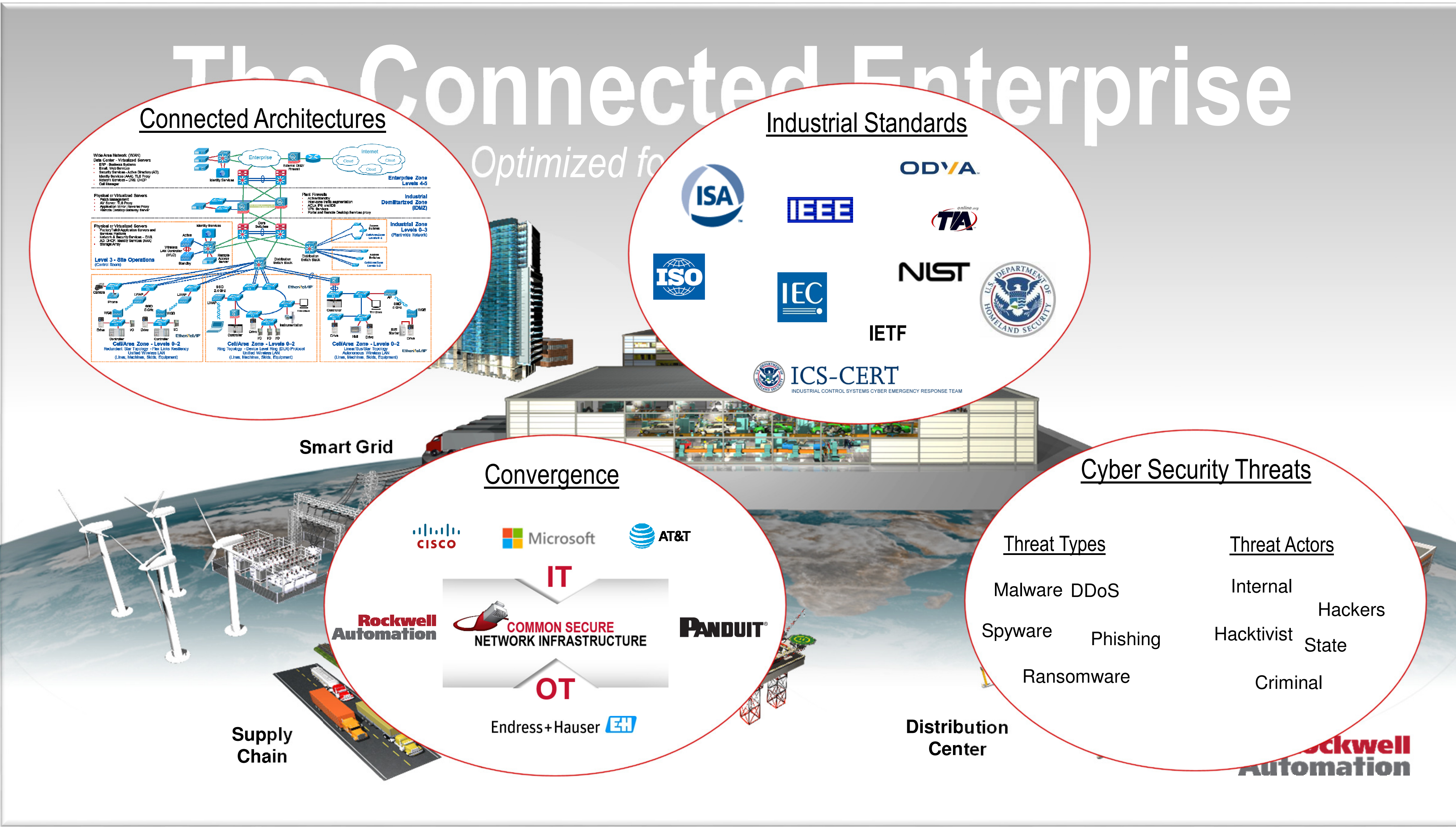
Networks Overview

Roman Foukal
Commercial Engineer A&S
TÜV Rheinland FS Technician ID No 322/15 Machinery

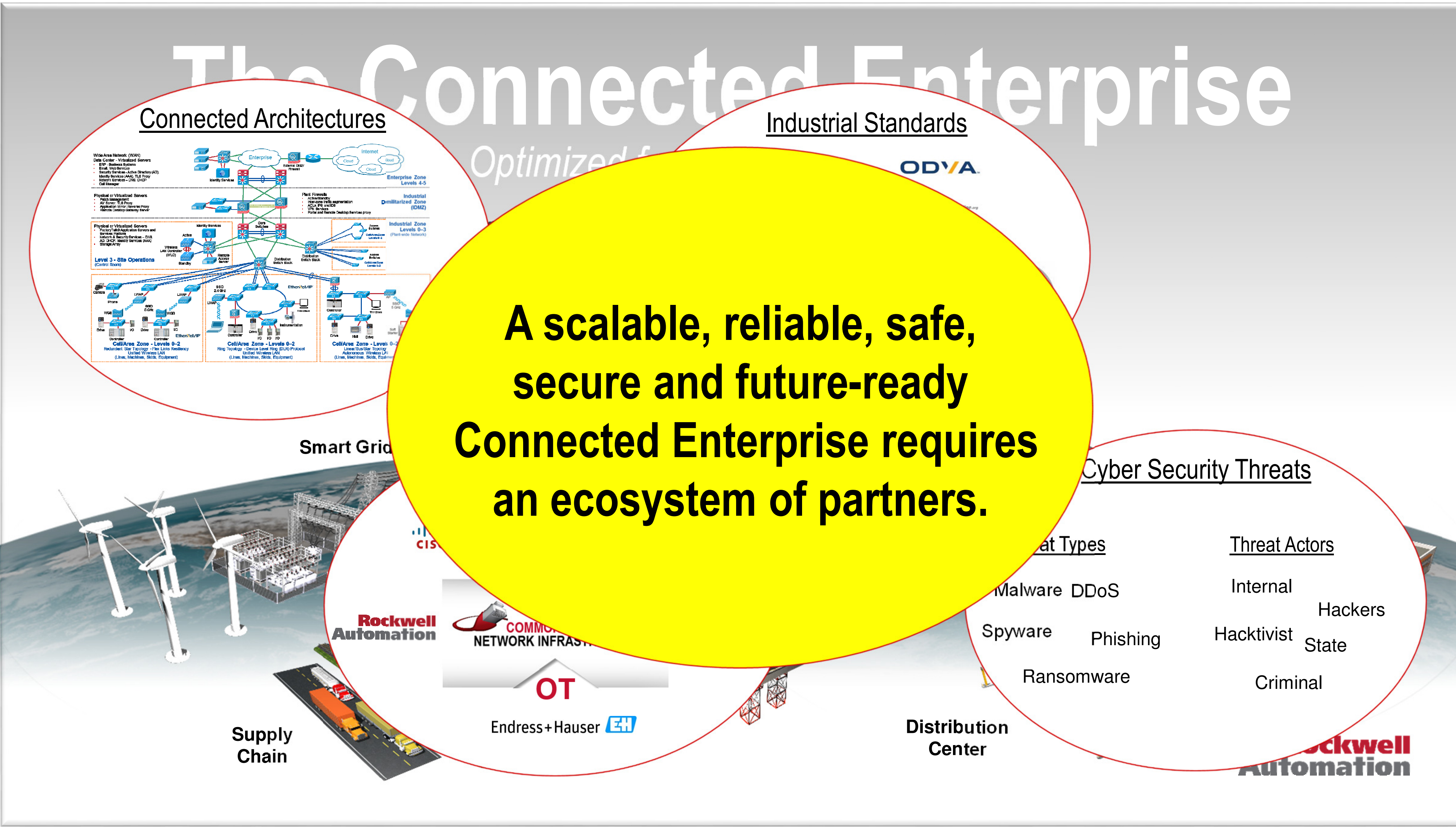
5. a 6. září 2018

Rockwell Automation

Challenges Associated with Technology Convergence



The Connected Enterprise
Optimized fo
Connected Architectures
Industrial Standards
ISA
ODVA
IEEE
TIA
ISO
IEC
NIST
IETF
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
Smart Grid
Convergence
CISCO
Microsoft
AT&T
IT
Rockwell Automation
COMMON SECURE
NETWORK INFRASTRUCTURE
PANDUIT
OT
Endress+Hauser
Supply Chain
Distribution Center
Cyber Security Threats
Threat Types
Malware
DDoS
Spyware
Phishing
Ransomware
Threat Actors
Internal
Hackers
Hacktivist
State
Criminal



The Connected Enterprise
Connected Architectures
Industrial Standards
ODVA
A scalable, reliable, safe, secure and future-ready Connected Enterprise requires an ecosystem of partners.
Smart Grid
Cyber Security Threats
Threat Actors
Malware
DDoS
Spyware
Phishing
Ransomware
Internal
Hackers
Hacktivist
State
Criminal
Rockwell Automation
NETWORK INFRAS
OT
Endress+Hauser
Supply Chain
Distribution Center

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!

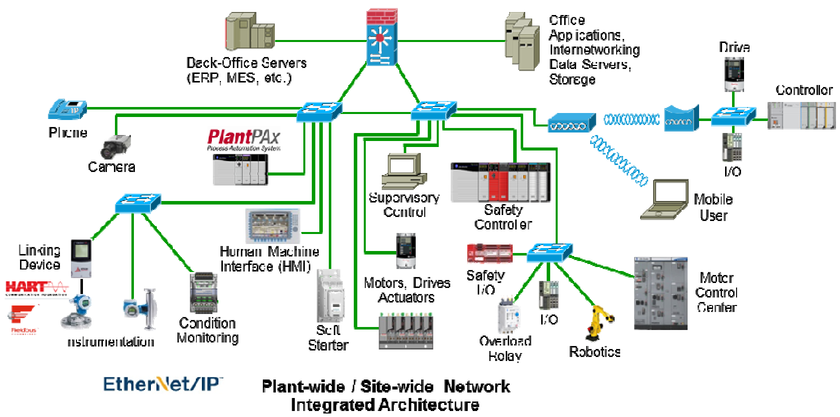
~~"one-size-fits-all"~~

- 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

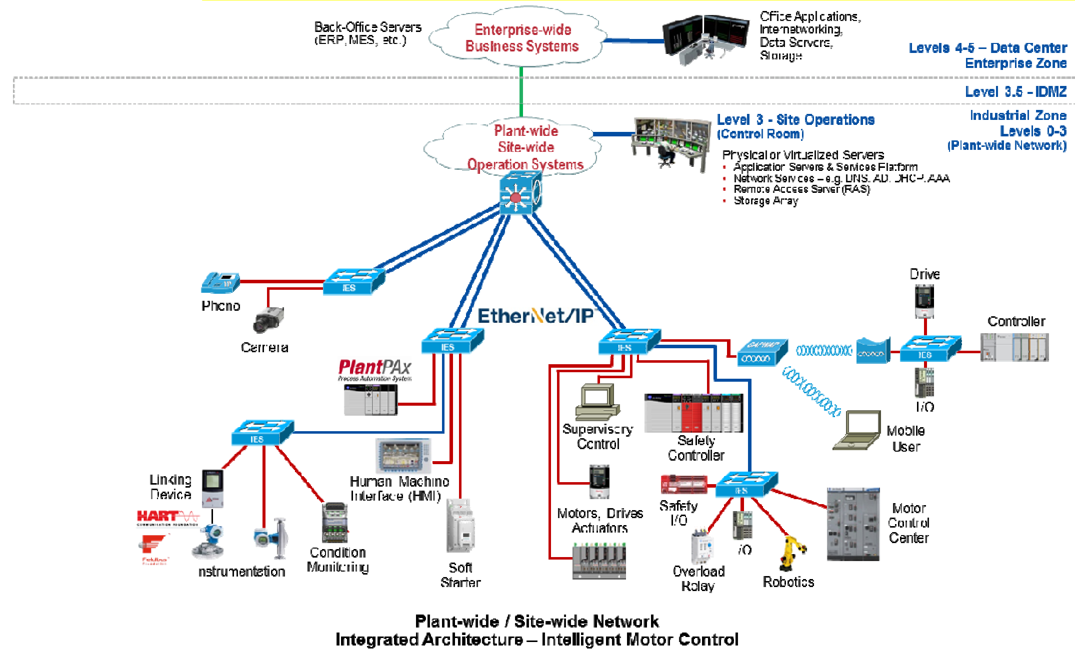
Challenges Associated with Technology Convergence

Large LAN, Lacking Natural Boundaries and Segmentation



Flat, Open and Non-Resilient IACS Network Infrastructure

Smaller Connected LANs to Create Boundaries and Segmentation

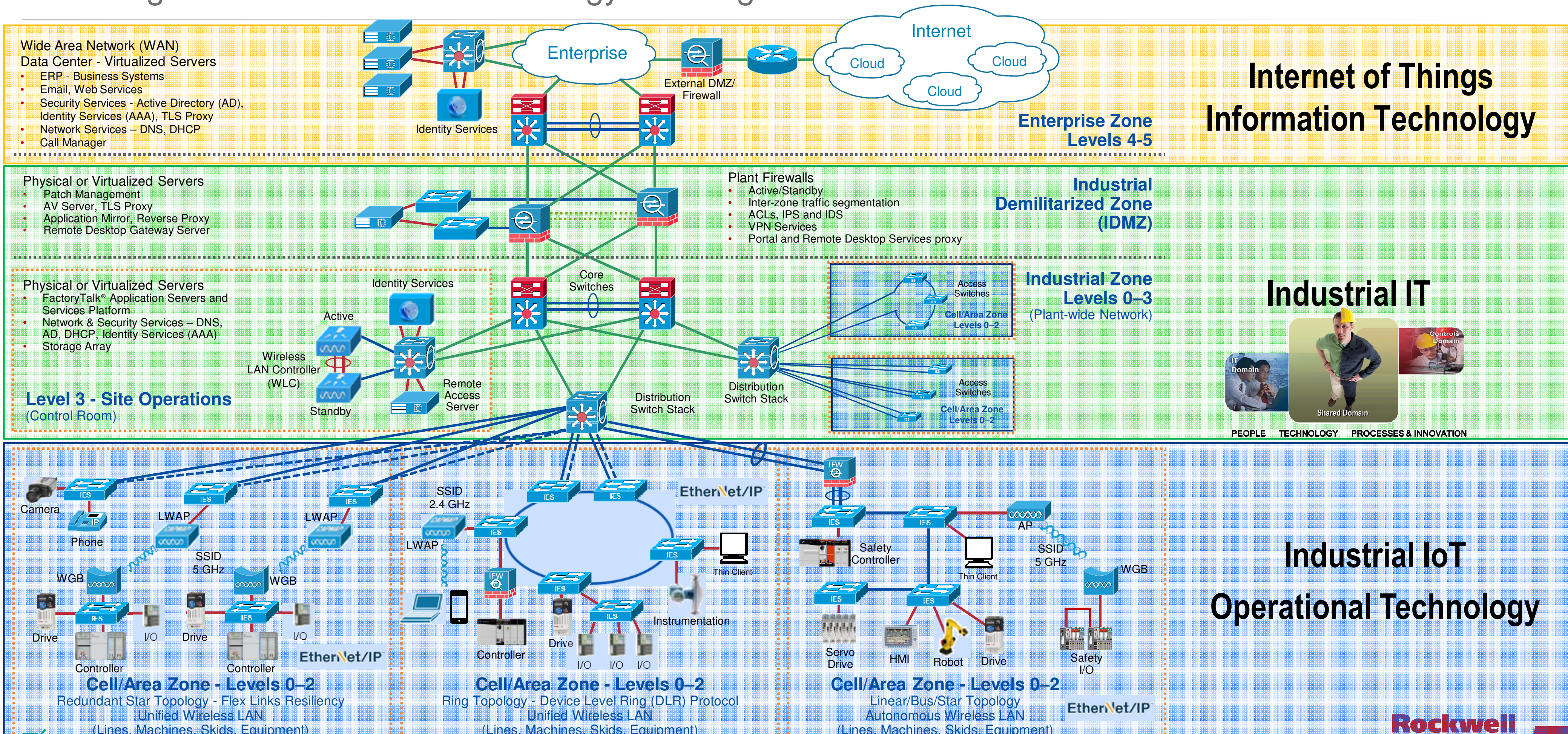


Structured and Hardened IACS Network Infrastructure

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

Key Requirements

Reliable and Secure Network Architectures for The Connected Enterprise

Structured and Hardened Architectures

Reliable and Secure Network Architectures for The Connected Enterprise

Key Requirements:

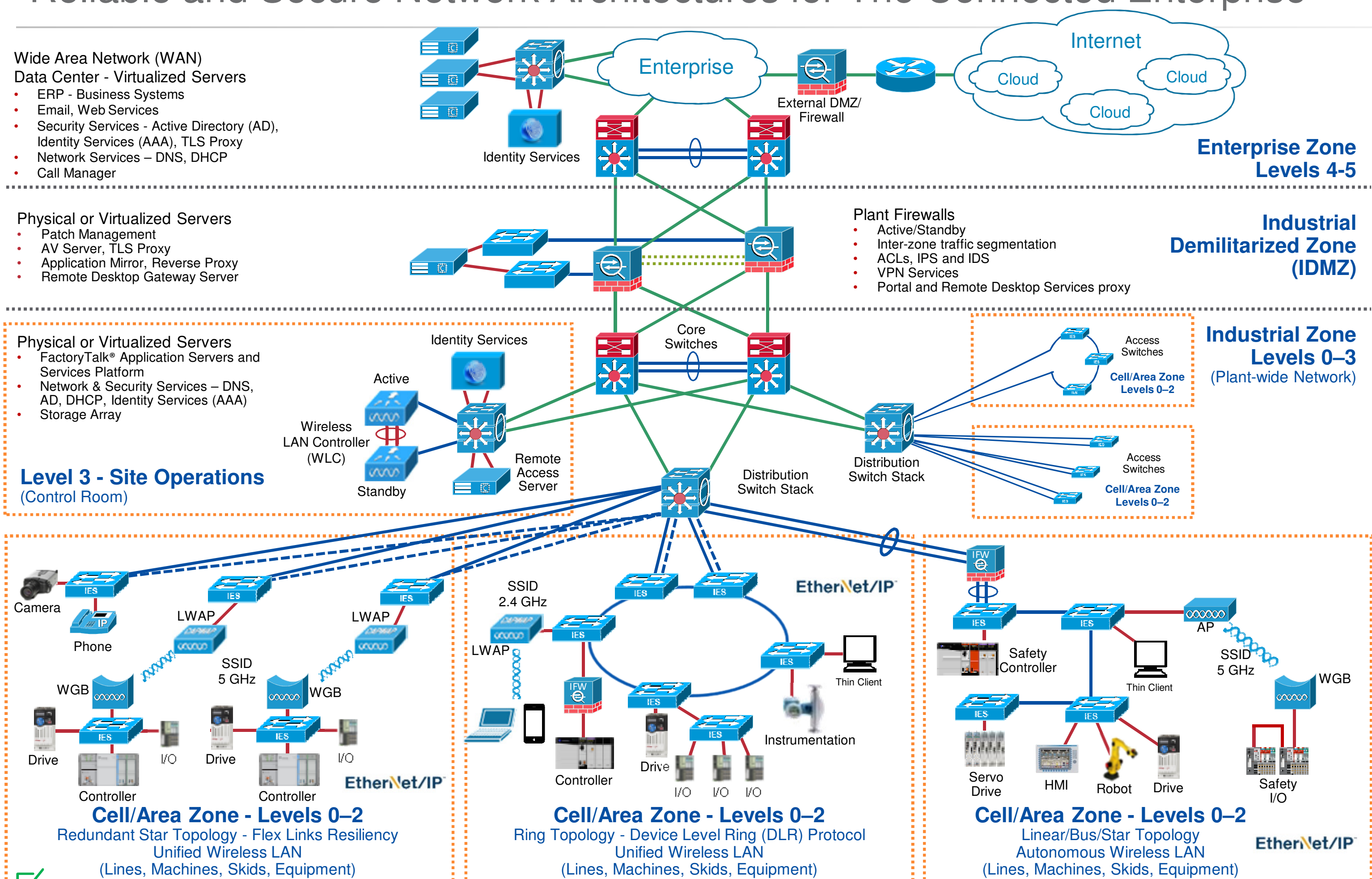
- Scalable
- Reliable
- Safe
- Secure
- Future-ready

Key Tenets:

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

Structured and Hardened Architectures

Reliable and Secure Network Architectures for The Connected Enterprise



Key Tenets:

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

Structured and Hardened Architectures

Reliable and Secure Network Architectures for The Connected Enterprise

- Smart IIoT Devices
  - Hardened, ODVA Conformance Tested
- Zoning (Segmentation)
  - Logical Model based on Standards
  - Switch Hierarchy (L2/L3), VLANs, NAT
- Managed Infrastructure
  - Loop prevention, Security, Diagnostics
- Resiliency
  - Robust Physical Layer
  - Redundant Path Topology with Resiliency Protocols
  - Redundant Switches and Firewalls
- Time-critical Data
  - Data Prioritization via Quality of Service (QoS)
  - Time Synchronization via IEEE 1588 Precision Time Protocol (PTP)
- Wireless – Mobility
  - Unified and Autonomous Architectures
  - Equipment and Personnel
- Holistic Defense-in-Depth Security
  - Multiple Layers, at different IACS Levels, with diverse technology
- Convergence-ready
  - Network Address Translation (NAT)

Key Tenet

Smart IIoT Endpoints

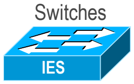
EtherNet/IP Network Technology and Devices

Single Industrial Network Technology

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

EtherNet/IP™

Layer No.		Layer Name	Function (Open Systems Interconnection)	Examples (Industrial Internet of Things (IIoT))
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™

Open Systems Interconnection

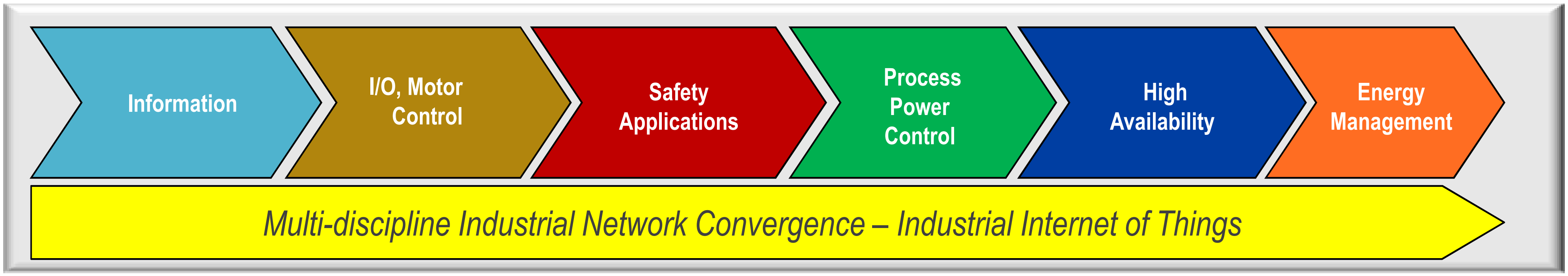
What makes EtherNet/IP industrial?

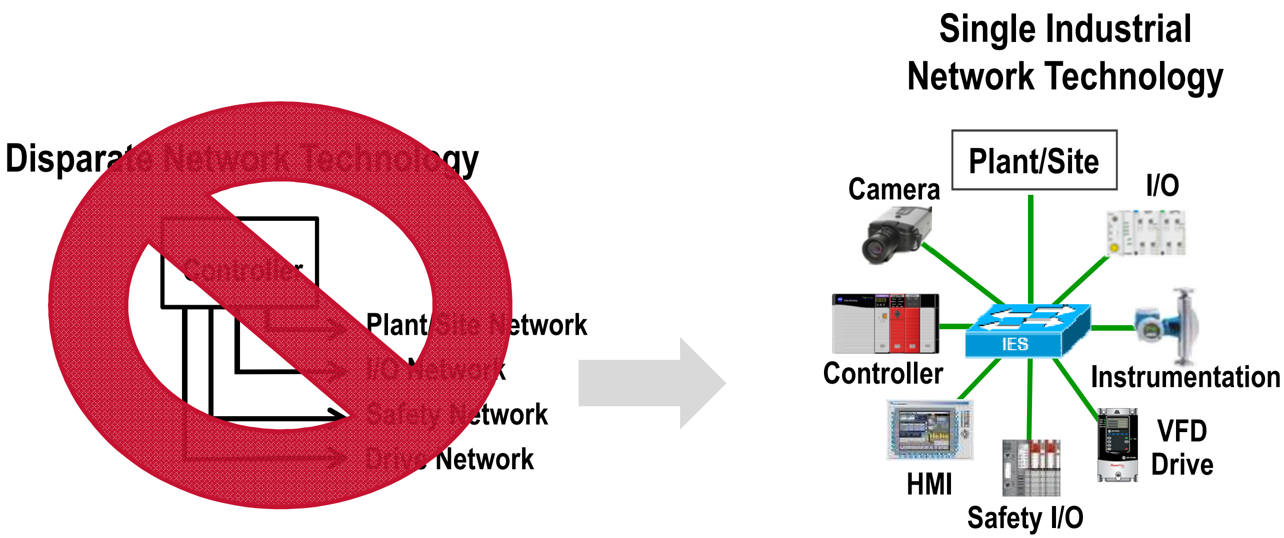
Layer No.		Layer Name	Function	Examples
Layer 7		Application	Network Services to User App	CIP - IEC 61158
Layer 6		Presentation	Encryption/Other processing	
Layer 5		Session	Manage Multiple Applications	
Layer 4		Transport	Reliable End-to-End Delivery Error Correction	IETF TCP/UDP
Layer 3	Routers	Network	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

Industrial Application Convergence

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





EtherNet/IP™

EtherNet/IP Device Selection

- 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

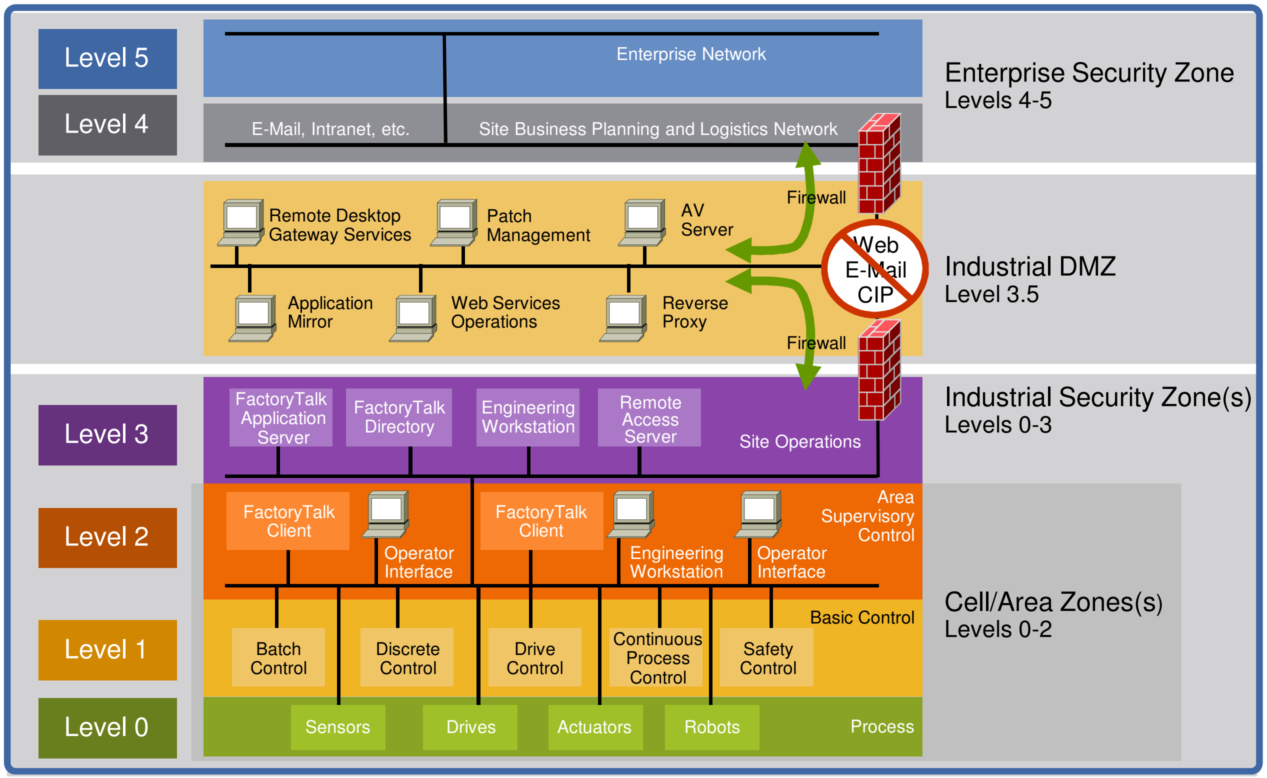
- Operational Levels
  - ISA 95, Purdue – Levels 0-5
    - Level 0 Sensor/Actuators
    - Level 1 Controller
    - Level 2 Local Supervisor
    - Level 3 Site Operations
    - Levels 4-5 Enterprise
- Functional / Security Zones
  - IEC-62443, NIST 800-82, DHS/INL/ICS-CERT
    - Enterprise, Industrial,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



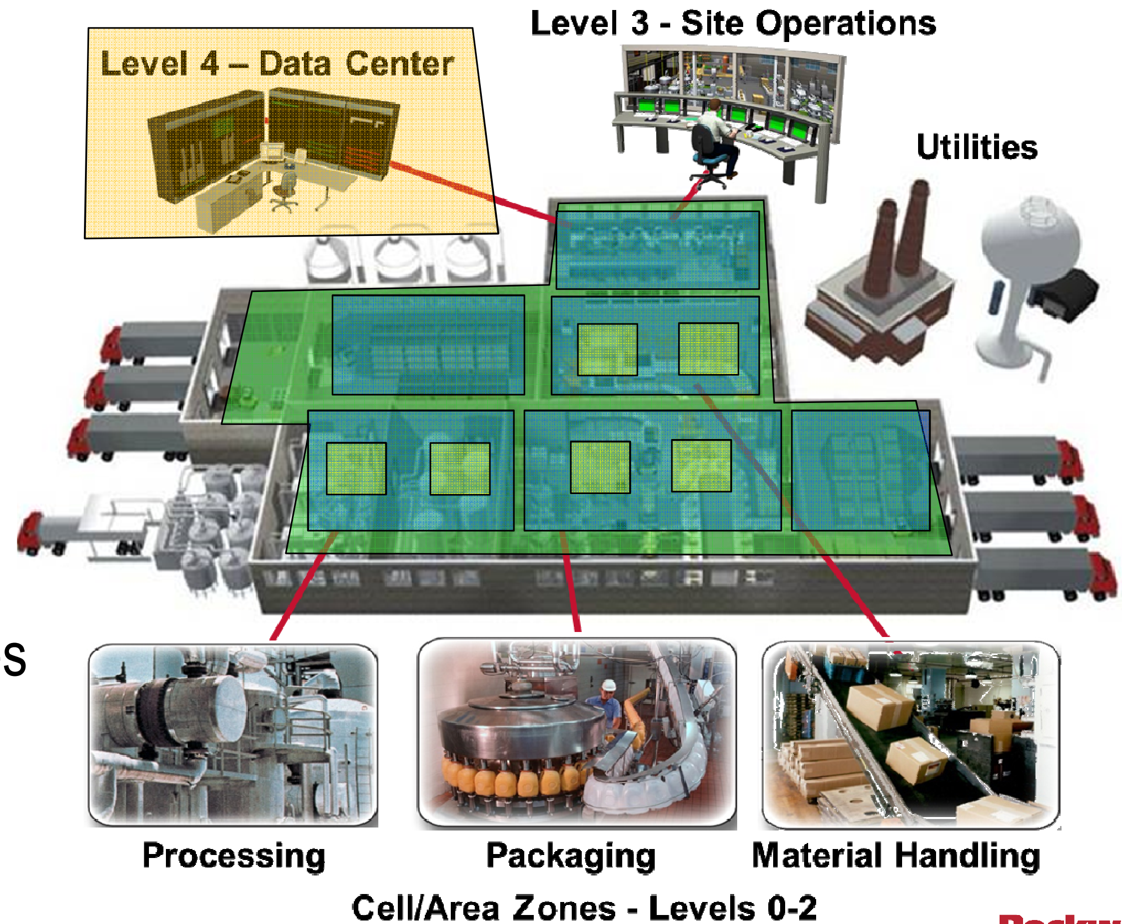
- Levels – ISA 95, Purdue Reference Model
- Zones – IEC 62443, NIST 800-82, DHS/INL/ICS-CERT Recommended Practices

Plant-wide Functional / Security Zoning

Logical Zoning (Segmentation)

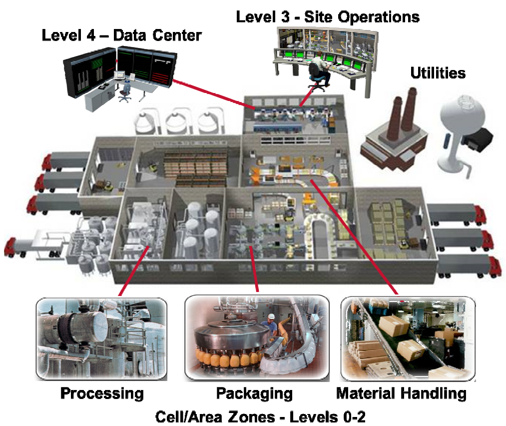
Plant-wide Zoning

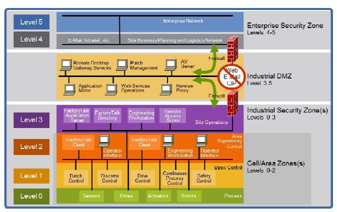
- Functional / Security Areas
- Smaller Connected LANs
  - Smaller Broadcast Domains
  - Smaller Fault Domains
  - Smaller Domains of Trust
- IEC 62443-3-2 Security Zones and Secure Conduits Model
- DHS/INL/ICS-CERT Best Practices
- Industrial IoT Technology
- Building Block Approach for Scalability

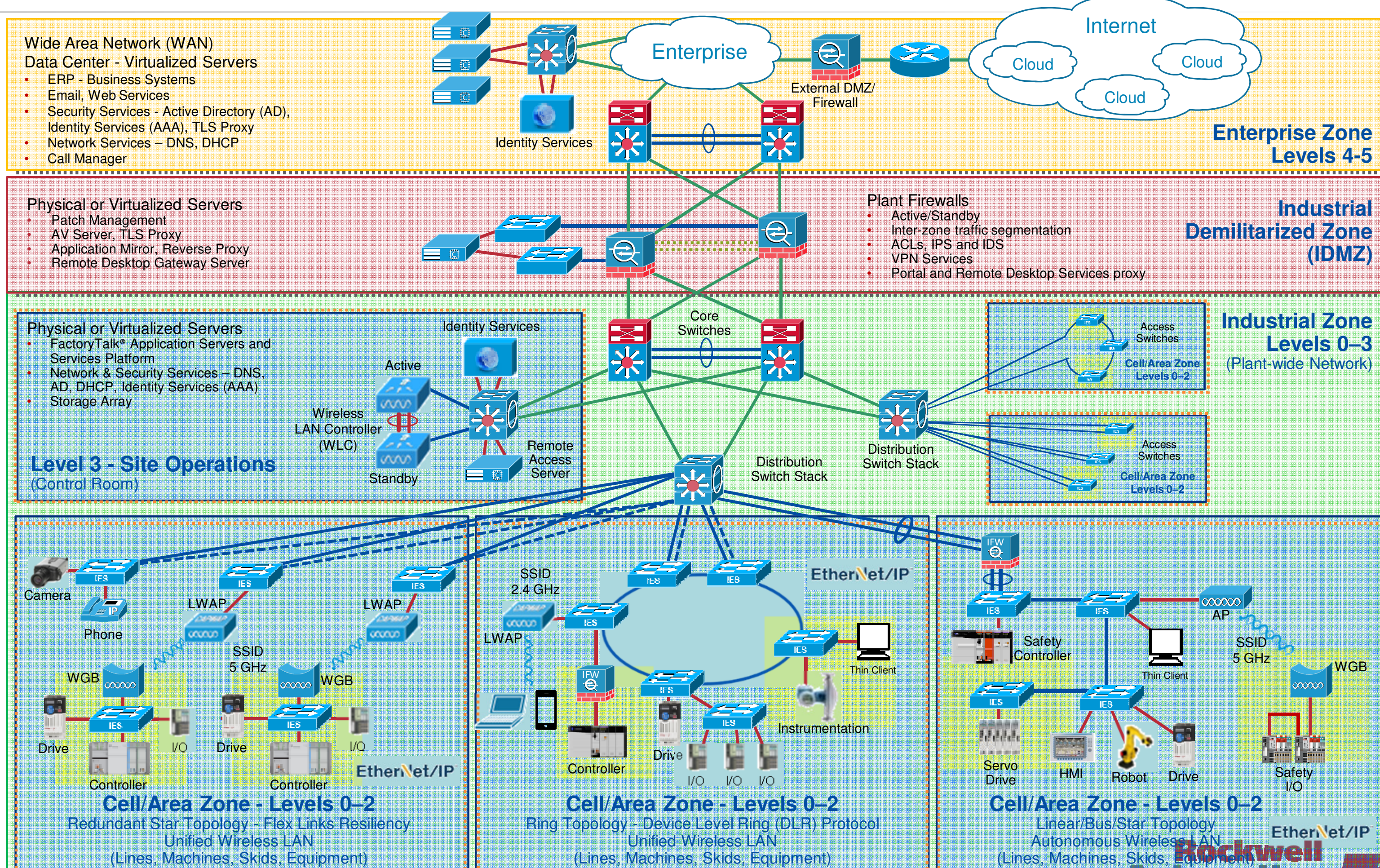


Plant-wide Functional / Security Zoning

Logical Zoning (Segmentation)







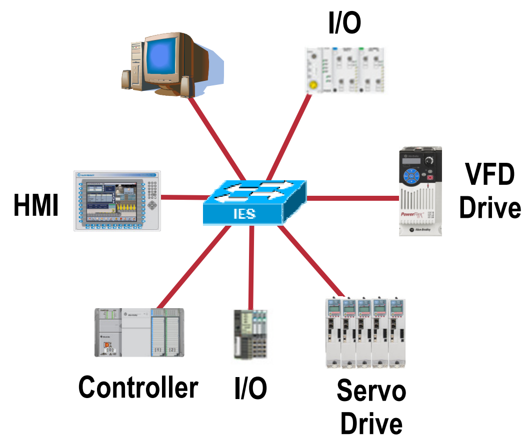
Key Tenet

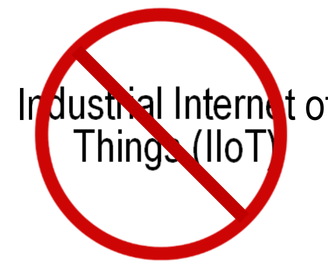
Segmentation – Network Services

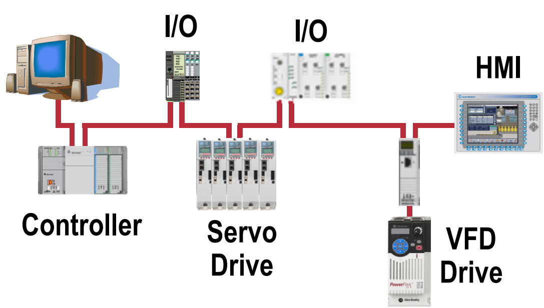
Islands of Automation with Isolated Local Area Networks (LANs)

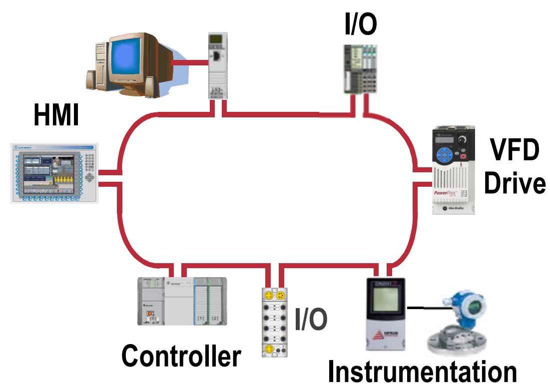
Segmentation – Network Services

Sneakernet



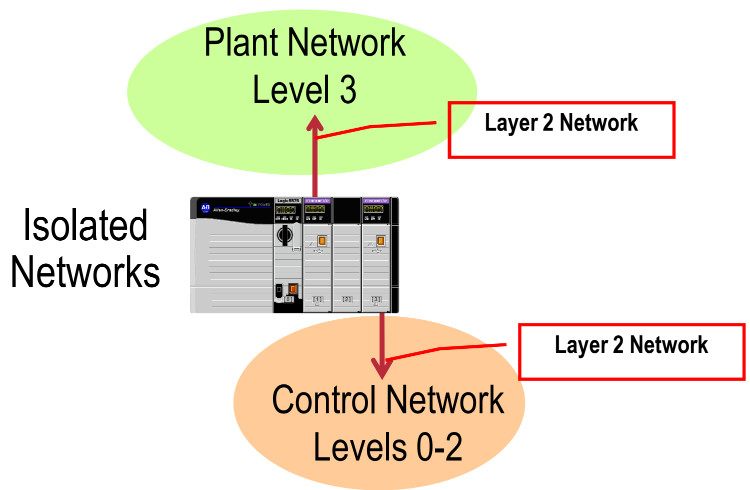


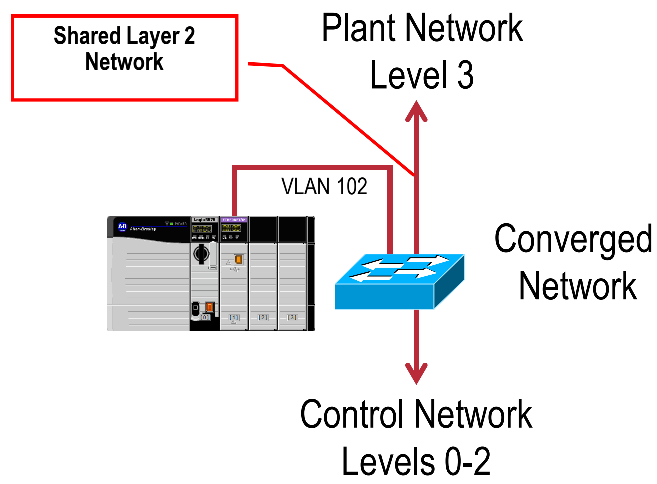




Multiple Network Interface Cards (NICs) - CIP™ Bridge

Segmentation – Network Services



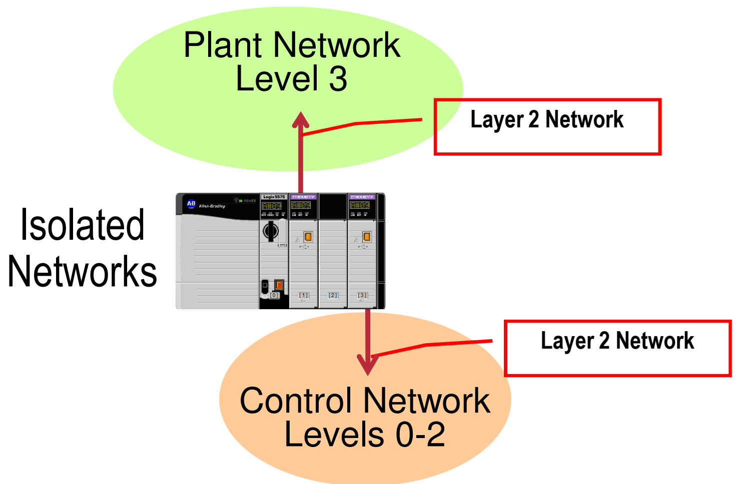


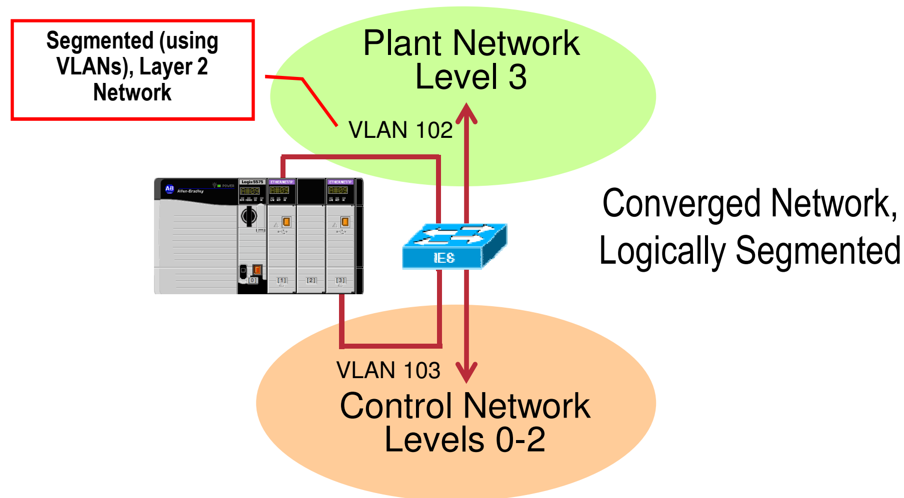
- Benefits
  - Clear network ownership demarcation line
- Challenges
  - Limited visibility to control network devices for asset management
  - Limited future-ready capability
  - Smaller PACs may not support

- 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



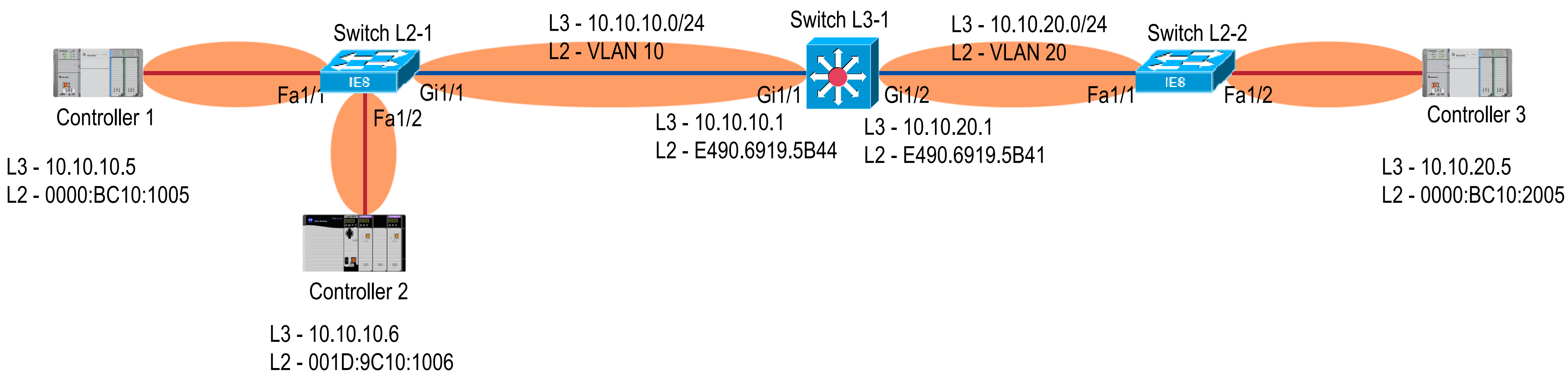


- Benefits
  - Clear network ownership demarcation line
- Challenges
  - Limited visibility to control network devices for asset management
  - Limited future-ready capability
  - Smaller PACs may not support

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

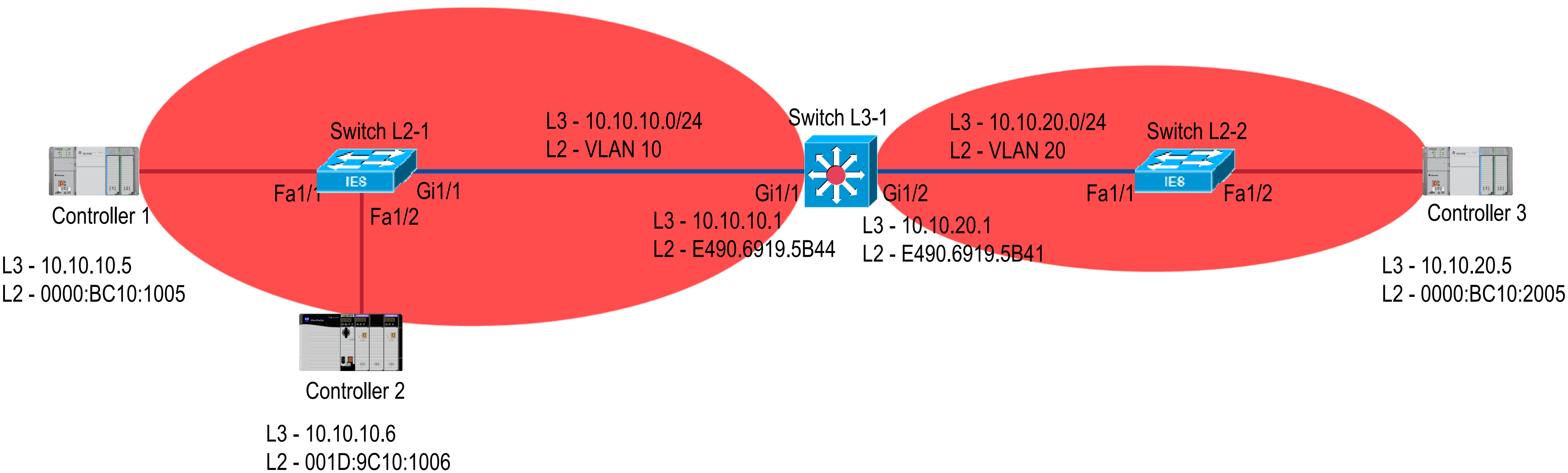
Layer 2 Collision Domains

Segmentation – Network Services



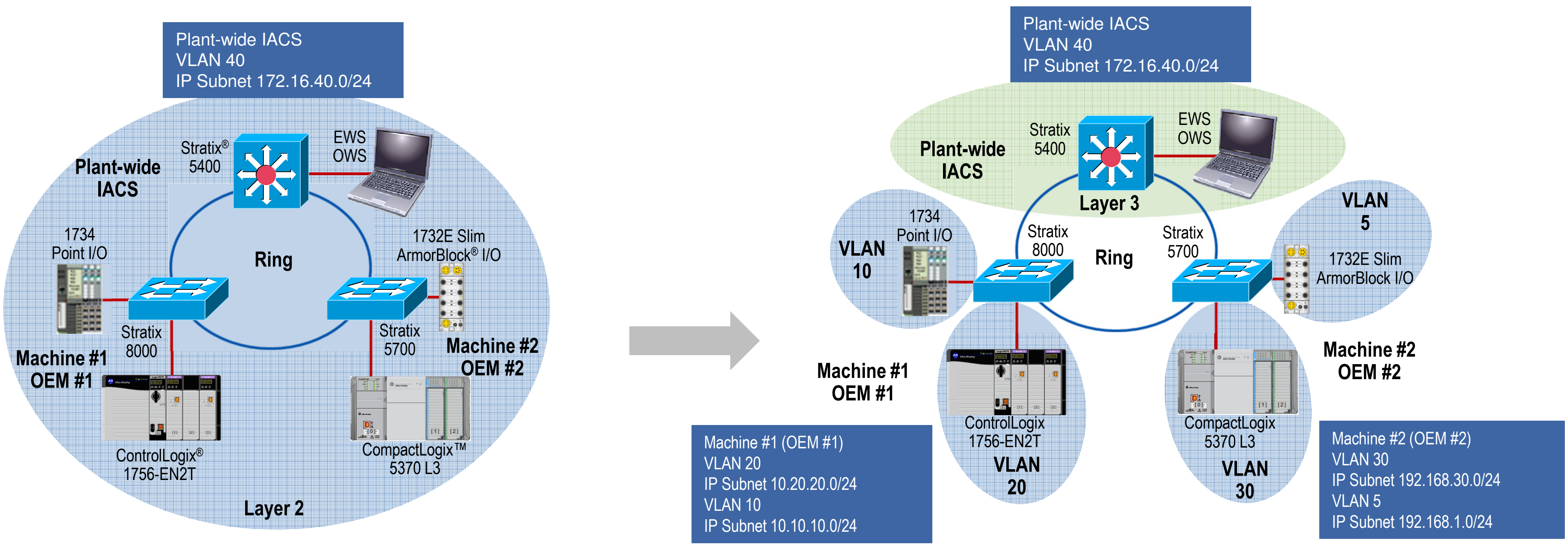
Layer 2 Broadcast Domains - Switch Hierarchy

Segmentation – Network Services



Switch Hierarchy, Virtual LANs (VLANs)

Segmentation – Network Services



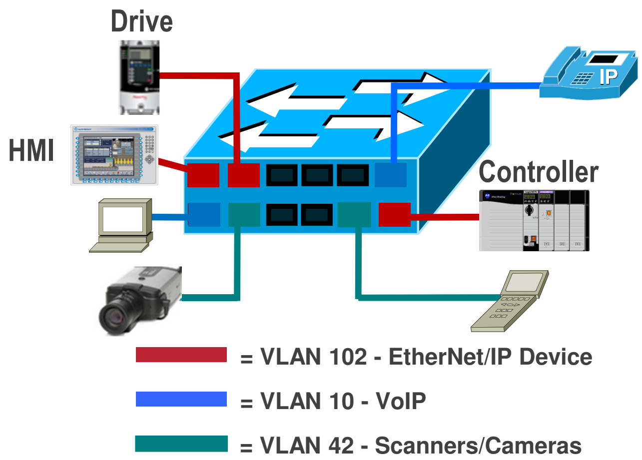
Large Flat LAN
Larger Layer 2 Broadcast Domain

Small Connected LANs
Smaller Layer 2 Broadcast Domains

Virtual Local Area Networks (VLANs)

Segmentation – Network Services

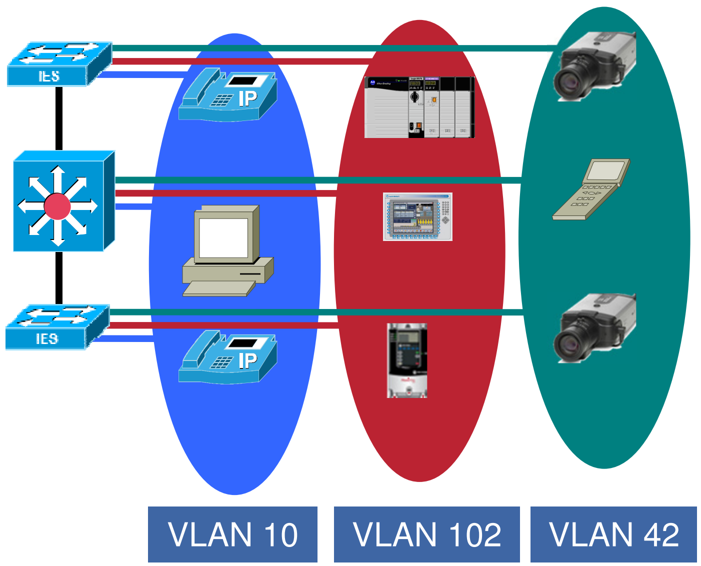
- Layer 2 network service, VLANs segment a network logically without being restricted by physical connections
  - VLAN established within or across switches
- Data is only forwarded to ports within the same VLAN
  - Devices within each VLAN can only communicate with other devices on the same VLAN
- Segments 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)

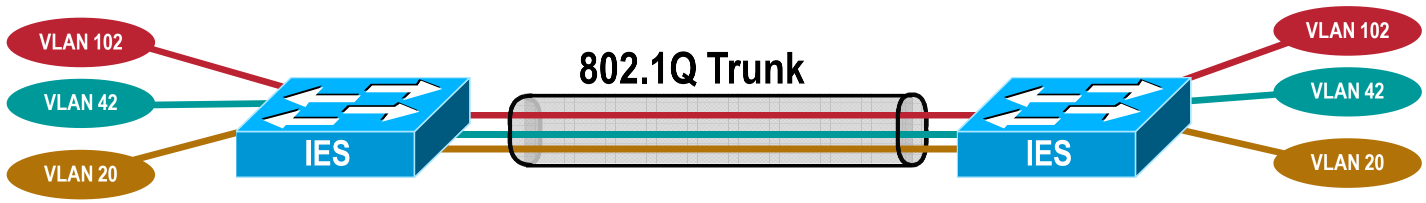
Segmentation – Network Services

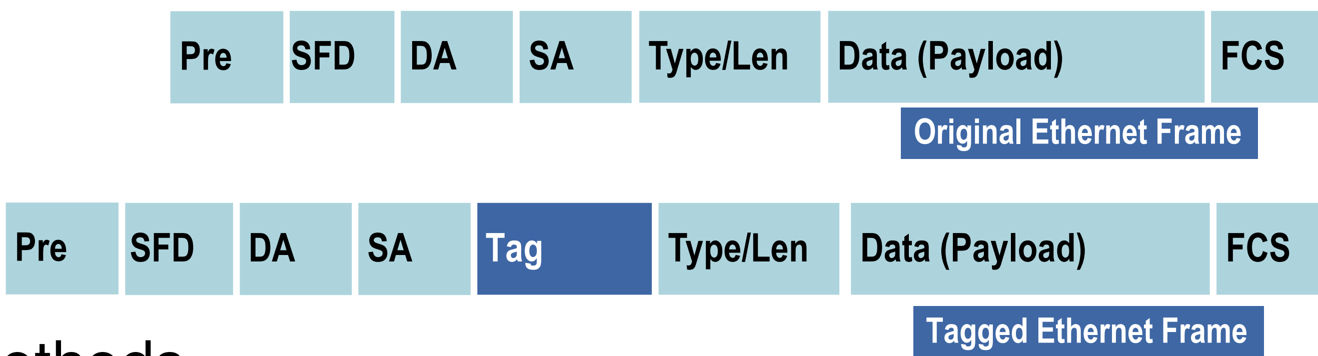
- Layer 2 VLAN Trunking
  - Independent of physical switch location
  - Logically group assets by type, role, logical area, physical area or a hybrid of these
  - Devices communicate as if they are on the same physical segment – no re-cabling required
- Software configurable using managed switches
- 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

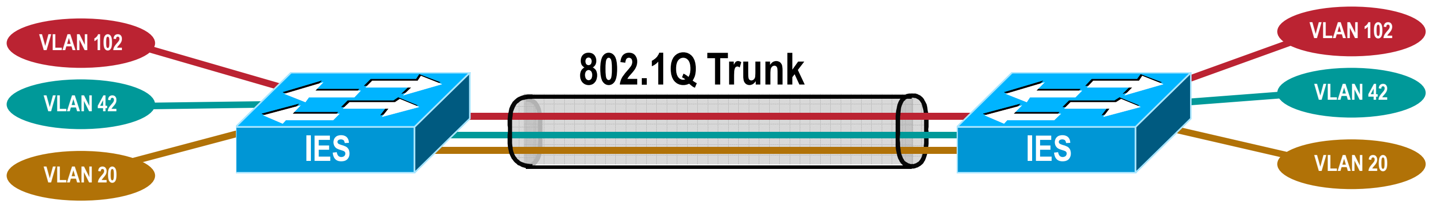




- Trunking Methods
  - IEEE 802.1Q, generally referred to as “dot1q”

Virtual Local Area Networks (VLANs)

Segmentation – Network Services

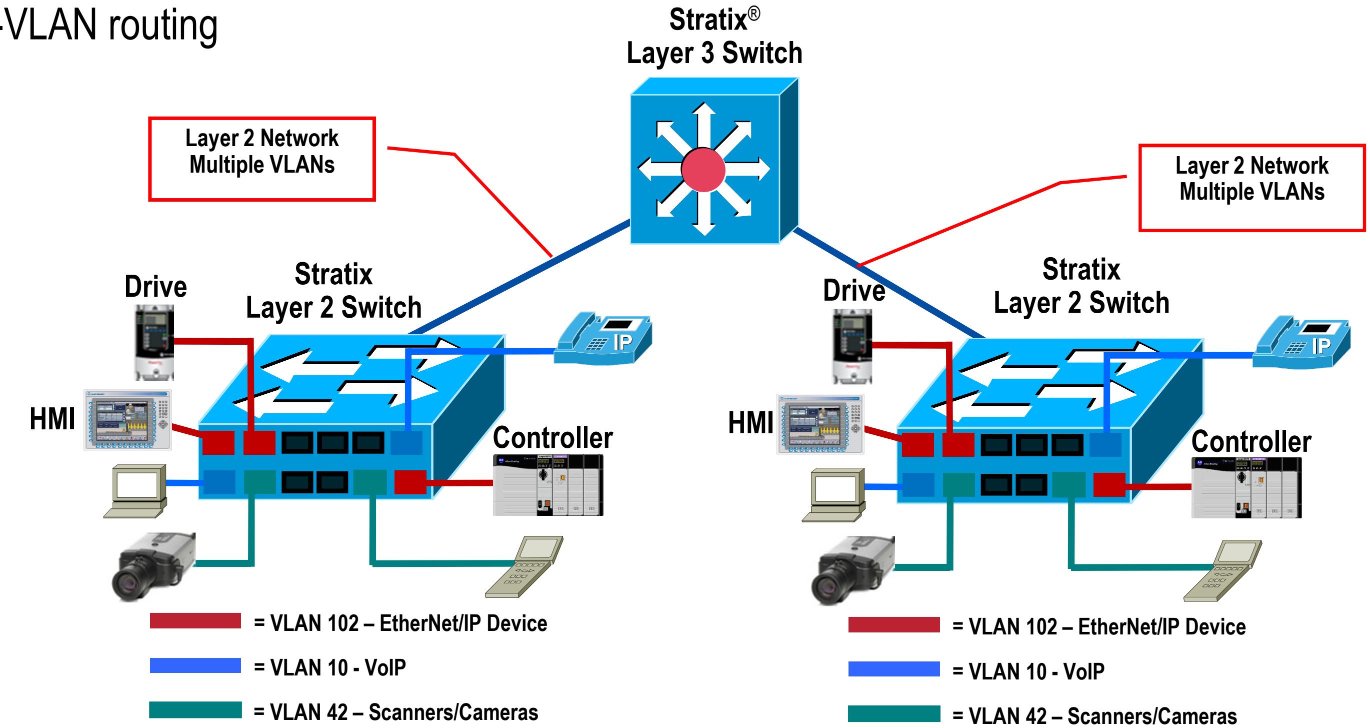


- VLAN Trunking Protocol (VTP)
  - Provides centralized VLAN management, runs only on trunks
  - Three modes:
    - Server: updates clients and servers
    - Client: receive updates - cannot make changes
    - Transparent: allow updates to pass through
- Use VTP transparent mode to decrease potential 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

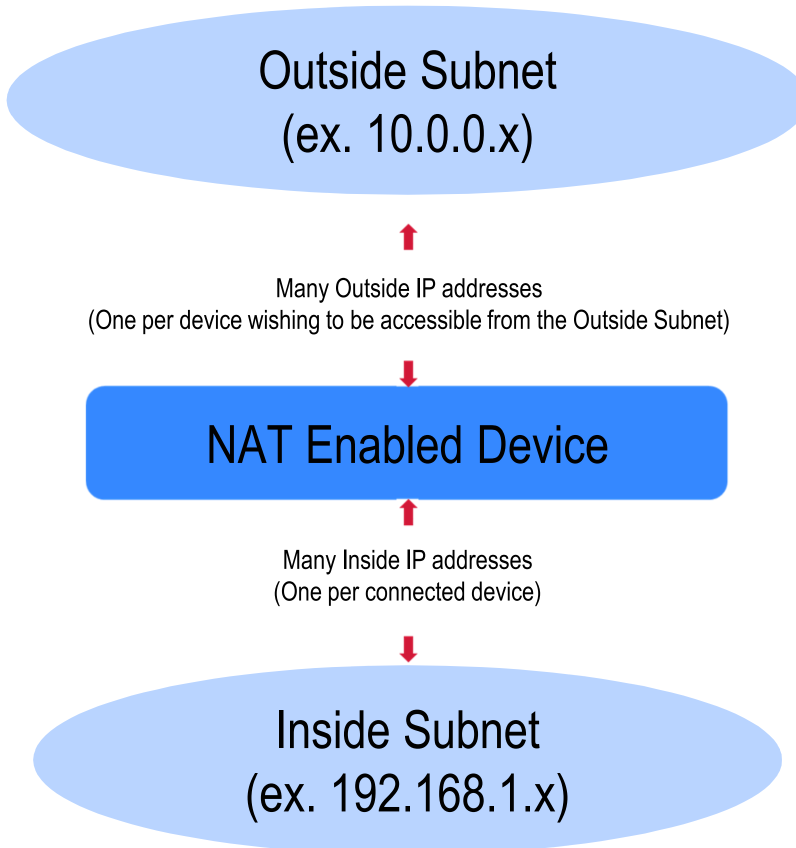
VLANs

- 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

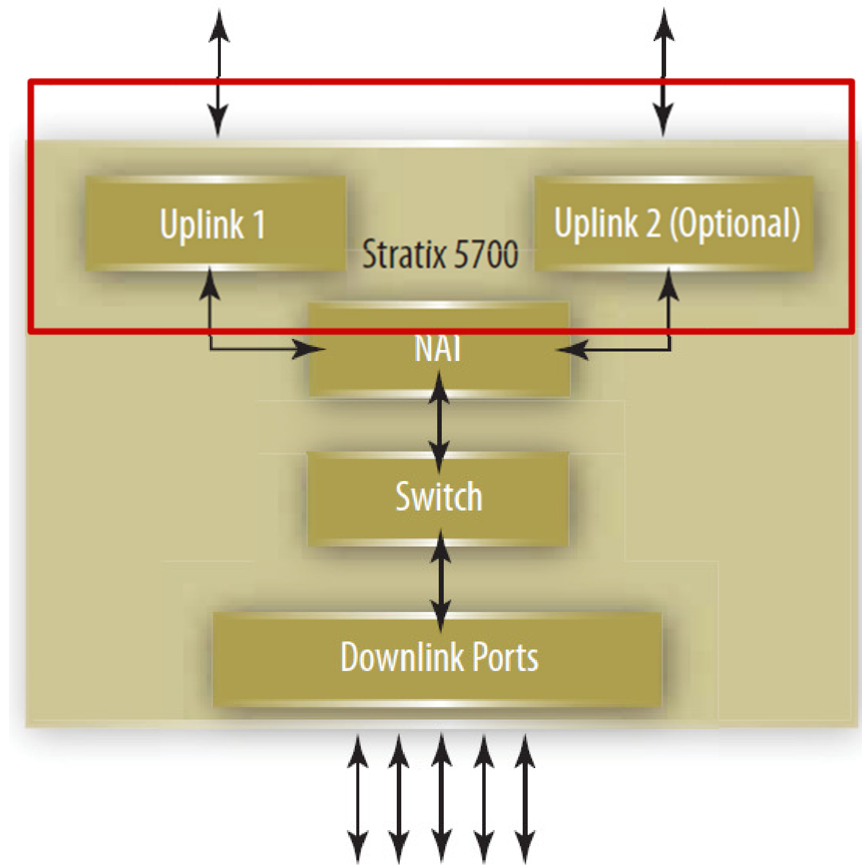


Network Address Translation (NAT) - Layer 3 Address Segmentation

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

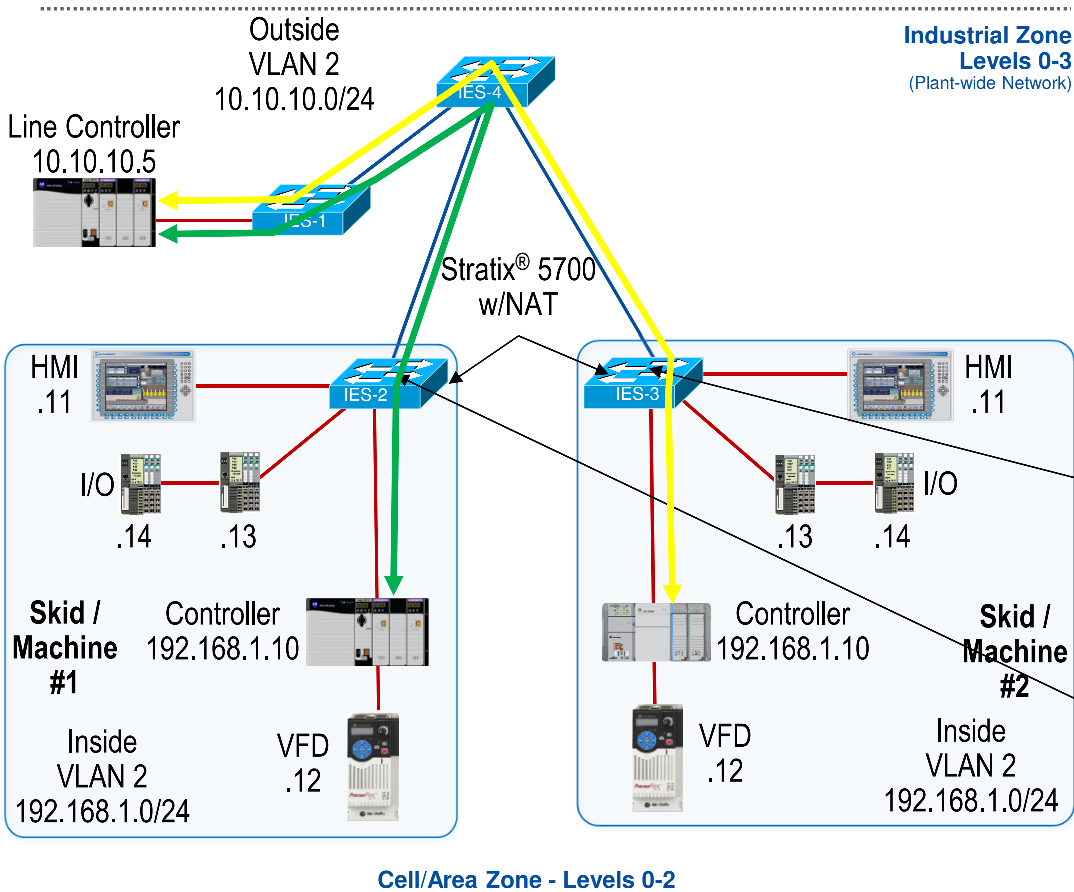
- Hardware based implementation, performance is at wire speed throughout switch loading
- NAT device does not act as a router and utilizes 2 translations tables – inside to outside & outside to inside
  - Supports multiple VLANs through NAT boundary enhancing segmentation flexibility (communication between 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

Rockwell Automation

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

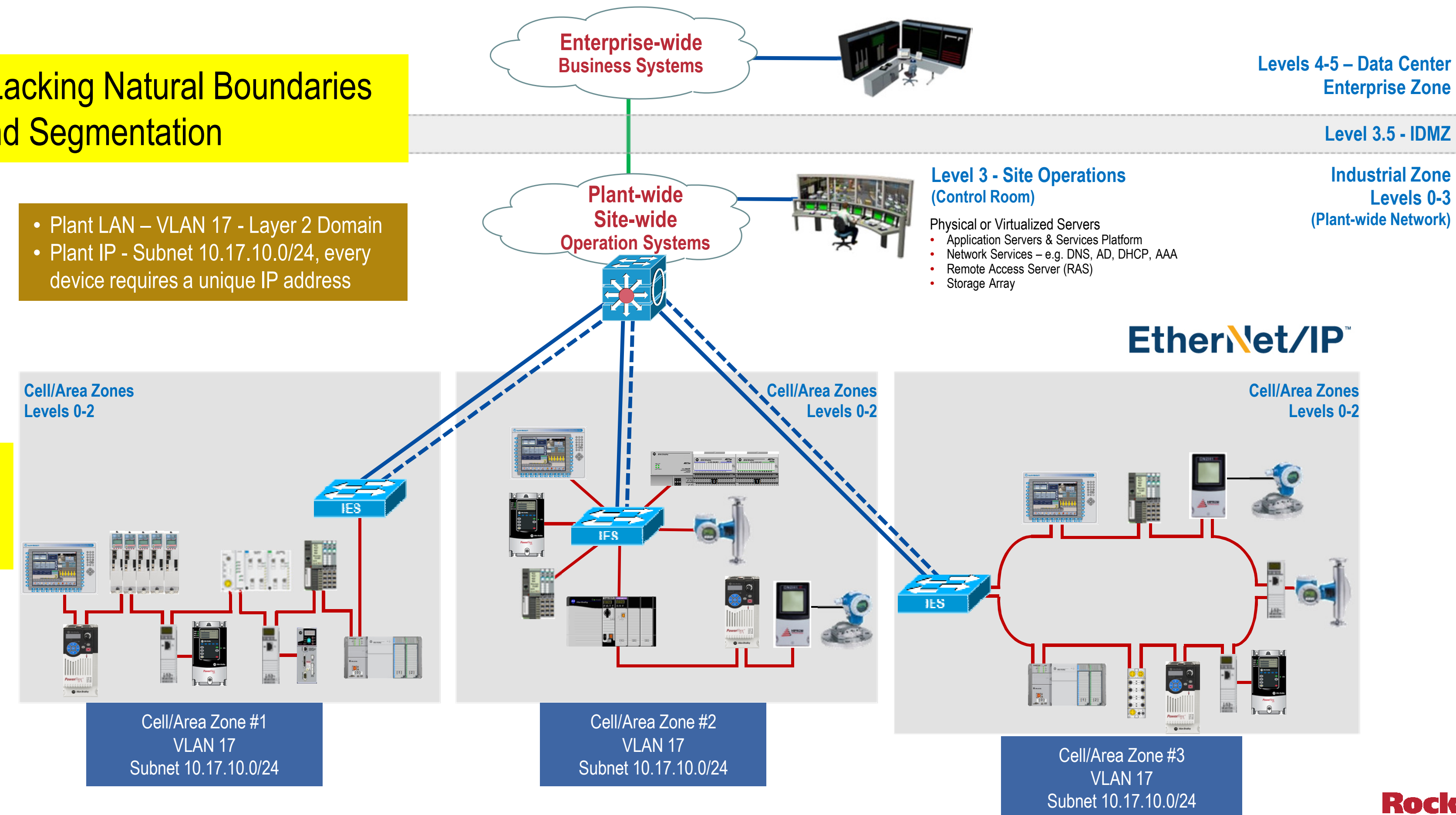
No Segmentation (not recommended)

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



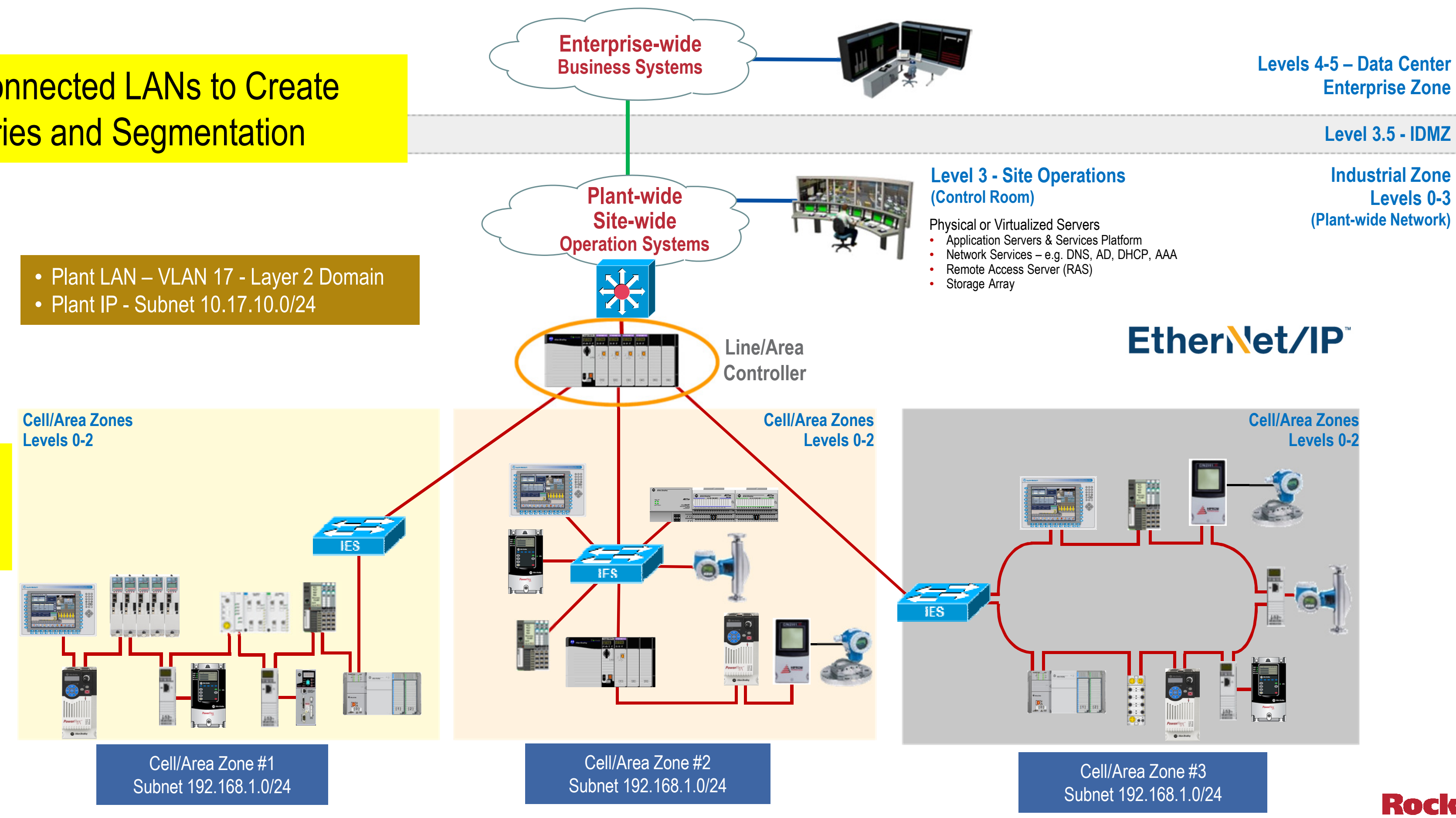
Rockwell Automation

Multiple Network Interface Cards (NICs) - CIP Bridge Segmentation

Segmentation – Network Services

Smaller Connected LANs to Create Boundaries and Segmentation

- Unique Layer 2 Broadcast Domains
- Reused IP Address Space



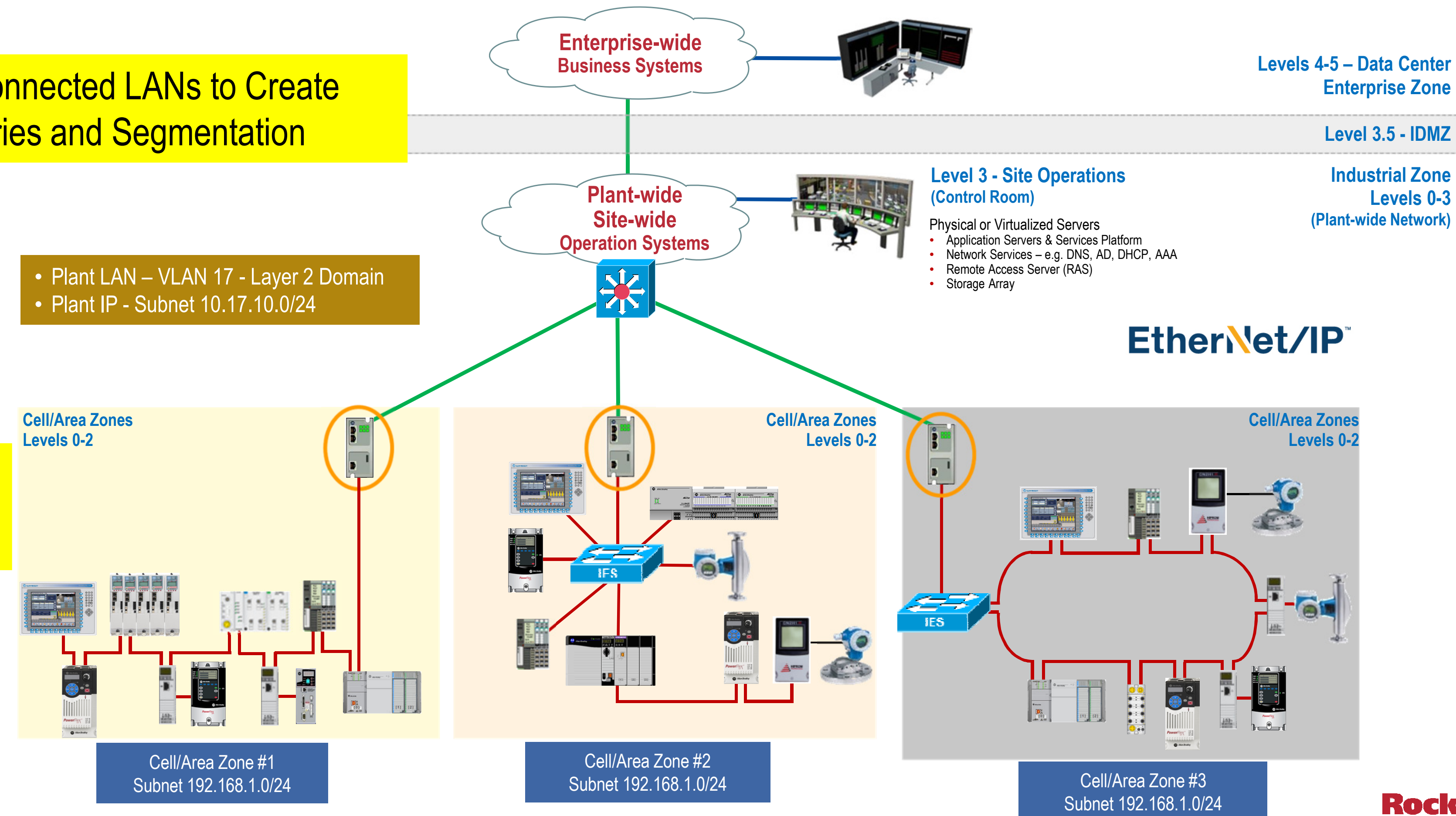
Rockwell Automation

Layer 3 NAT Appliance Segmentation

Segmentation – Network Services

Smaller Connected LANs to Create Boundaries and Segmentation

- Unique Layer 2 Broadcast Domains
- Reused IP Address Space



Rockwell Automation

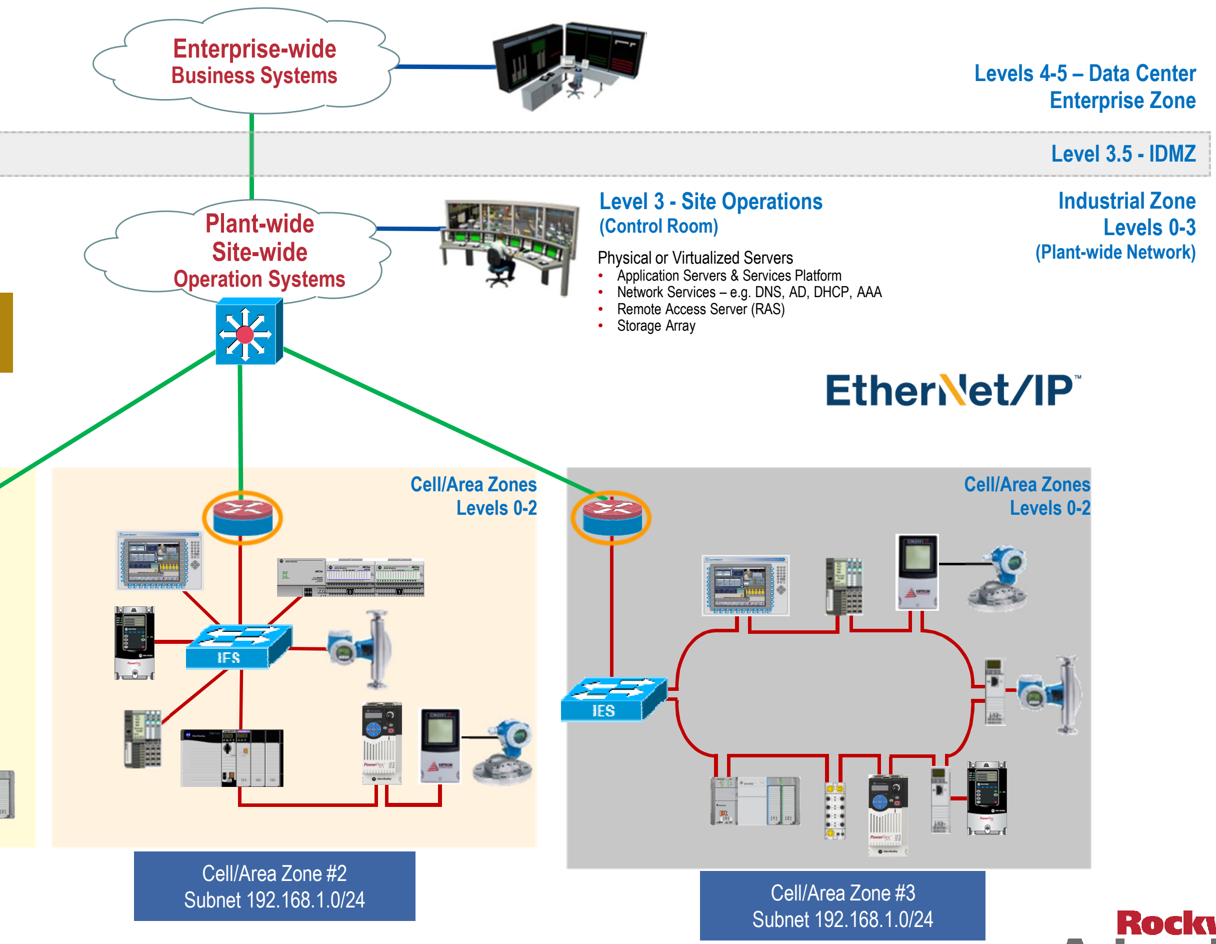
Layer 3 NAT - Integrated Services Router Segmentation

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



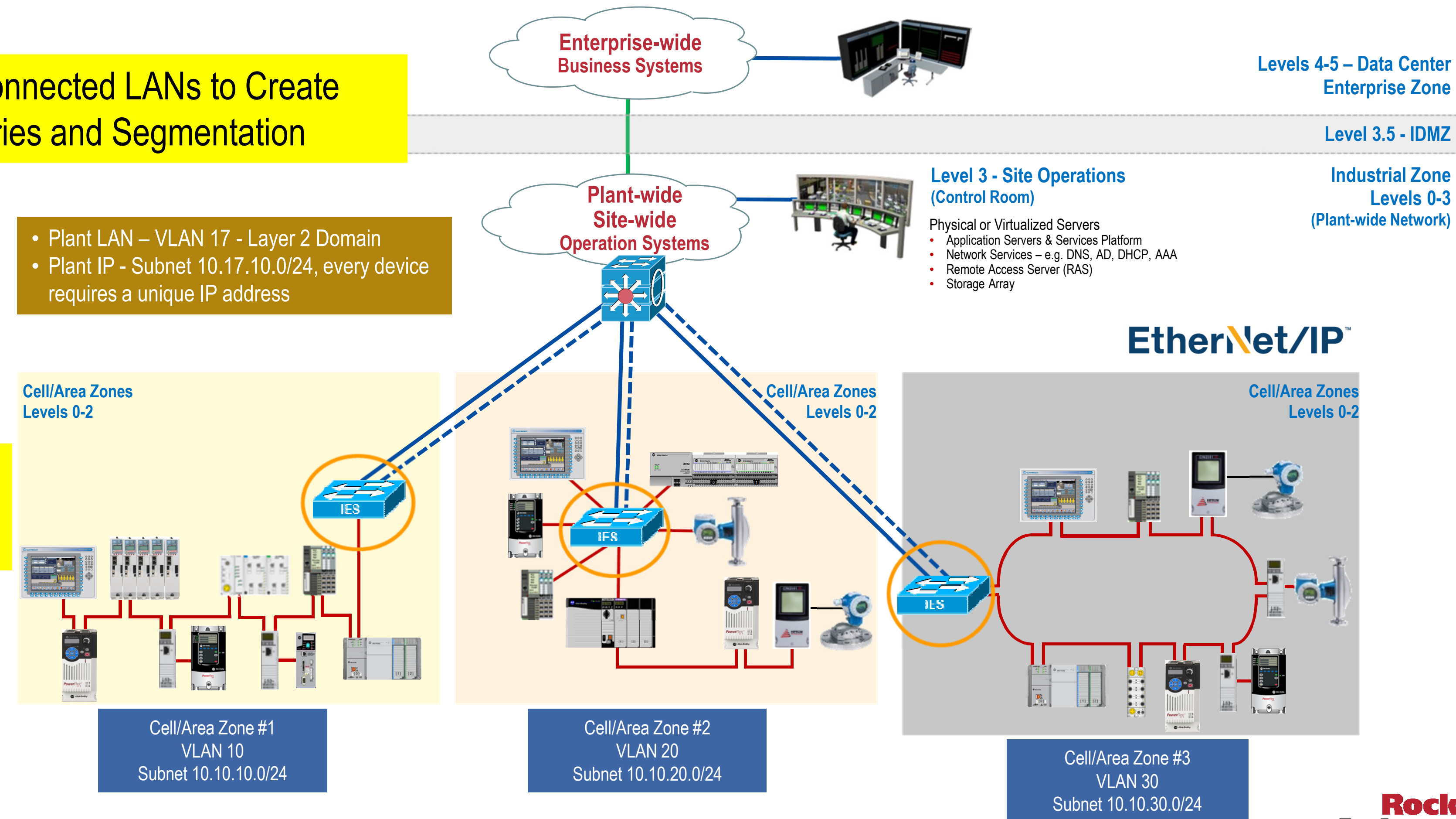
VLAN Segmentation without NAT

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, every device requires a unique IP address

- Unique Layer 2 Broadcast Domains
- Unique IP Address Space



Rockwell Automation

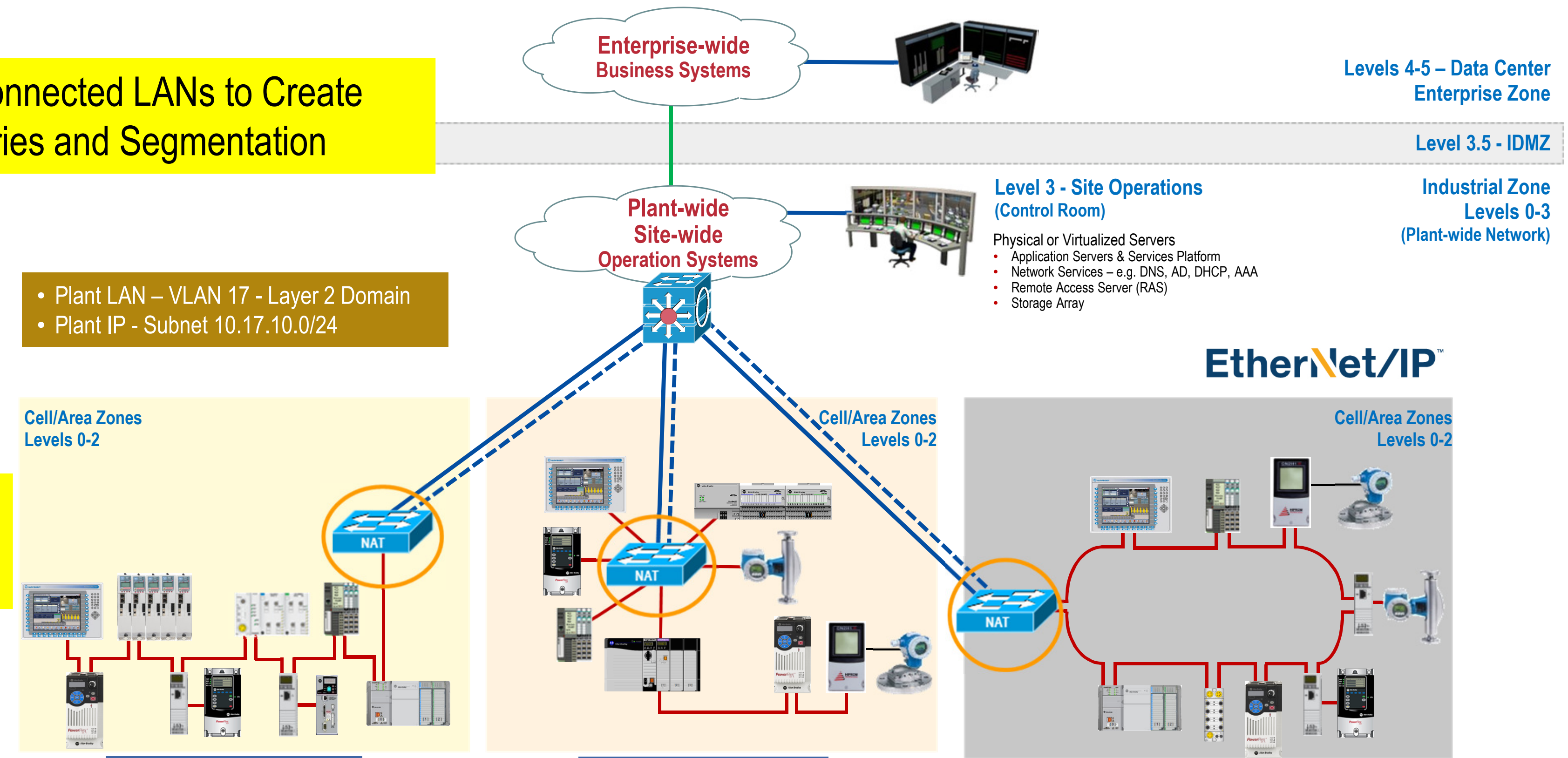
VLAN Segmentation with Layer 2 NAT

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



Cell/Area Zone #1
VLAN 10
Subnet 192.168.1.0/24

Cell/Area Zone #2
VLAN 20
Subnet 192.168.1.0/24

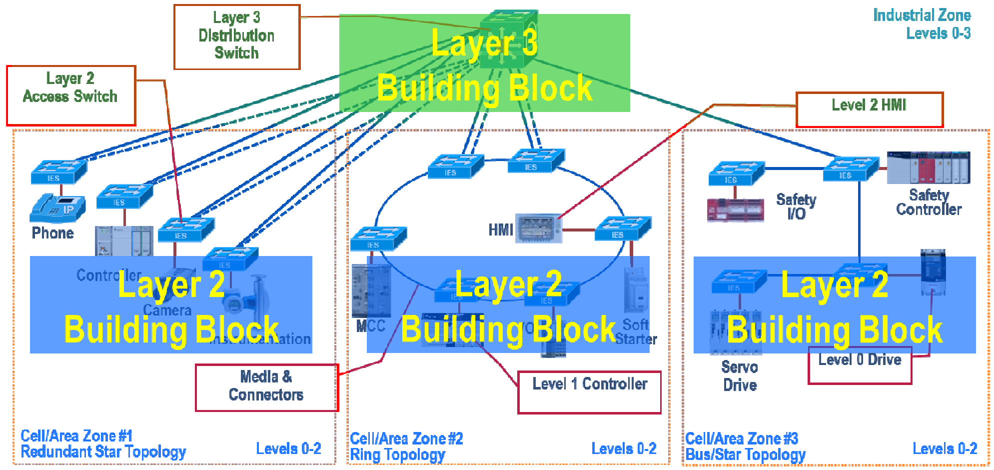
Cell/Area Zone #3
VLAN 30
Subnet 192.168.1.0/24

Rockwell Automation

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

Otázky?

Děkuji Vám za pozornost

Roman Foukal,
Commercial Engineer A&S / TÜV FS Technician #322/15
+420 724 980 366 / rfoukal@ra.rockwell.com

Děkuji za pozornost!

Connect with us.
www.rockwellautomation.com