Intelligent Motor Control

Industrial Networks Designs and Considerations

David C. Mazur, P.Eng., Ph.D. & Gregory S. Wilcox

IEEE

Speakers

Rockwell Automation

David C. Mazur, P.Eng., Ph.D.

Global Technical Consultant

David received his B.S. EE degree summa cum laude and first in his class from Virginia Polytechnic Institute and State University, Blacksburg, VA in 2011. David graduated with his M.S. EE degree in 2012 for his work based on rotor angle measurement of synchronous machines from Virginia Polytechnic Institute and State University. He graduated with his Ph.D. in Mining Engineering in September 2013 for his work with the IEC 61850 standard. He is an active member of the IEEE IAS and serves as working group chair for the Communication-Based Protection of Industrial Applications Working Group. He also serves as a member of the Mining Industry Committee (MIC) as well as the Industrial and Commercial Power Systems Committee (I&CPS). David is also an active voting member of the IEEE Standards Association (SA).

Rockwell Automation

Gregory Wilcox

Development Manager for Reference Architectures

Gregory leads a multi-company effort to establish tested and validated design guidelines that helps to reduce risk, simplify design and speed deployment of large-scale industrial automation network infrastructures. As a major contributor to the Cisco and Rockwell Automation Alliance, Gregory has advanced the adoption of convergence between industrial automation technology (IAT) and information technology (IT). Gregory has been designing and implementing industrial automation network solutions for the past 28 years, with 24 of those years at Rockwell Automation, holding roles of increasing responsibility such as Application Engineer and Solution Architect, resulting in extensive experience in developing control and information solutions for industrial applications. Prior to joining Rockwell Automation, Gregory worked in the defense industry developing industrial automation and control system solutions for both discrete and process applications.

IEEE

Agenda

IEEE

Agenda

IEEE

Industrial Networks Trends

- Open networks are in demand
  - Broad availability of products, applications and vendor support for Industrial Automation and Control System (IACS)
  - Network standards for coexistence and interoperability of industrial automation devices
- Convergence of network technologies
  - Reduce the number of disparate networks in an operation and create seamless information sharing throughout the plant-wide / site-wide architecture
  - Use of common network design, deployment and troubleshooting tools across the plant-wide / site-wide architecture; avoid special tools for each application

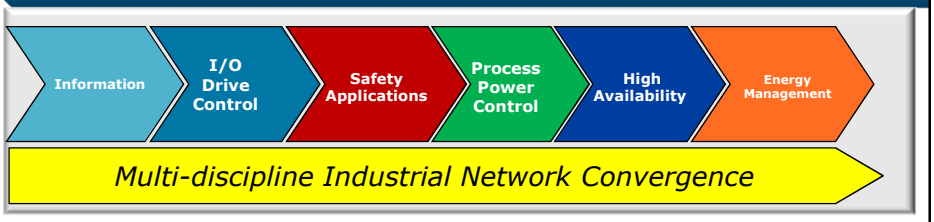
IEEE

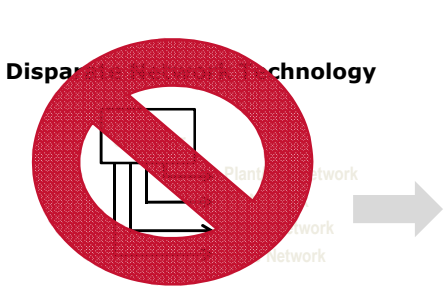
Industrial Networks Trends

- Better asset utilization to support lean initiatives
  - Common network infrastructure assets, while accounting for environmental requirements
  - Reduce training, support, and inventory for different networking technologies
- Future-ready – maximizing investments and minimizing risks
  - Support new technologies and features without a network forklift upgrade

IEEE

Industrial Applications Convergence



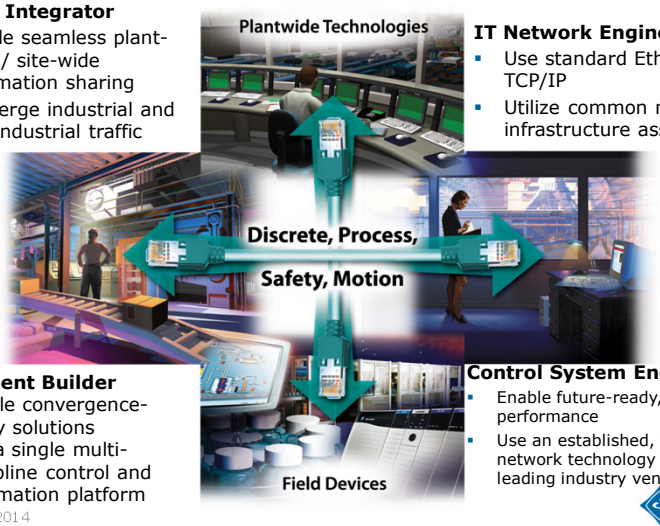


7 2/10/2014

Industrial Network Technology should service…

System Integrator
- Enable seamless plant-wide / site-wide information sharing
- Converge industrial and non-industrial traffic

IT Network Engineer
- Use standard Ethernet and TCP/IP
- Utilize common network infrastructure assets & tools

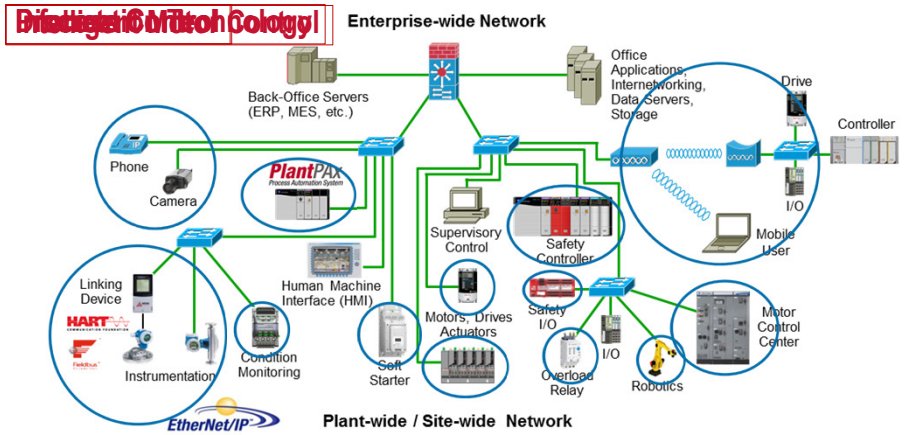


Equipment Builder
- Enable convergence-ready solutions
- Use a single multi-discipline control and information platform

Control System Engineer
- Enable future-ready, high performance
- Use an established, widely accepted network technology supported by leading industry vendors

8 2/10/2014

Network Technology Convergence



IEEE

Industrial Network Design Methodology

- Understand application and functional requirements
  - Devices to be connected – industrial and non-industrial
  - Data requirements for availability, integrity and confidentiality
  - Commu
  - Types o
    drive co
- Develop
  - **Migrate**
  - Define z
    in the lo
- Develop
  with and support the logical framework
- Deploy a Defense-in-Depth Security Model
- Reduce risk, simplify design, and speed deployment:
  - Use information technology (IT) standards
  - Follow industrial automation technology (IAT) standards
  - Utilize reference models and reference architectures

Because Network Infrastructure Matters

IEEE

Cabling Benefits

- UL / cUL listed for use with high voltage power cables
  - 600V cable designed to support high voltage applications
  - UL rated for use in Power Limited Trays
- Provides reliable network connection in harsh conditions
  - Protected from noise, chemicals, thermal and mechanical issues for the harshest possible industrial environments (M3I3C3E3 rated)
  - Foil and braided shield for maximum noise immunity
  - Wide thermal operational range (-20C … 80C)
- Cat 5e cable enables high speed data rate
  - More data can be transferred in a shorter period of time
- Copper cabling standard but fiber can be used for longer runs

IEEE

Embedded Systems – Rugged Industrial Design

Lightning Strike

- +/- 2KV, 40A surge repeatedly applied to the network cable
- IEC 61000-4-5

Industrial Noise

- +/- 1KV high voltage burst applied to the network cable
- IEC 61000-4-4

No Communication Failures!
No Dropped Packets!
Less Down Time!

Radio Frequency Interference

- 150kHz … 80MHz interference applied to the network cable
- IEC 61000-4-6

Static Discharge

- +/- 8KV ESD event at 12 locations on the MCC and network cable
- IEC 61000-4-2

IEEE

Network Design Considerations

Recommendations and guidance to help reduce **Latency** and **Jitter**, to help increase data **Availability**, **Integrity** and **Confidentiality,** and to help design and deploy a **Scalable**, **Robust**, **Secure** and **Future-Ready** network infrastructure

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation
- Resiliency Protocols and Redundant Topologies
- Time Synchronization
- Prioritization - Quality of Service (QoS)
- Multicast Management
- Convergence-Ready Solutions
- Security - Defense-in-Depth
- Scalable Secure Remote Access

IEEE

Integrated Architecture

Plant-wide Optimization

Machine Builder Performance

IEEE

Ethernet/IP: The Industrial Protocol

- ODVA
  - Supported by global industry leaders such as Cisco System
    Omron®, Schneider Electric®, Bosch Rexroth AG®,
    Endress+Hauser and Rockwell Automation
  - Conformance & Performance Testing
- Standard
  - IE… ol (IEEE-1588)
  - IE… net Protocol (IP)
  - O…
  - IE… C 61158
- IT I… ble)
- Multi-discipline control and information platfc
- Established - products, applications and venc

www.odva.org

What's the difference?

- Ethernet IP
- EtherNet/IP

OSI 7-Layer Reference Model

Open Systems Interconnection

What makes EtherNet/IP industrial?

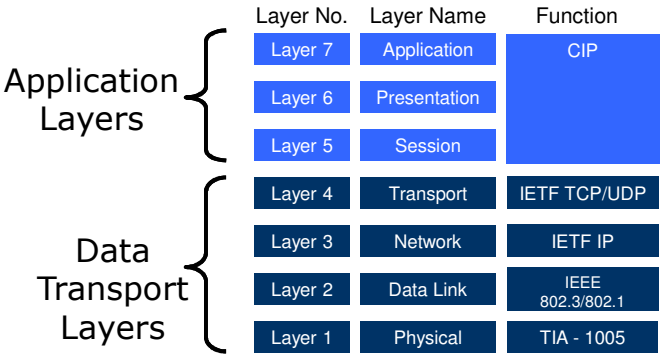
Layer Name	Layer No.	Function	Examples
Application	Layer 7	Network Services to User App	CIP IEC 61158
Presentation	Layer 6	Encryption/Other processing	
Session	Layer 5	Manage Multiple Applications	
Transport	Layer 4	Reliable End-to-End Delivery Error Correction	IETF TCP/UDP
Network	Layer 3	Packet Delivery,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

Physical Layer Hardening | Infrastructure Device Hardening | Common Application Layer Protocol

5-Layer TCP/IP Model

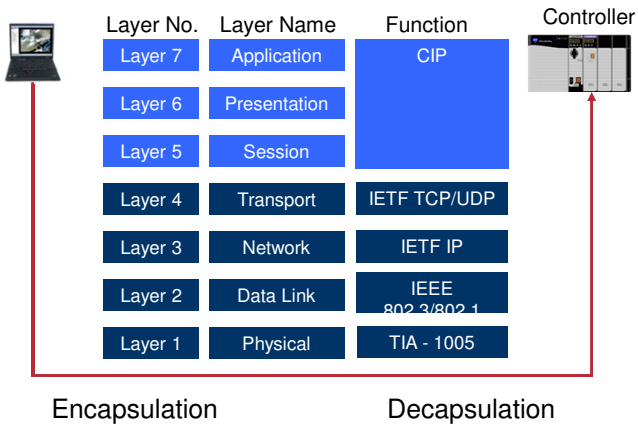
16

OSI Reference Model



IEEE

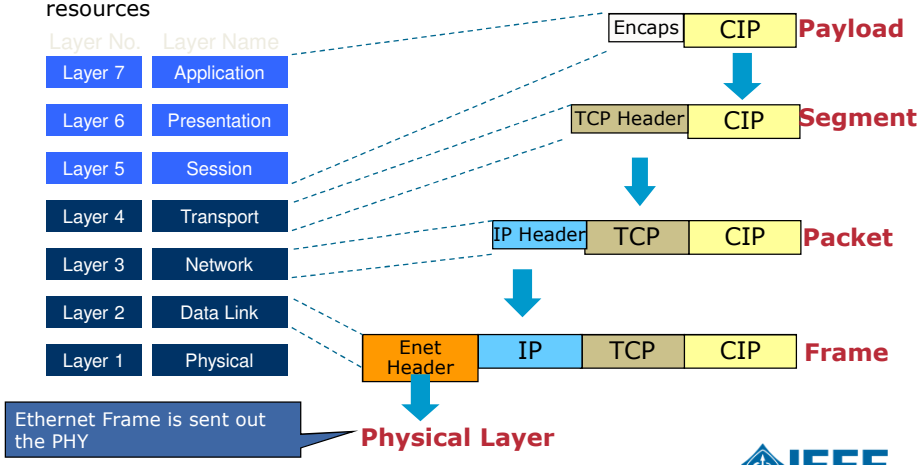
Protocol Stack



IEEE

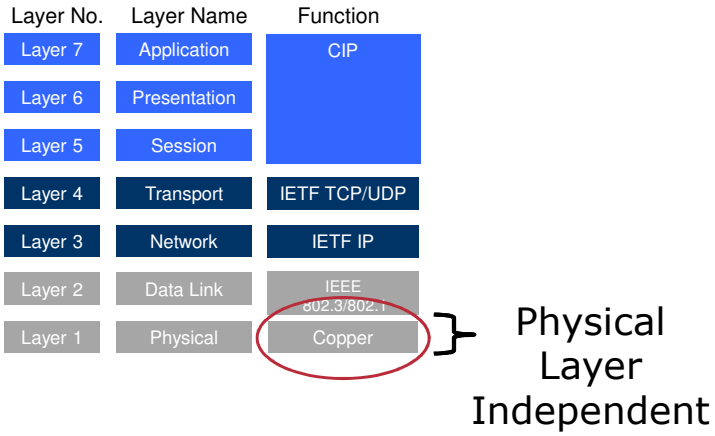
Encapsulation Example

- The Ethernet message structure is a concatenation of protocols
  - EtherNet/IP defines an Encapsulation protocol that sets up the TCP resources



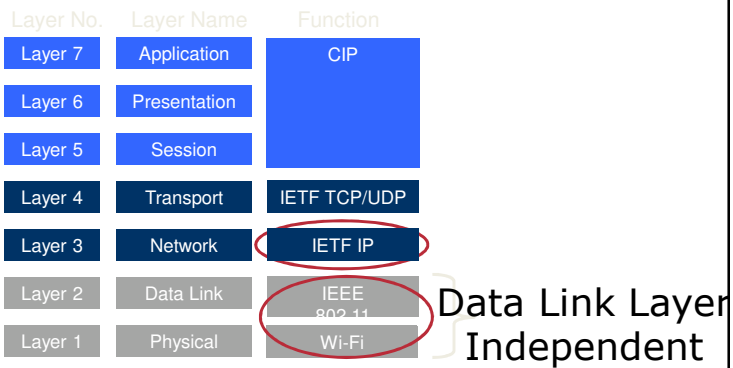
IEEE

OSI Model: Physical Layer Independent



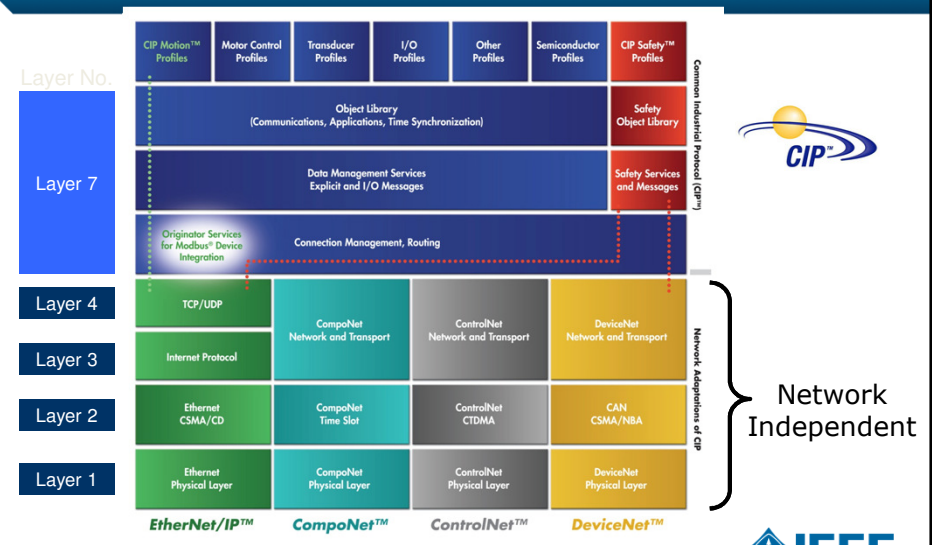
IEEE

OSI Model: Data Link Layer Independent



IEEE

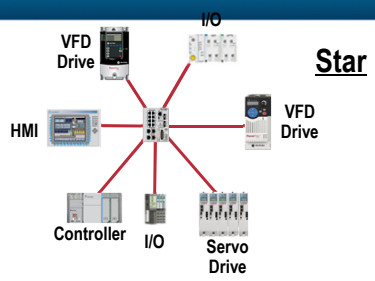
OSI Reference Model: Network Independent



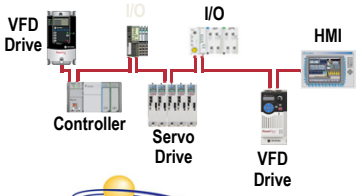
IEEE

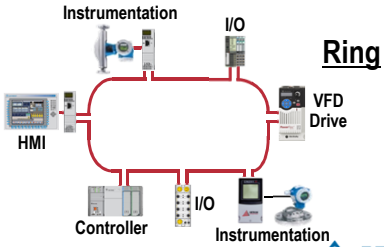
Network Architectures

- Isolated Network with Single Controller (ODVA)
- Examples
  - Equipment Builder Solution (Machine or Process Skid)



Linear





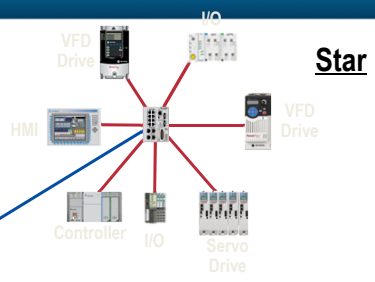
EtherNet/IP

IEEE

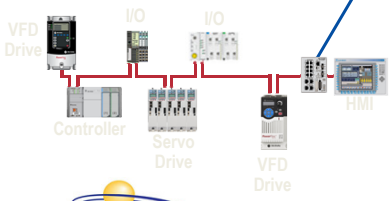
23 2/10/2014

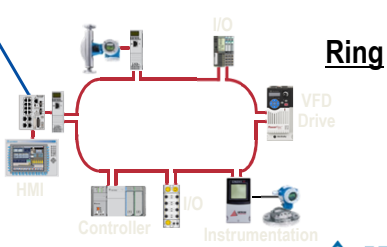
Network Architectures

- Isolated Network with Multiple Controllers (ODVA)
- Examples
  - Integrated Equipment Builder Solutions
  - Single Cell/Area Zone, Multiple Machines/Lines or Skids/Areas



Linear





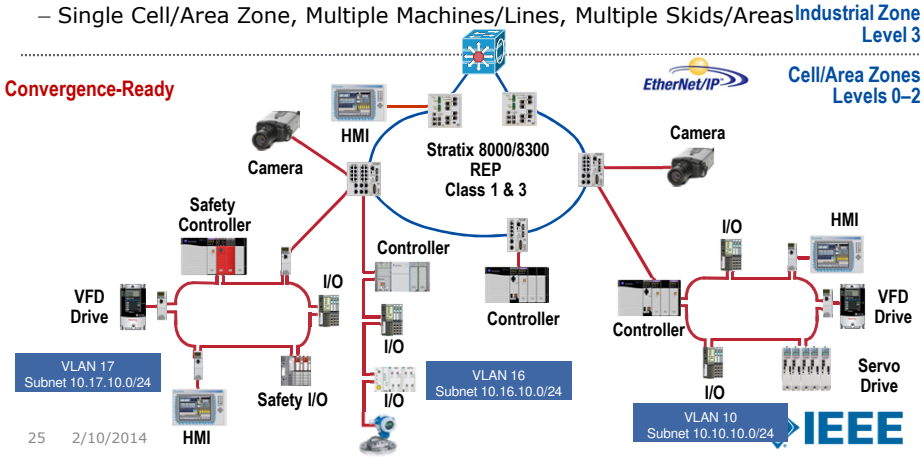
EtherNet/IP

IEEE

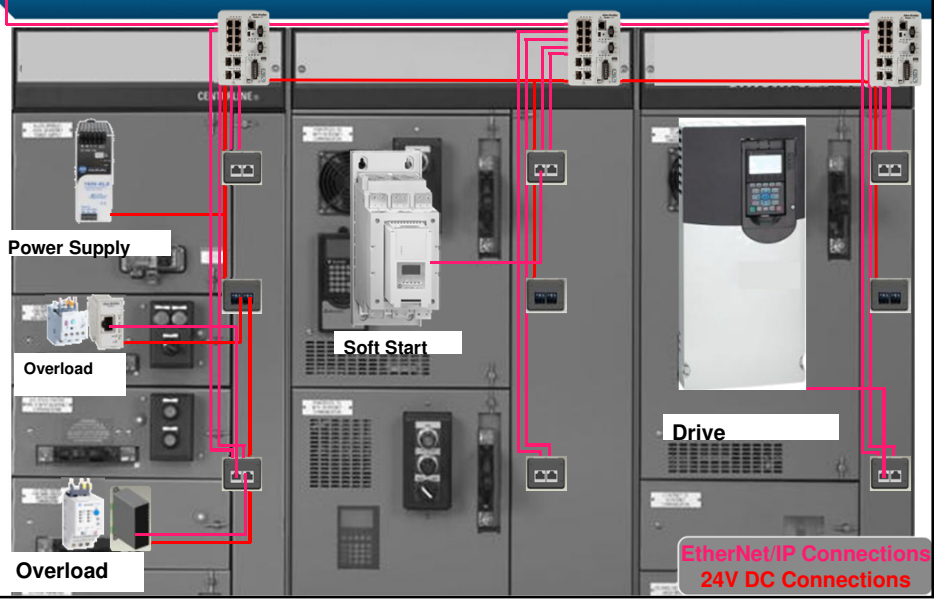
24 2/10/2014

Network Architectures

- Connected and Integrated Control System (ODVA)
- Examples
  - Integrated Equipment Builder Solutions or End User Plant-wide / Site-wide Network
  - Single Cell/Area Zone, Multiple Machines/Lines, Multiple Skids/Areas

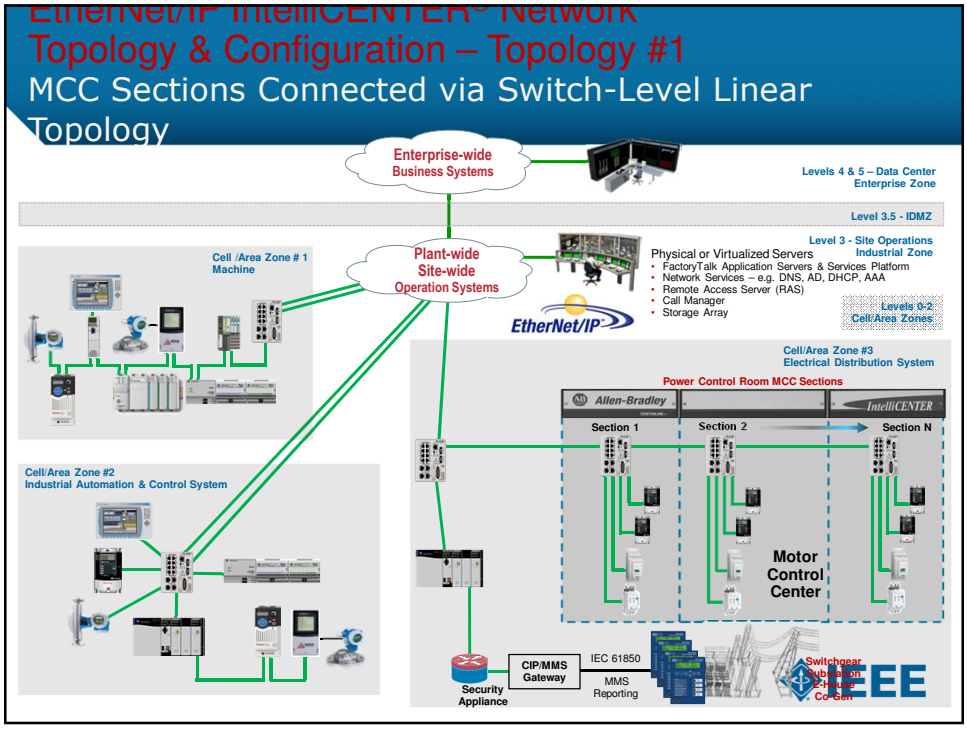


Topology Layouts



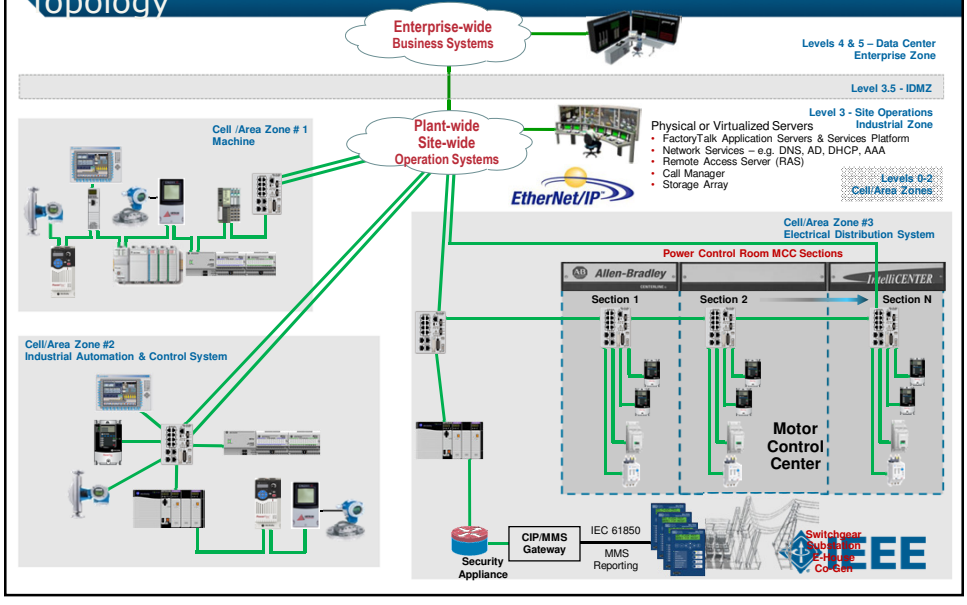
EtherNet/IP IntelliCENTER® Network Topology & Configuration – Topology #1

MCC Sections Connected via Switch-Level Linear Topology

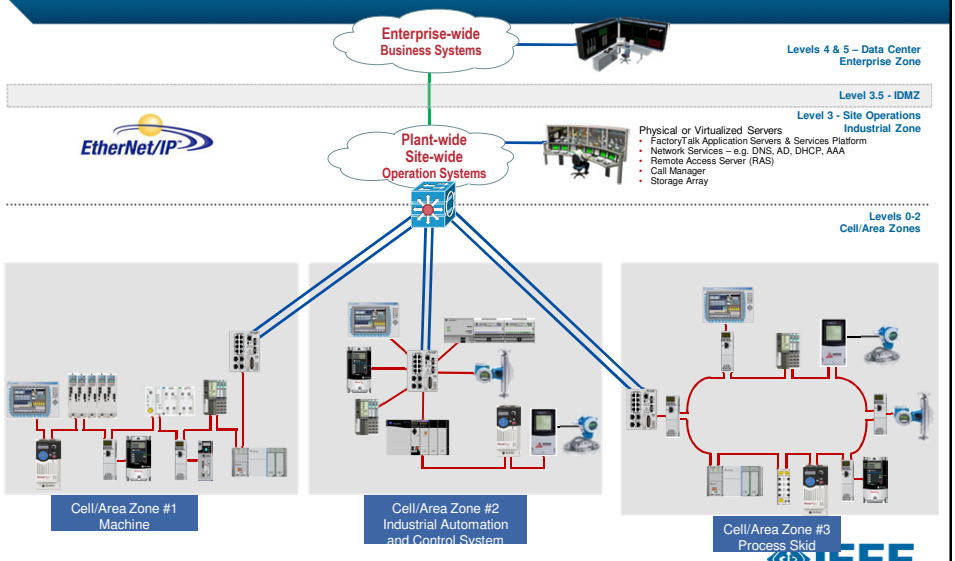


EtherNet/IP IntelliCENTER® Network Topology & Configuration – Topology #2

MCC Sections Connected via Switch-Level Ring Topology



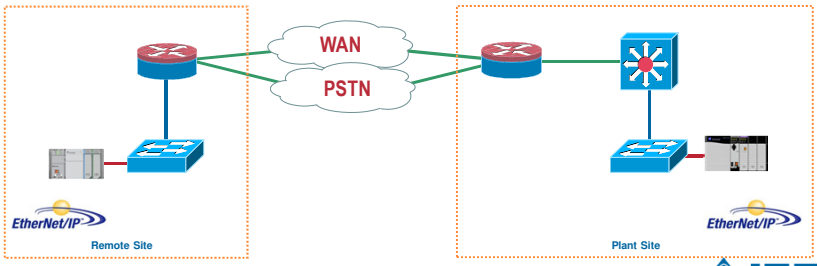
Network Architectures



IEEE

Network Architectures: Site-to-Site Connection

- Broad geographic area
  - WAN Examples:
    - Point-to-Point Link – PSTN Leased Lines – T1, E1
    - Circuit Switching - ISDN
    - Packet Switching - Frame Relay, Broadband DSL, Broadband Cable
  - Higher Latency
    - Use case examples – HMI and Data Collection



IEEE

Benefits of Ethernet/IP

- Single industrial network technology for:
  - Multi-discipline Network Convergence - Discrete, Continuous Process, Batch, Drive, Safety, Motion, Power, Time Synchronization, Supervisory Information, Asset Configuration/Diagnostics, and Energy Management
- Established – 375+ vendors, over 7,500,000 nodes
  - Risk reduction – broad availability of products, applications and vendor support
  - ODVA: Cisco Systems, Endress+Hauser, Rockwell Automation are principal members
  - Supported – Defined QoS priority values for EtherNet/IP devices

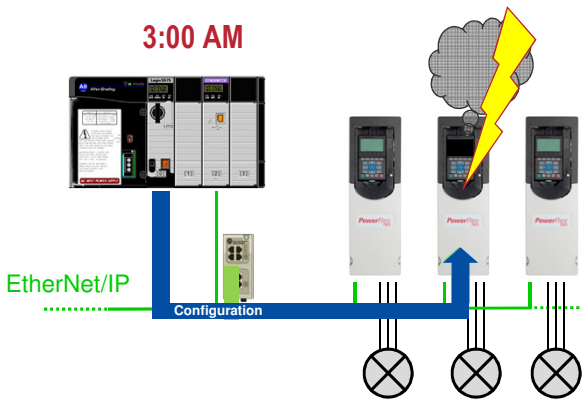
IEEE

Benefits of EtherNet/IP

- Standard – IEEE 802.3 Ethernet and IETF TCP/IP Protocol Suite
  - Enables convergence of IAT and IT – voice, video and data - 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
- Common industrial application layer protocol
  - DeviceNet, ControlNet and EtherNet/IP - seamless bridging throughout CIP networks

IEEE

Automatic Device Configuration



Saves the End-User time / money by reducing down-time

33

Intelligent Motor Control

Real Time Network Design and Segmentation

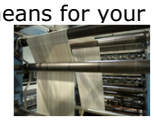
David C. Mazur, P.Eng., Ph.D. & Gregory S. Wilcox

IEEE

Application Requirements

- What is real-time?
  - Application dependent ….. only you can define what this means for your application.





Function	Information Integration, Slower Process Automation	Time-critical Discrete Automation	Motion Control
Communication Technology	.Net, DCOM, TCP/IP	Industrial Protocols - CIP	Hardware and Software solutions, e.g. CIP Motion, PTP
Period	10 ms to 1000 ms	1 ms to 100 ms	100 µs to 10 ms
Industries	Oil & gas, chemicals, energy, water	Auto, food & beverage, semiconductor, metals, pharmaceutical	Subset of discrete automation
Applications	Pumps, compressors, mixers, instrumentation	Material handling, filling, labeling, palletizing, packaging	Printing presses, wire drawing, web making, pick & place

Source: ARC Advisory Group

IEEE

Network Technology Convergence

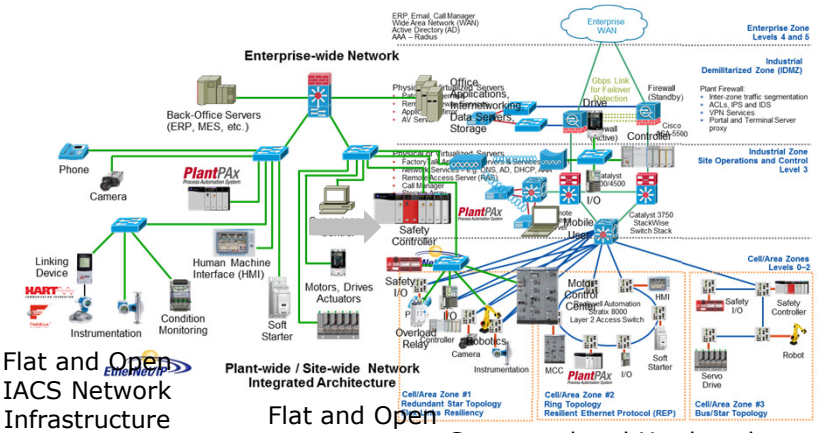
- Theoretical Ethernet @ 100 Mbps
  - Short frame with 64 bytes (1 bit – 10ns) ≈ 148,000 frames/second
  - Long frames with 1518 bytes ≈ 8,000 frames/second
- Theoretical EtherNet/IP @ 100 Mbps
  - Typical I/O frame size (64 byte + 36 byte I/O data) ≈ 104,000 frames/second
  - Maximum I/O frame size (64 byte + 511 byte I/O data) ≈ 21,000 frames/second
    - Normal CIP Forward_Open
- I/O Scanner exchanges 36 bytes of I/O data with 10 I/O adapters every 1 ms
  - The I/O Scanner must be able to:
    - Consume 10,000 frames/second
    - Product 10,000 frames/second

Design considerations you should consider

- Performance of Scanner
  - Maximum # of Adapters (CIP Connections)
  - Minimum RPI (how fast)
  - Maximum I/O Data Size per RPI
- Performance of Adapters
  - Minimum RPI (how fast)
  - Maximum I/O Data Size per RPI
- Network Infrastructure Latency and Jitter
- Speed / Duplex
- Physical Environment – e.g. EMI Interference

This represents about 10% of the total network bandwidth

Segmentation



Flat and Open IACS Network Infrastructure

Flat and Open IACS Network Infrastructure

Structured and Hardened IACS Network Infrastructure

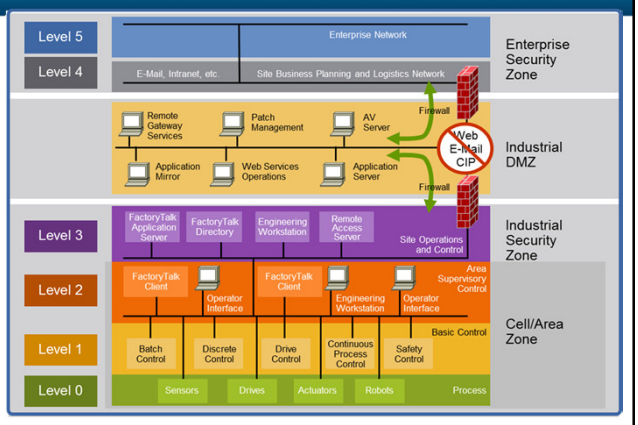
IEEE

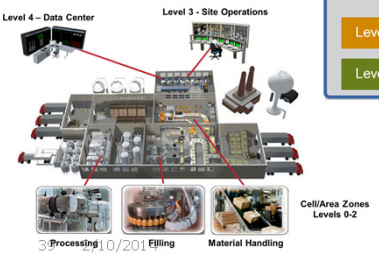
Segmentation

- Smaller modular building blocks to help 1) minimize network sprawl and 2) build scalable, robust and future-ready network infrastructure
  - Smaller fault domains (e.g. Layer 2 loops)
  - Smaller broadcast domains
  - Smaller domains of trust (security)
- Multiple techniques to create smaller network building blocks (Layer 2 domains)
  - Structure and hierarchy
    - Logical model – geographical and functional organization of IACS devices
    - Campus network model - multi-tier switch model – Layer 2 and Layer 3
    - Logical framework
  - Segmentation
    - Multiple network interface cards (NICs) – e.g. CIP bridge
    - Network Address Translation (NAT) appliance
    - Virtual Local Area Networks (VLANs)
    - VLANs with NAT
    - Integrated Services Router

IEEE

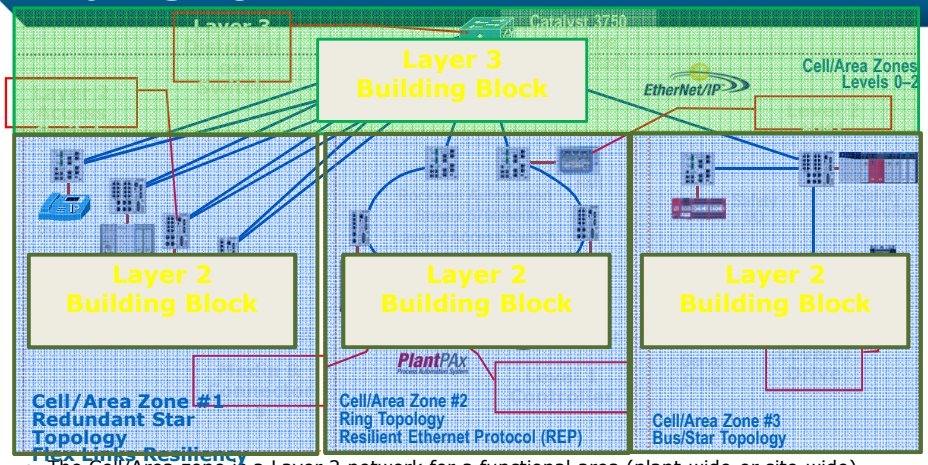
Structure and Hierarchy





Logical Model
Industrial Automation and Control System (IACS)
Converged Multi-discipline Industrial Network

Structure and Hierarchy – Logical Framework

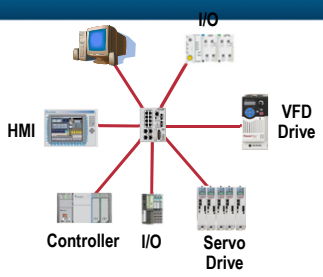


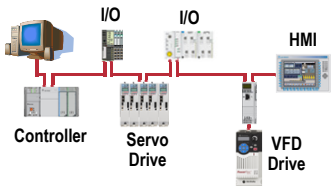
- The Cell/Area zone is a Layer 2 network for a functional area (plant-wide or site-wide)
  Key network considerations include:
  - Structure and hierarchy using smaller Layer 2 building blocks
  - Logical segmentation for traffic management and policy enforcement (e.g. QoS, Security) to accommodate time-sensitive applications

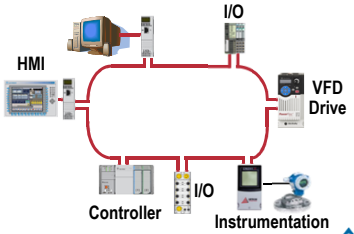
Islands of Automation with Isolated Networks

- Islands of Automation

Sneakernet



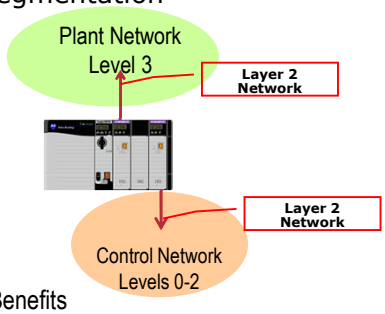




IEEE

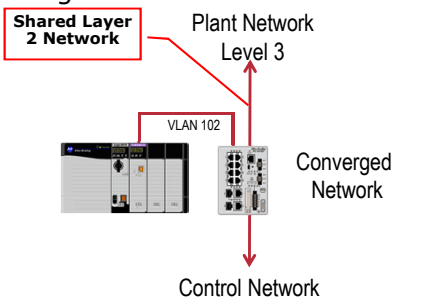
Segmentation– Multiple Network Interface Cards

- Isolated networks - two NICs for physical network segmentation



- 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

- Converged networks – logical segmentation

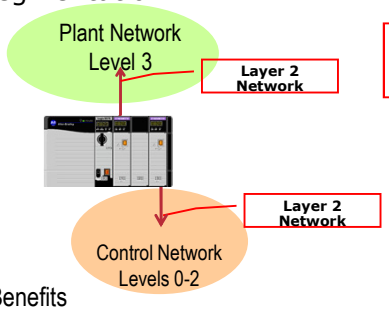


- Benefits
  - Plant-wide information sharing for data collection and asset management
  - Future-ready
- Challenges
  - Blurred network ownership demarcation line

IEEE

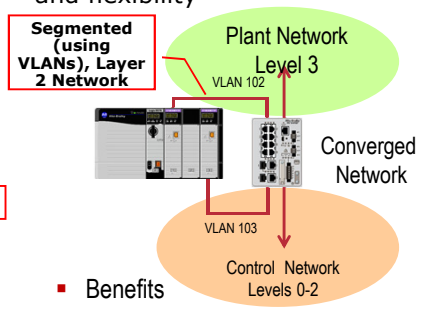
Segmentation

- Isolated networks - two NICs for physical network segmentation



- 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

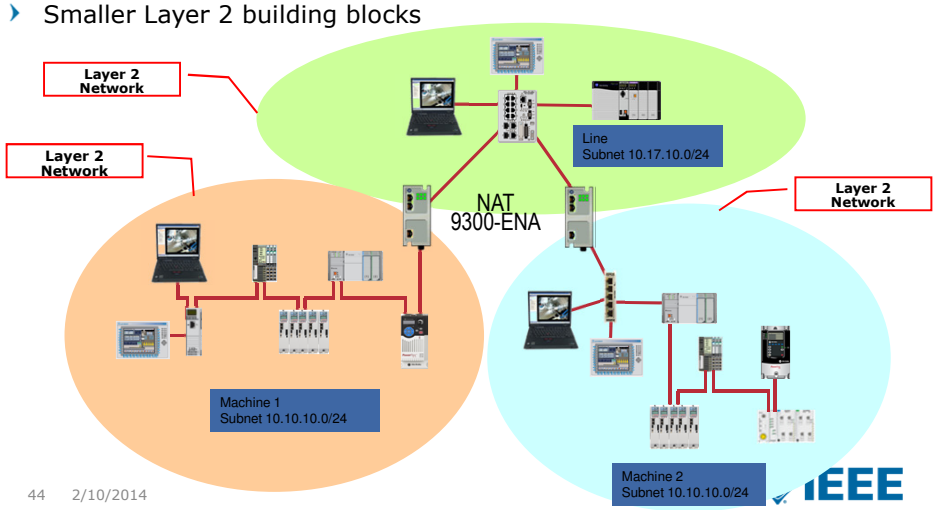
- Converged networks - logical segmentation - two NICs for scalability, performance, capacity and flexibility



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

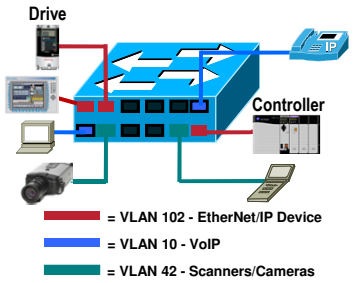
Network Address Translations (NAT) Appliance

- Segmented Networks - Layer 2 (e.g. VLAN) and Layer 3 (e.g. subnet)
- Smaller Layer 2 building blocks



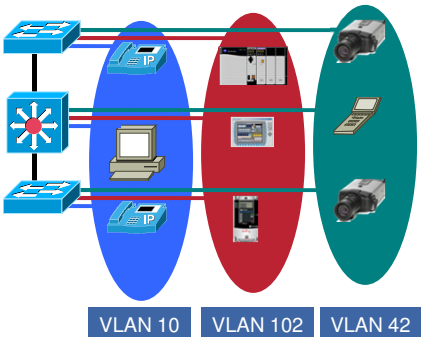
Virtual Local Area Networks (VLANs)

- 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



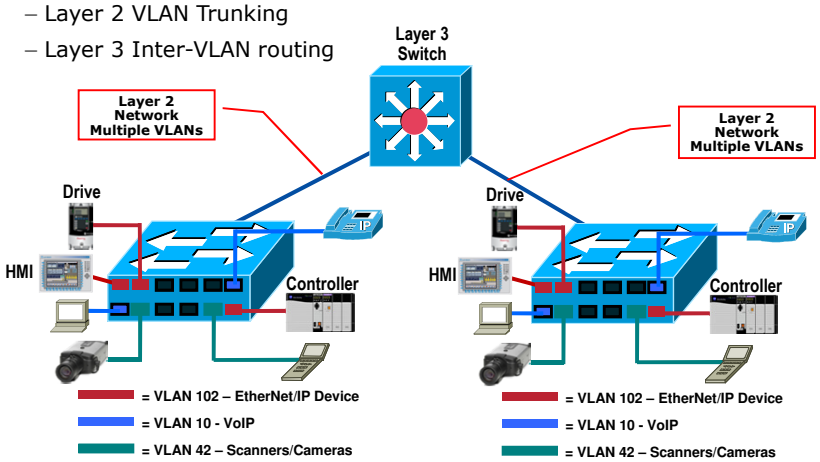
VLANs

- 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



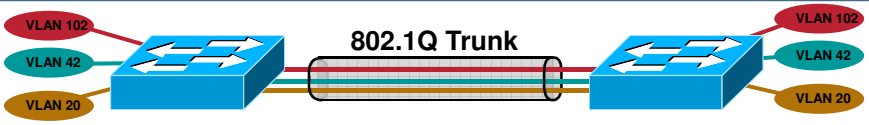
VLANs

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



IEEE

VLAN Trunking

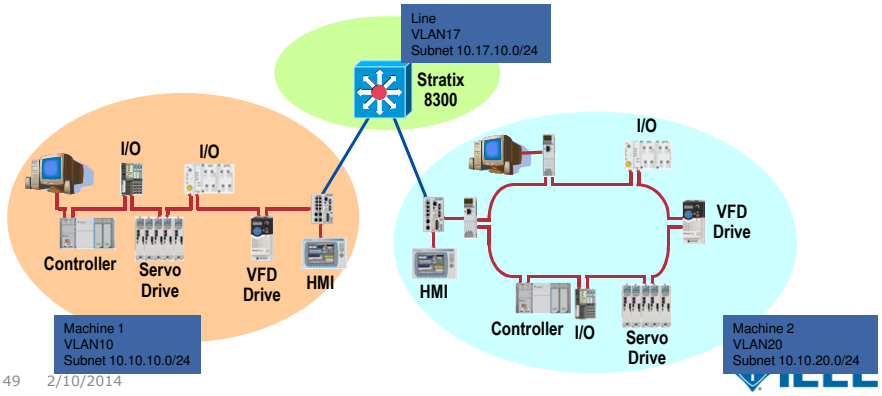


- VLAN Trunking Protocol (VTP)
  - Provides centralized VLAN management, runs only on trunks
  - Three modes:
    - Server: updates clients and servers
    - Client: receive updates - cannot make changes
    - Transparent: allow updates to pass through
- Use VTP transparent mode to decrease potential for operational error
  - Configured by default on Stratix 5700/8000/8300
  - Define VLANs at each switch, no centralized management

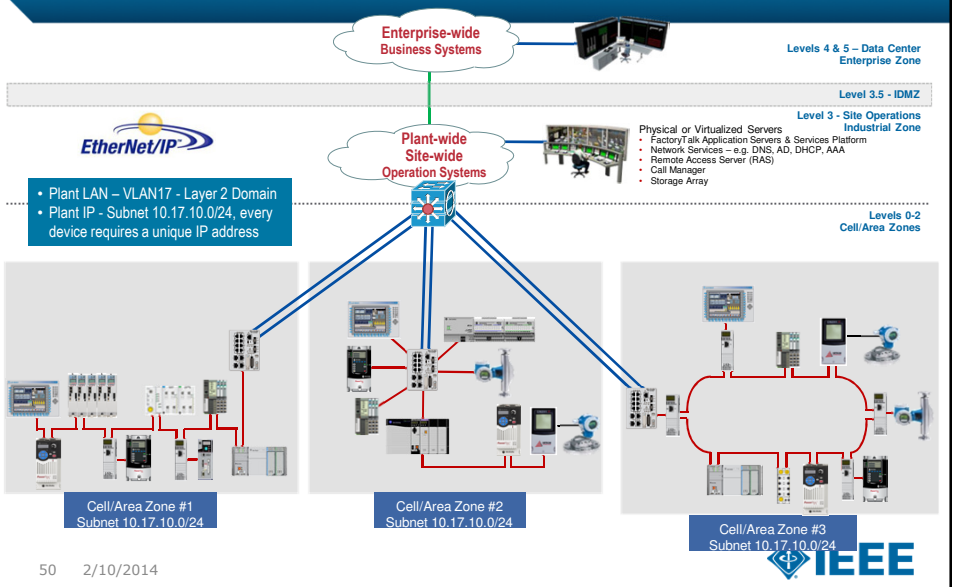
IEEE

VLAN Example

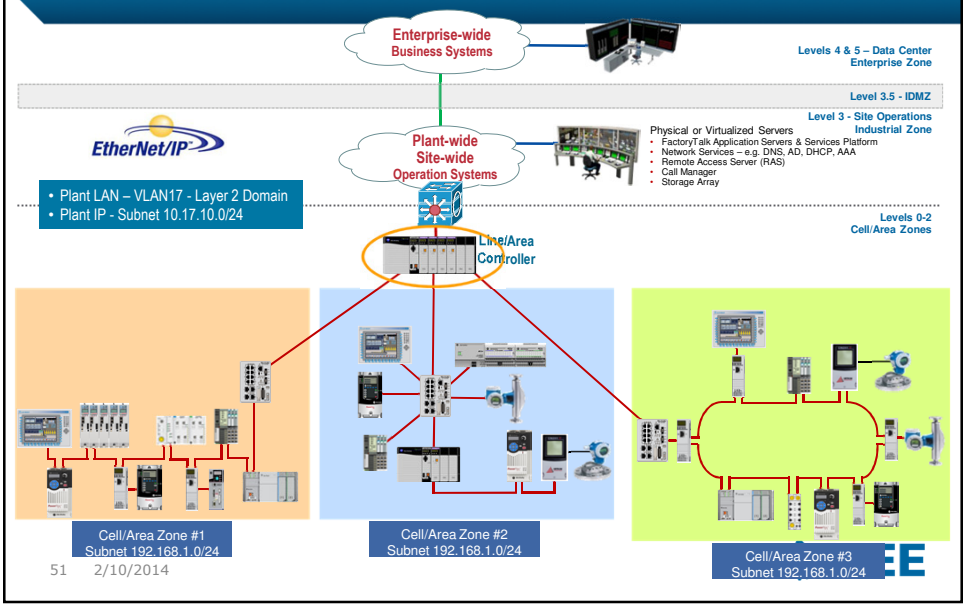
- Smaller Layer 2 building blocks
- Isolated Network with Multiple Controllers (ODVA)
  - Examples:
    - Single Cell/Area Zone, Single Line, Multiple Machines (vendors)



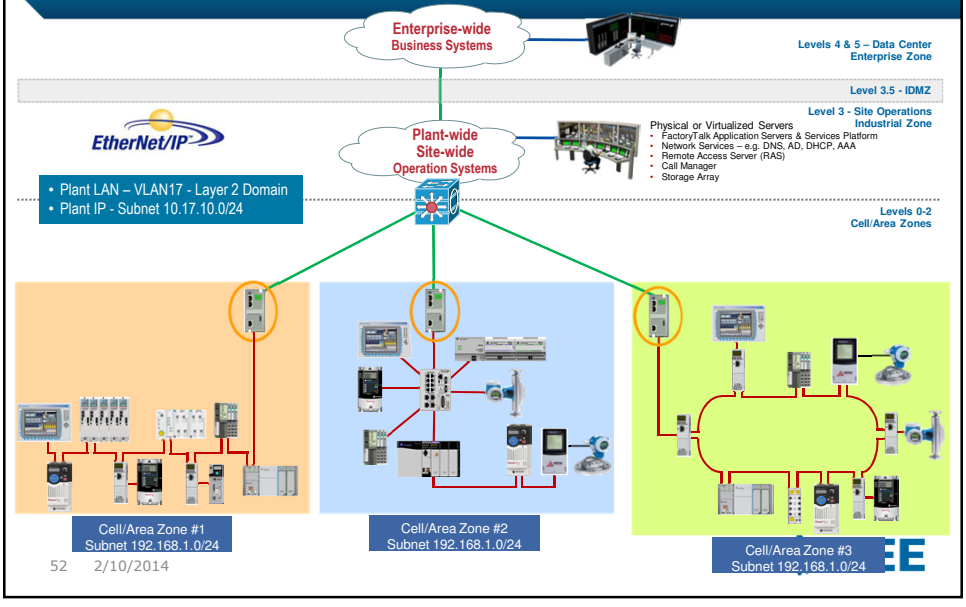
No Segmentation (Not Recommended)

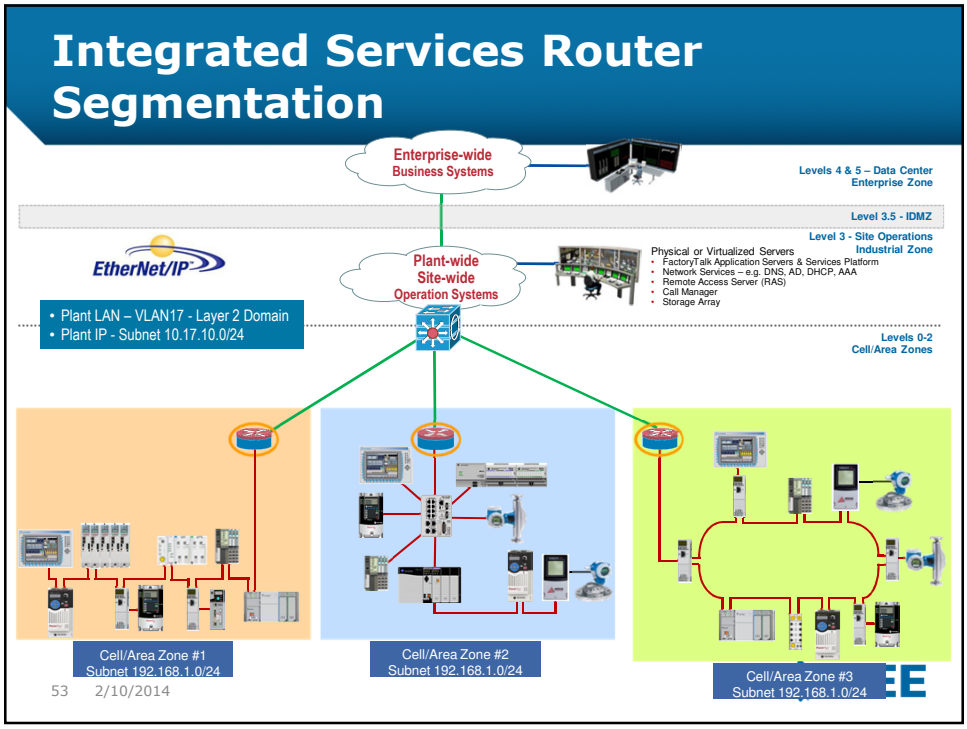


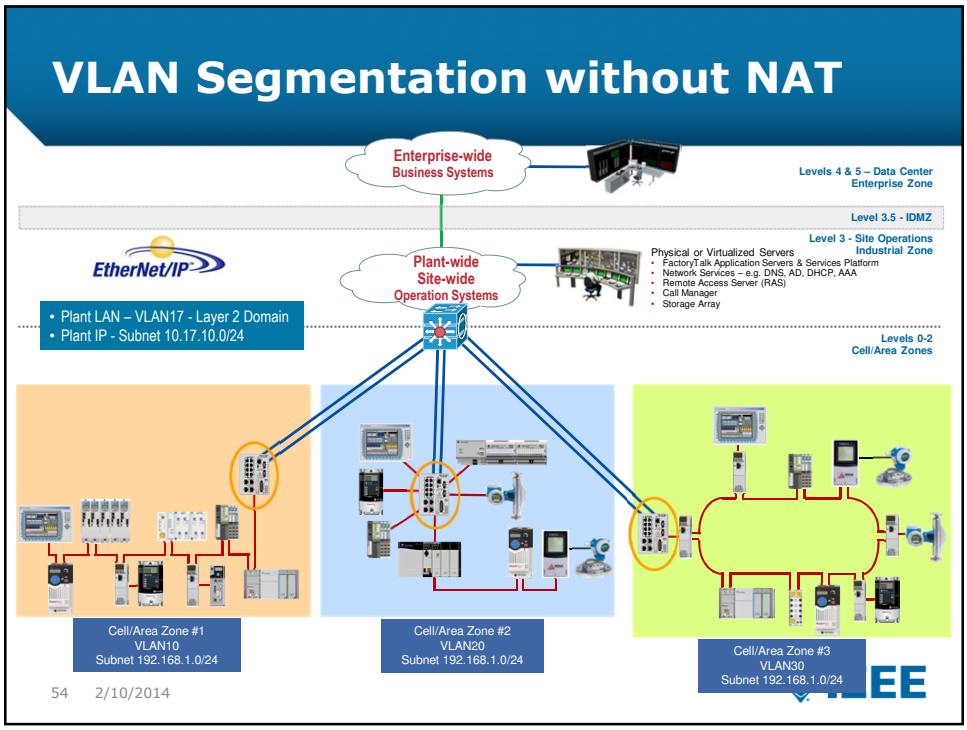
Multiple NIC Segmentation



NAT Segmentation




Integrated Services Router Segmentation
Enterprise-wide Business Systems
Levels 4 & 5 – Data Center Enterprise Zone
Level 3.5 - IDMZ
Level 3 - Site Operations Industrial Zone
EtherNet/IP
Plant-wide Site-wide Operation Systems
Physical or Virtualized Servers
FactoryTalk Application Servers & Services Platform
Network Services – e.g. DNS, AD, DHCP, AAA
Remote Access Server (RAS)
Call Manager
Storage Array
Plant LAN – VLAN17 - Layer 2 Domain
Plant IP - Subnet 10.17.10.0/24
Levels 0-2 Cell/Area Zones
Cell/Area Zone #1 Subnet 192.168.1.0/24
Cell/Area Zone #2 Subnet 192.168.1.0/24
Cell/Area Zone #3 Subnet 192.168.1.0/24
53 2/10/2014


VLAN Segmentation without NAT
Enterprise-wide Business Systems
Levels 4 & 5 – Data Center Enterprise Zone
Level 3.5 - IDMZ
Level 3 - Site Operations Industrial Zone
EtherNet/IP
Plant-wide Site-wide Operation Systems
Physical or Virtualized Servers
FactoryTalk Application Servers & Services Platform
Network Services – e.g. DNS, AD, DHCP, AAA
Remote Access Server (RAS)
Call Manager
Storage Array
Plant LAN – VLAN17 - Layer 2 Domain
Plant IP - Subnet 10.17.10.0/24
Levels 0-2 Cell/Area Zones
Cell/Area Zone #1 VLAN10 Subnet 192.168.1.0/24
Cell/Area Zone #2 VLAN20 Subnet 192.168.1.0/24
Cell/Area Zone #3 VLAN30 Subnet 192.168.1.0/24
54 2/10/2014

Design Considerations

Segmentation Techniques	Positive Design Considerations	Negative Design Considerations
No Segmentation (Not Recommended)	• Initially, may appear to be simpler to design and deploy • Link Resiliency (redundant path topologies)	• Same Layer 2 broadcast and fault domain, not a scalable or future-ready solution • Every node requires a unique IP address • Blurred demarcation line of network ownership
Multiple NIC Segmentation	• Simple to design and deploy • Smaller Layer 2 domains (broadcast and fault) • Reusable IP addresses / subnets • Clear demarcation line of network ownership	• Not scalable or future-ready, only CIP traffic can traverse a CIP bridge, limited quantity of bridge modules • Smaller PACs do not support a dual NIC • No Link Resiliency (redundant path topologies)
NAT Appliance Segmentation 9300-ENA	• Smaller Layer 2 domains (broadcast and fault) • Reusable IP addresses / subnets • Clear demarcation line of network ownership	• More difficult to design, deploy and manage - manual entry and management of IP address translations • No Link Resiliency (redundant path topologies)
Unified Threat Management Security Appliance Stratix 5900	• Smaller Layer 2 domains (broadcast and fault) • Reusable IP addresses / subnets • Clear demarcation line of network ownership • Enhanced security features	• More difficult to design, deploy and manage - manual entry and management of IP address translations • No Link Resiliency (redundant path topologies)
VLANs Only Segmentation Stratix 5700	• Scalable and future-ready • Smaller Layer 2 domains (broadcast and fault) • Smaller domains of trust (management of security policies) • Link Resiliency (redundant path topologies)	• Layer 3 switch or router is required to forward (route) information between VLANs • Every node requires a unique IP address • Blurred demarcation line of network ownership
VLAN Segmentation with NAT Stratix 5700	• Scalable and future-ready • Smaller Layer 2 domains (broadcast and fault) • Smaller domains of trust (management of security policies) • Reusable IP addresses / subnets • Link Resiliency (redundant path topologies)	• Layer 3 switch or router is required to forward (route) information between VLANs • More difficult to design, deploy and manage - manual entry and management of IP address translations • Blurred demarcation line of network ownership

Industrial Traffic Prioritization

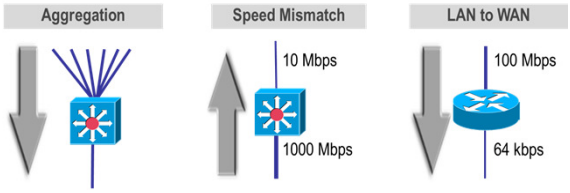
Not all traffic is created equal!	Control (e.g., CIP)	Video	Data (Best Effort)	Voice
Bandwidth	Low to Moderate	Moderate to High	Moderate to High	Low to Moderate
Random Drop Sensitivity	High	Low	High	Low
Latency Sensitivity	High	High	Low	High
Jitter Sensitivity	High	High	Low	High

Plant-wide / site-wide networks must prioritize industrial automation and control system (IACS) traffic (CIP) over other traffic types (HTTP, SMTP, etc.) to ensure deterministic data flows with low latency and low jitter

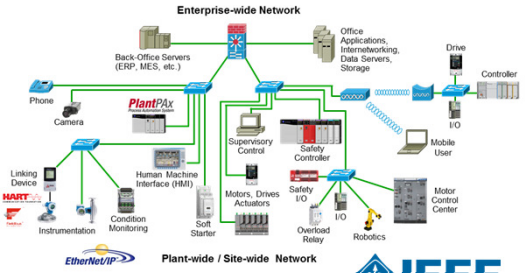
Different industrial traffic types (HMI, I/O, Safety, Motion) have different requirements for latency, packet loss and jitter

Quality of Service (QoS)

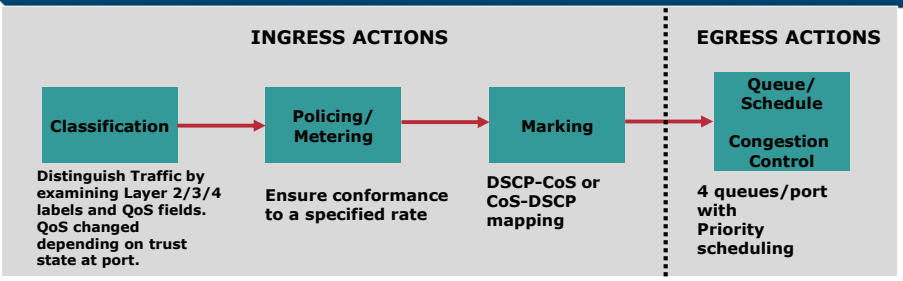
- QoS helps mitigate the following network issues:
  - End-to-end delay
    - Fixed delay – latency
    - Variable delay – jitter
  - Bandwidth capacity issues
  - Packet loss



- QoS design considerations:
  - QoS prioritizes traffic into different service levels
  - Provides preferential forwarding treatment to some data traffic, at the expense of others
  - Allows for predictable service for different applications and traffic types



Quality of Service (QoS)



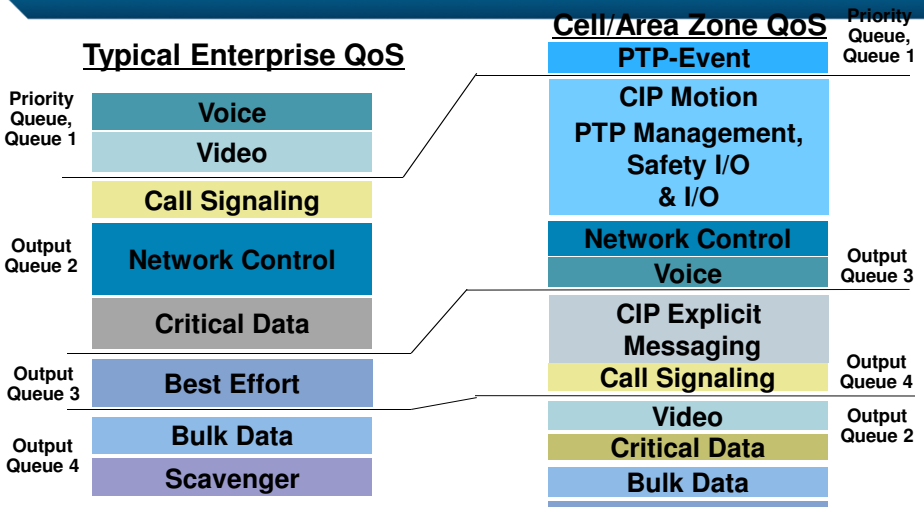
- QoS classification based on Layer attributes:
  - Layer 2 Destination MAC Address
  - Layer 2 EtherType
  - Layer 3 Source / Destination IP Address
  - Layer 4 TCP / UDP Source or Destination Port Number
- ODVA EtherNet/IP QoS Specification
  - Layer 2 … Class of Service (CoS) … 802.1Q/p
  - Layer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

QoS ODVA and DSCP and CoS Priority values

Traffic Type	CIP Priority	DSCP Layer 3	CoS Layer 2	CIP Traffic Usage
PTP event (IEEE 1588)	n/a	59	7	PTP event messages, used by CIP Sync
PTP General (IEEE 1588)	n/a	47	5	PTP management messages, used by CIP Sync
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 recommendations at present
CIP UCMM CIP class 3	All	27	3	CIP messaging

IEEE

Prioritization

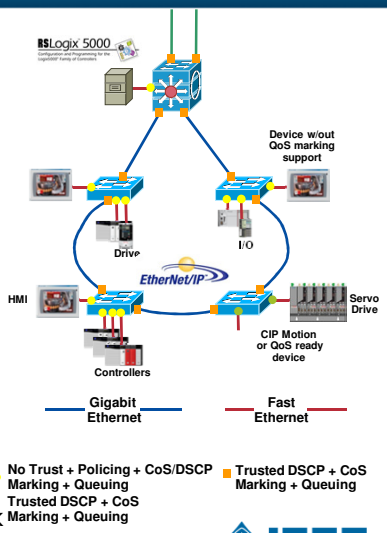


Note: Due to queue characteristics of the Stratix 5700/8000/8300, the queue order of priority is different than general enterprise switch.

IEEE

QoS Design Considerations

- QoS trust boundary moving from switch access ports to QoS-capable CIP devices
  - Stratix 5700/8000/8300 Smartport enables Trusted Markings
- For existing CIP devices, marking at the switch access port is based on port number
  - CIP I/O UDP 2222
  - CIP Explicit TCP 44818
  - Established through Stratix Express Setup
- Prioritize traffic to reduce latency and jitter for CIP I/O traffic
  - Prioritized traffic delivery for CIP Sync and CIP Motion
  - Minimize impacts by DDoS attacks
- Deploy QoS throughout the IACS network to take better advantage of QoS features



QoS Concluding Thoughts

- Plant-wide / site-wide networks must prioritize industrial automation and control system (IACS) traffic (CIP) over other traffic types (HTTP, SMTP, etc.) to ensure deterministic data flows with low latency and low jitter
- Quality of Service does not increase bandwidth.
  - QoS gives preferential treatment to EtherNet/IP IACS network traffic at the expense of other network traffic types
- QoS is integrated into the Stratix 5700/8000/8300 switch configurations
  - The Stratix 5700/8000/8300 recognizes or 'trusts' QoS capable devices and prioritizes CIP traffic as it exits from the switch
- Deploy QoS consistently throughout the EtherNet/IP IACS Network
  - The more IACS devices that implement QoS, the better that the network infrastructure devices (switches, routers) can take advantage of QoS features

Intelligent Motor Control

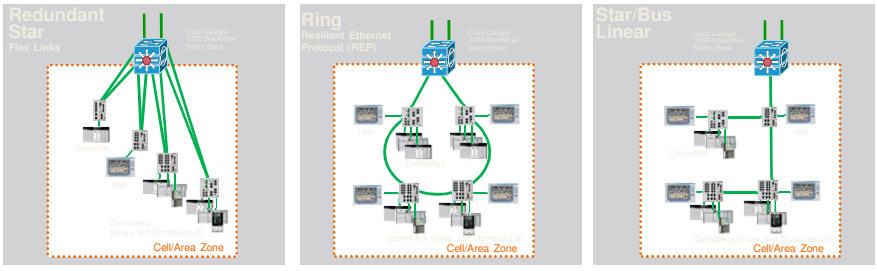
Designing Resilient, Fault Tolerant Industrial Networks

David C. Mazur, P.Eng., Ph.D. & Gregory S. Wilcox

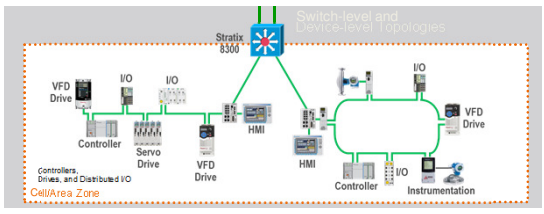
IEEE

Layer 2 Loop Avoidance Resiliency Schemes

Switch-level Topologies

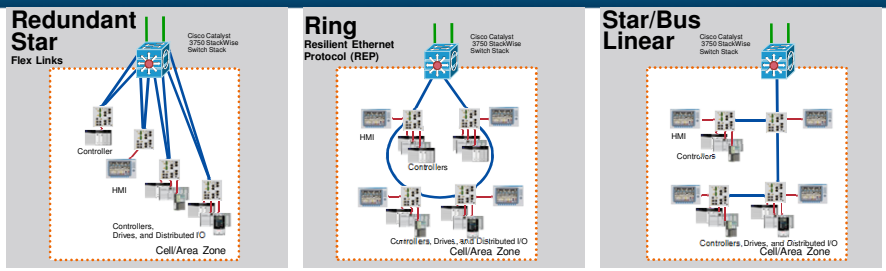


Device-level Topologies



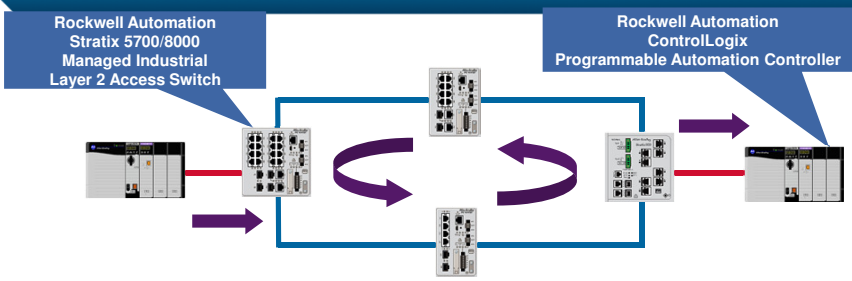
IEEE

Layer 2 Loop Avoidance Resiliency Schemes



	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

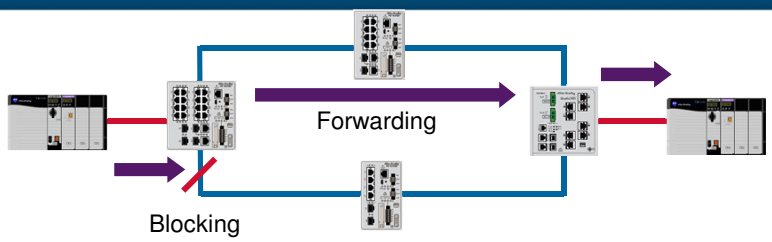
Layer 2– Loop Avoidance



- 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

IEEE

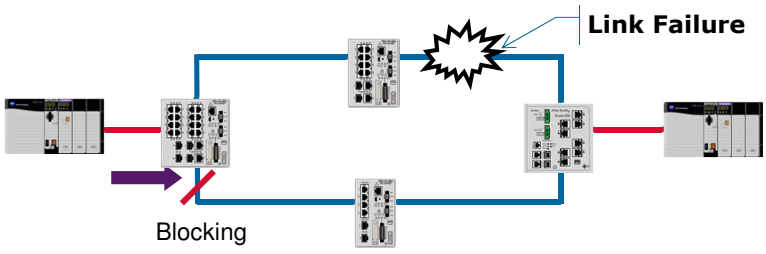
Layer 2 Loop Avoidance



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

IEEE

Layer 2 Loop Avoidance



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

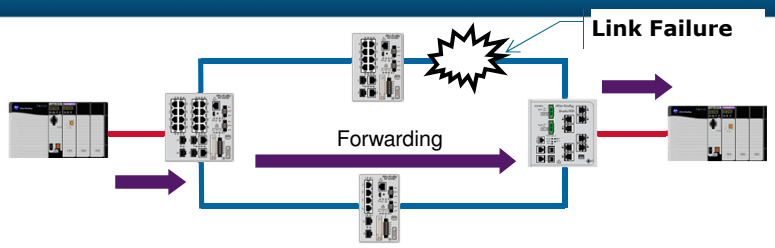
IEEE

Network Convergence

- 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 EtherNet/IP devices on the affected portion of the network may stop operating and may affect the industrial automation application.

IEEE

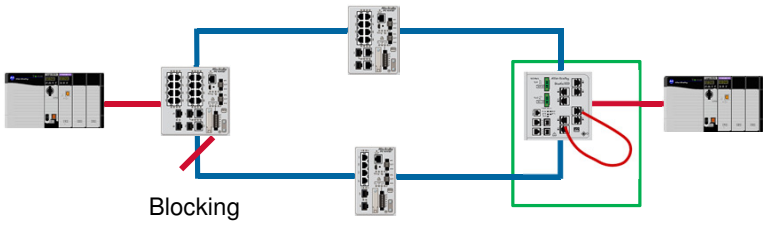
Example Layer 2 Loop Avoidance



- Network convergence must occur quickly enough to avoid a Logix Controller connection timeout:
  - Message (MSG) instruction - Explicit, CIP Class 3
    - Instruction timeout - 30 second default
    - KB #18945 - ControlLogix MSG instruction timeout values
  - I/O and Producer/Consumer - Implicit, CIP Class 1
    - Connection timeout - 4 x RPI, with a minimum of 100 ms
  - Safety I/O - Implicit, CIP Class 1
    - Connection timeout - 4 x RPI by default

IEEE

Layer 2 Loop Avoidance



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

IEEE

Switching Options

- Industrial versus COTS - Panel & DIN Rail Mounting vs. Table & Rack (e.g. 1RU)
- Managed versus Unmanaged

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

E

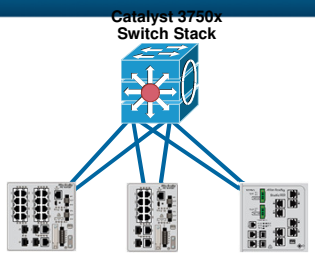
Network Resiliency Protocols

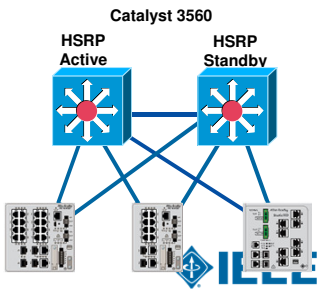
- Device-level Topology
  - Ring
    - Embedded switch technology EtherNet/IP IACS devices
    - Device Level Ring (DLR) Protocol – IEC & ODVA
- Switch-level Topology
  - Ring or Redundant Star
    - Spanning Tree Protocol (STP), Rapid STP (RSTP), Multiple instance STP (MSTP) – IEEE
      - Stratix 5700/8000/8300 – MSTP - default
      - Rapid Per VLAN Spanning Tree Plus (rPVST+) - Cisco Technology
  - Ring Only
    - Resilient Ethernet Protocol (REP) – Cisco Technology
  - Redundant Star Only
    - EtherChannel
      - Link Aggregation Control Protocol (LACP) - IEEE
    - Flex Links – Cisco Technology

IEEE

Network Resiliency Protocols

- Distribution switches typically provide first hop (default gateway) redundancy
  - StackWise (3750X), stack management
  - Hot Standby Router Protocol (HSRP)
  - Virtual Router Redundancy Protocol (VRRP)
  - Gateway Load Balancing Protocol (GLBP)



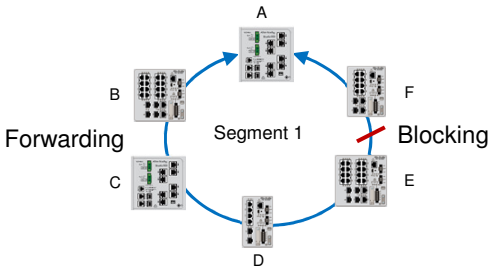


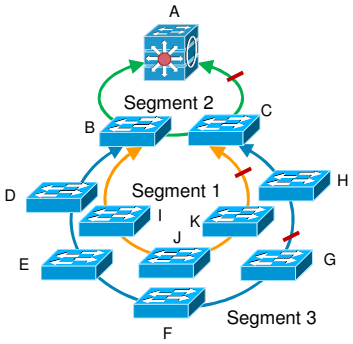
Network Resiliency Protocols

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		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	

Resilient Ethernet Protocol (REP)

REP segments apply to various Layer 2 Topologies





IEEE