Advances in Industrial Ethernet

Convergence of Control and Information

Lex Kasacavage
Solution Architect
Rockwell Automation

Industrial Ethernet

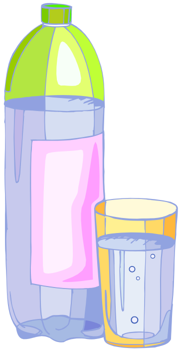
- Trends in Industrial Networks
- Fundamentals and Best Practices
  - Segmenting and Prioritizing
  - Resiliency and Redundancy
  - Physical Layer Considerations
- Security in Industrial Networks

Famous former truths

- ✓The world is flat

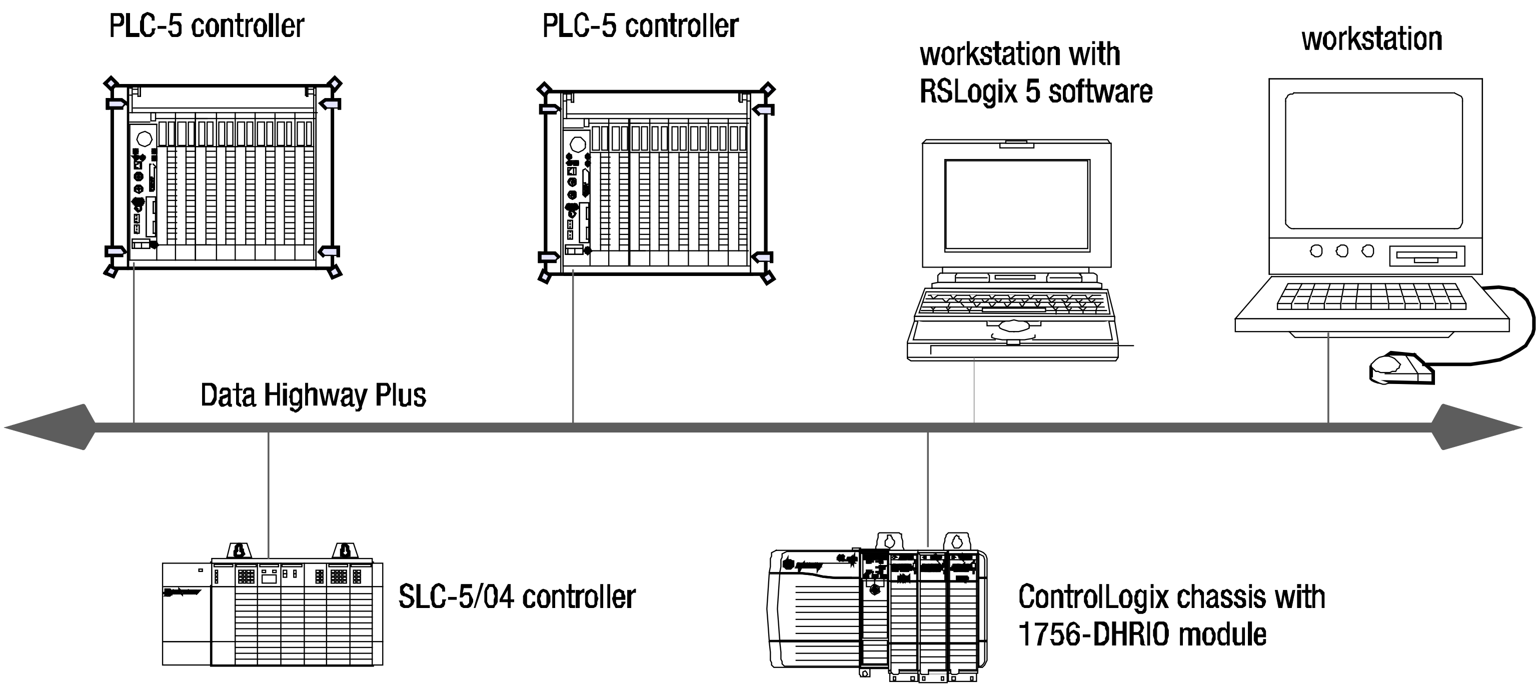
- ✓It's unsinkable
- ✓The money is in the hardware, not the software

- ✓640K is all the memory you'll ever need
- ✓People will never pay for bottled water

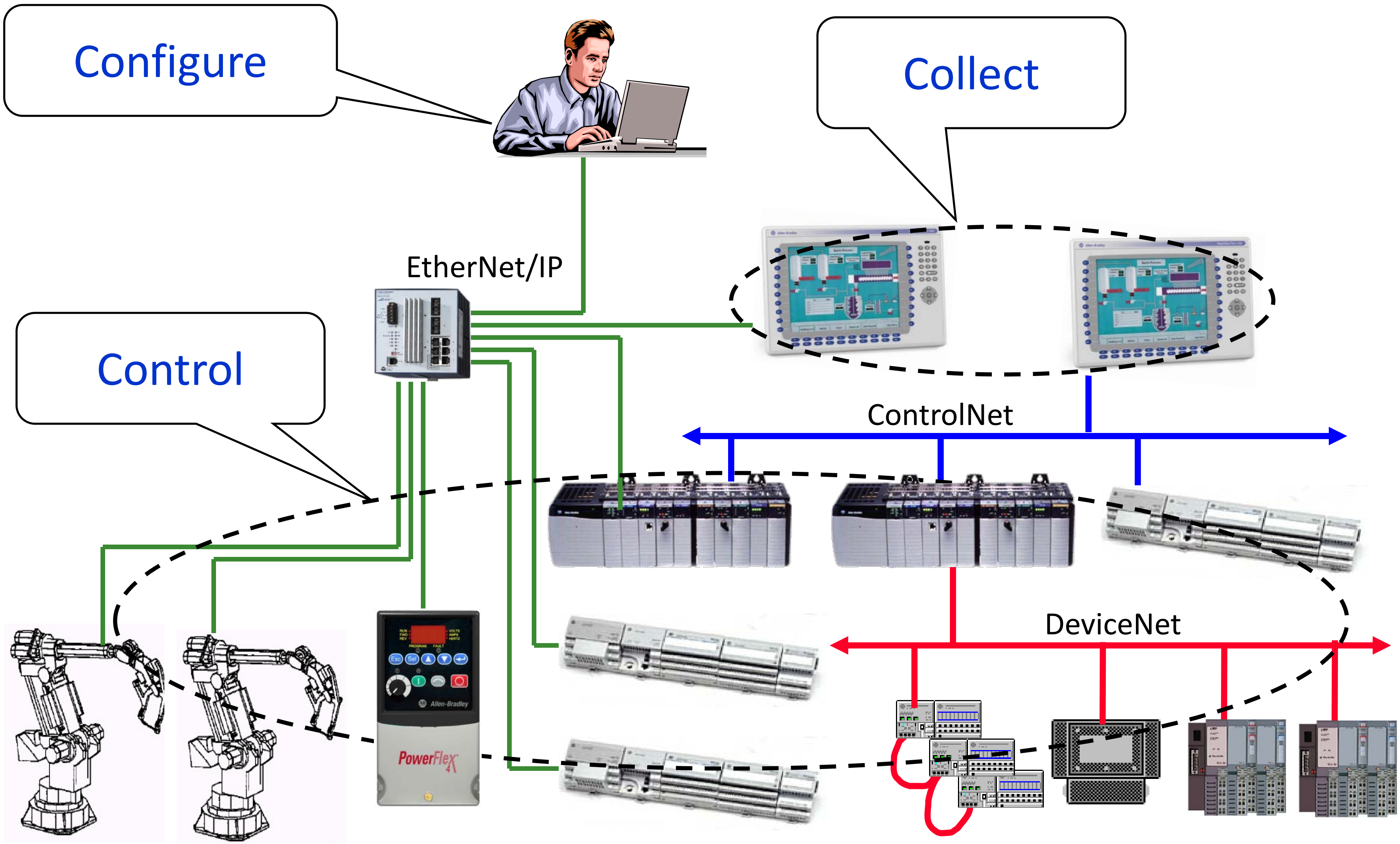


- ✓Enron is the place for your money
- ✓Ethernet will never be able to support real-time industrial control

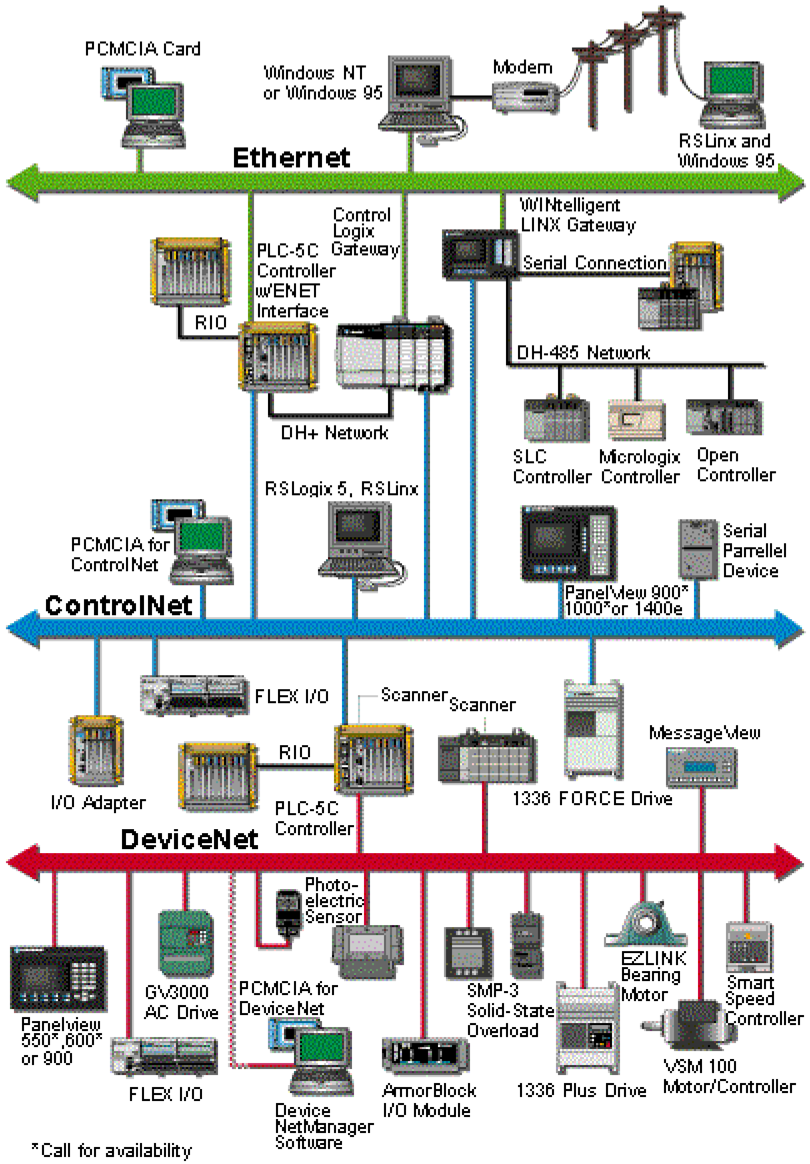
Industrial Control Networks – pre 2000



Industrial Control Networks – circa 2004

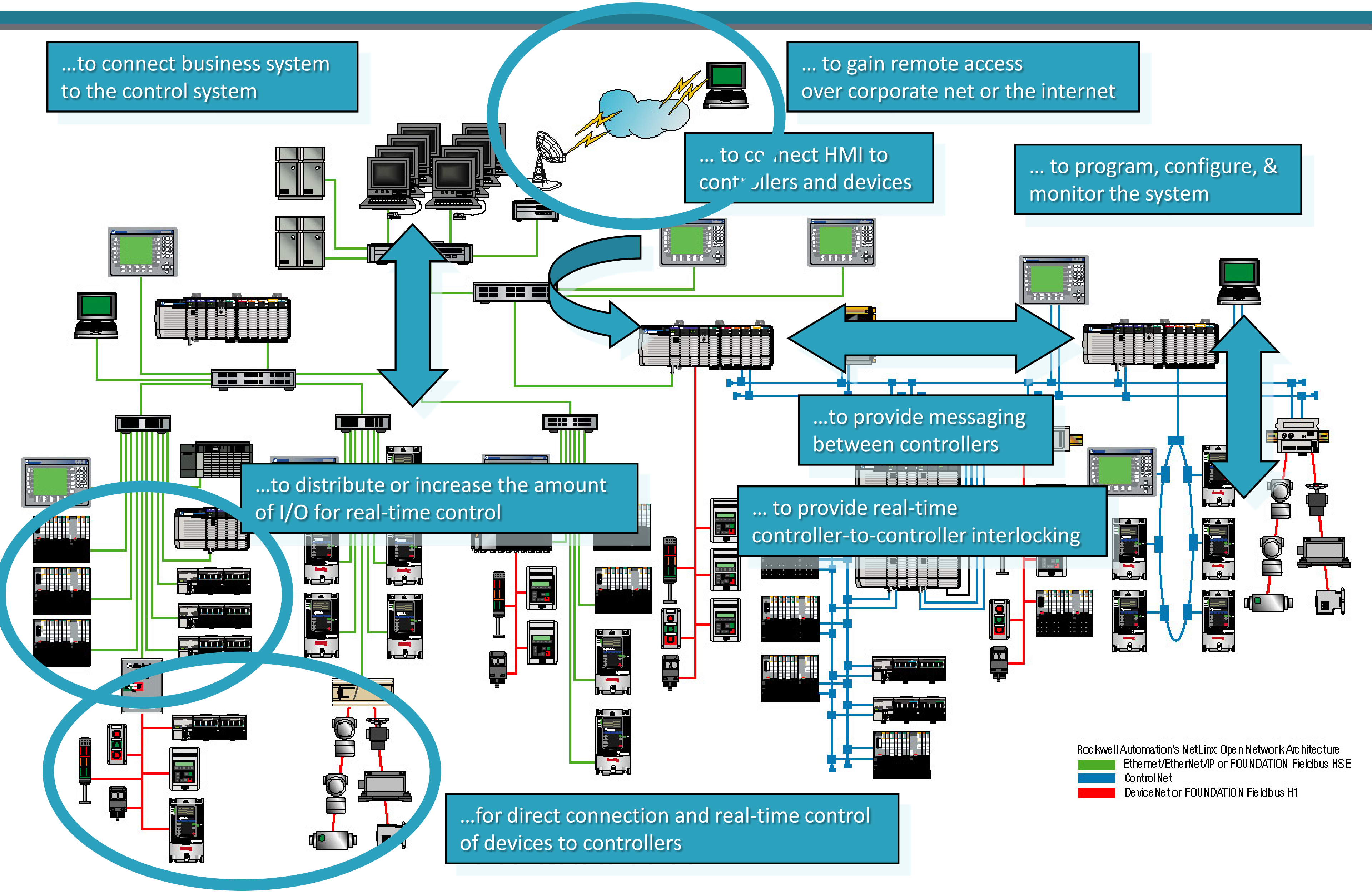


Industrial Control Networks – circa 2006



- Allow information to flow anywhere in a system
  - Devices on different networks can communicate with each other
- From a single workstation over heterogeneous networks enable the user to:
  - identify and configure all devices
  - program all control devices
  - collect information from any device
  - monitor the status of any device
- Permit information sharing
  - I/O monitored by multiple devices

Industrial Control Networks – 2009+

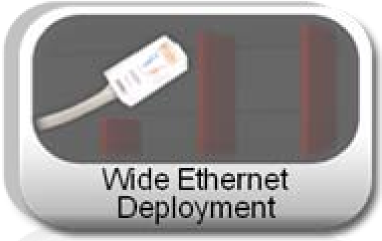


Trends in Industrial Networks

- 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
- Convergence of Network Technologies
  - Reduce the number of different networks in an operation and create seamless information sharing throughout the plantwide architecture
  - Use of common network design and troubleshooting tools across the plant and enterprise; avoid special tools for each application
- Better Asset Utilization to Support Lean Initiatives
  - Reduce training, support, and inventory for different networking technologies
  - Common network infrastructure assets, while accounting for environmental requirements
- Future-Ready – Maximizing Investments
  - Support new technologies and features without a network forklift upgrade

Trends in Industrial Networks
Wide Adoption of Ethernet on Factory Floor

- Standardization of connectors such as RJ45 make use of traditional IT and consumer goods main stream markets



- Real-time control over Ethernet is a reality

- Getting data from the shop floor via Ethernet is a natural fit for the IT staff who has experience managing Ethernet infrastructure

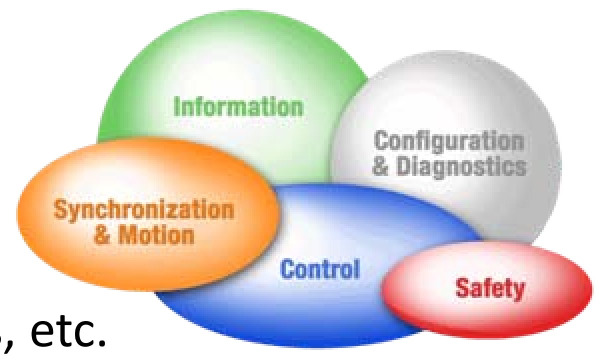
- Adoption by many vendors to support Ethernet on the manufacturing floor offers a wide variety of devices and solutions

- Migration of wireless, video, voice and real-time control on the manufacturing network infrastructure

Trends in Industrial Networks
Increasing Need for "Real-Time" Information

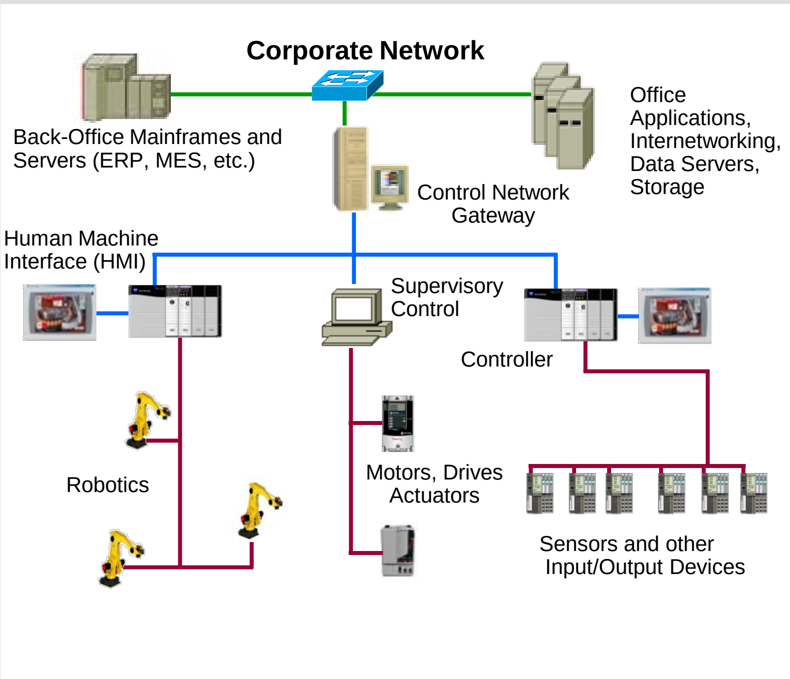
- Decision makers need information to make product, material, purchasing and resource decisions

- Information contained within the manufacturing environment needs to feed different business systems
  - Quality, scheduling, lot tracking, computerized maintenance, etc.

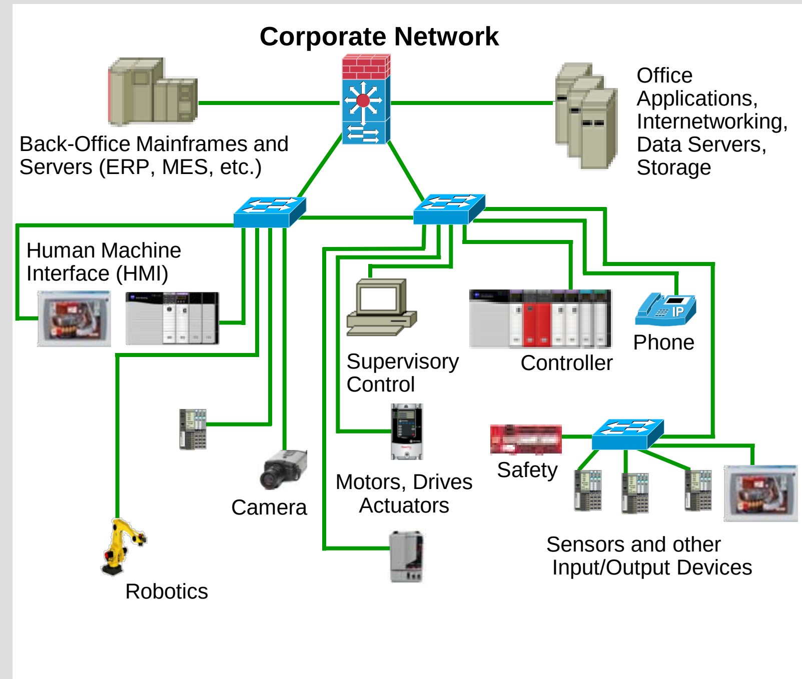


- Connectivity to archive important data
  - Historians, disaster recovery and security systems, etc.
- Recall, retrace and proof of critical manufacturing variables during product inception, packaging and delivery lifecycle

Industrial Network Convergence



Traditional – 3 Tier Industrial Network Model



Converged Ethernet Industrial Network Model

Industrial Ethernet - Enabling/Driving Convergence of Control and Information

Open System Interconnection (OSI)
Reference Model

Layer Name		Layer No.	Function	Examples
Application		Layer 7	Network Services to User App	Telnet/CIP
Presentation		Layer 6	Encryption/Other processing	JPEG/ASCII
Session		Layer 5	Manage Multiple Applications	OS Scheduling
Transport		Layer 4	Reliable delivery/Error correction	TCP - UDP
Network	Routers	Layer 3	Logical addressing - Routers	IP
Data Link	Switches	Layer 2	Media Access Control	IEEE 802.3
Physical	Cabling	Layer 1	Specifies voltage, pin-outs, cable	TIA - 1005

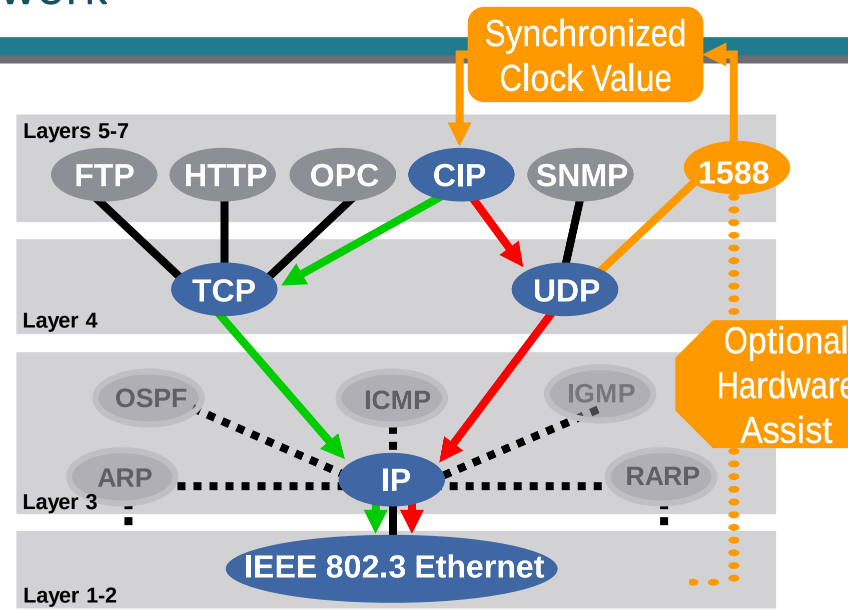
Encapsulation

De-Encapsulation

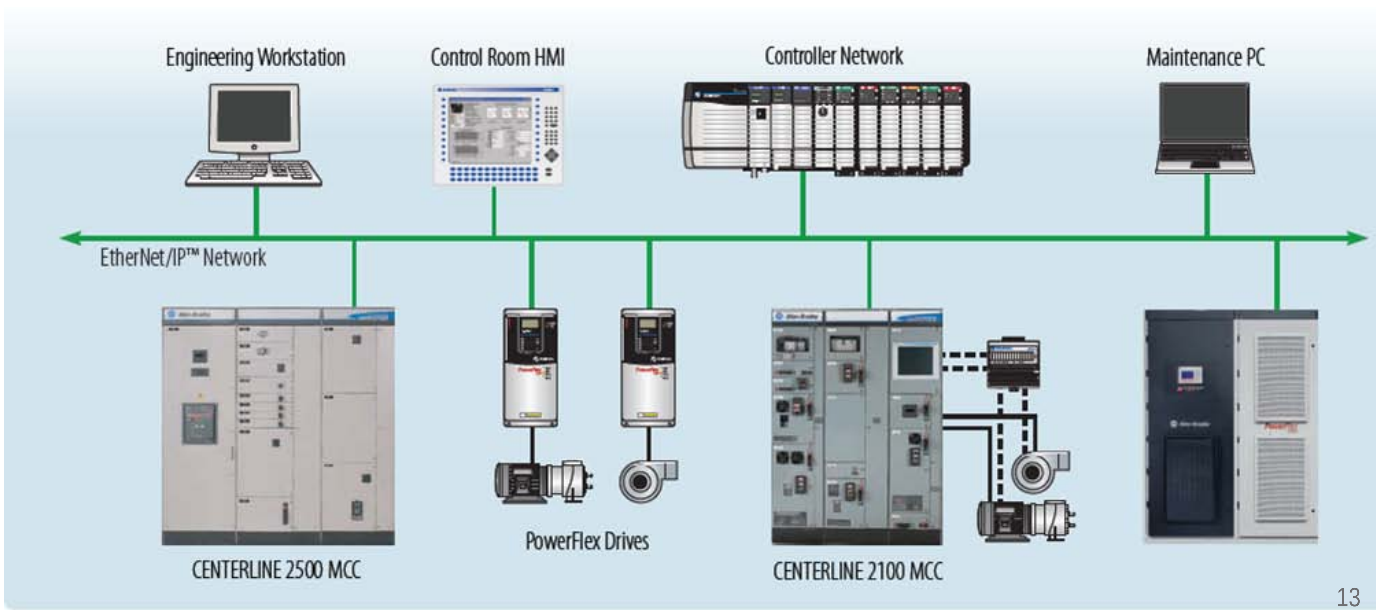
- The **<u>Open Systems Interconnection</u> (OSI)** model serves as a blueprint for all network communication technologies. Allows various "open" systems to communicate
- Dividing up all the processes of networking activity into seven layers. Each layer of the OSI model has a specific function in an ideal network and groups similar protocols together.

Layer 7 - Application
Time Synchronization Across the Network

- Time Synchronized Applications such as:
  - Input time stamping
    - Events and alarms
    - Sequence of Events recording
    - First fault detection
  - Time scheduled outputs

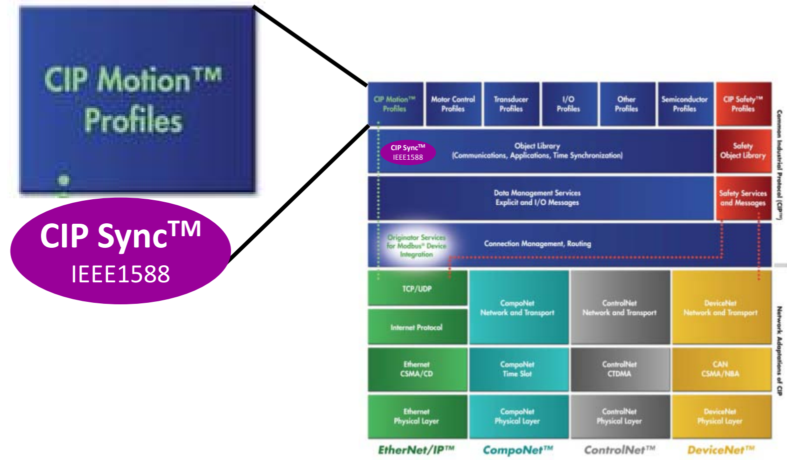


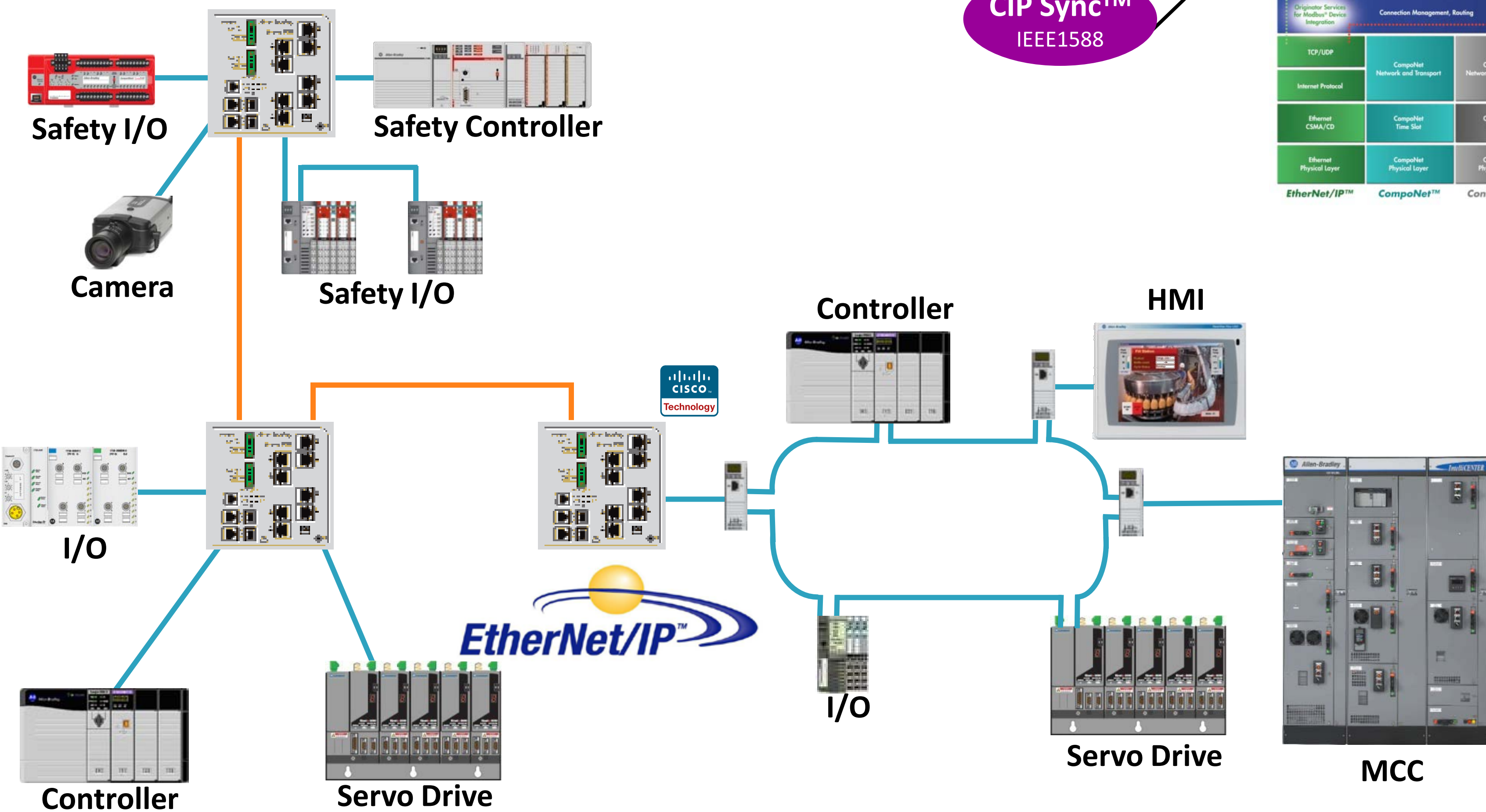
- IEEE-1588 precision clock synchronization protocol standard
  - Referred to as precision time protocol **(PTP)**
  - Provides +/- 100 ns distributed node time synchronization



Layer 7 - Application
Motion control with Ethernet

- High speed coordinated multi-axis servo control
- Same wire as standard control



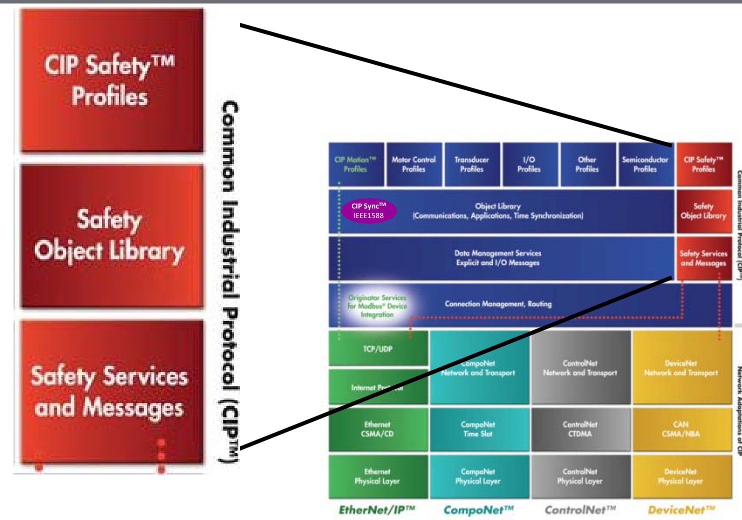


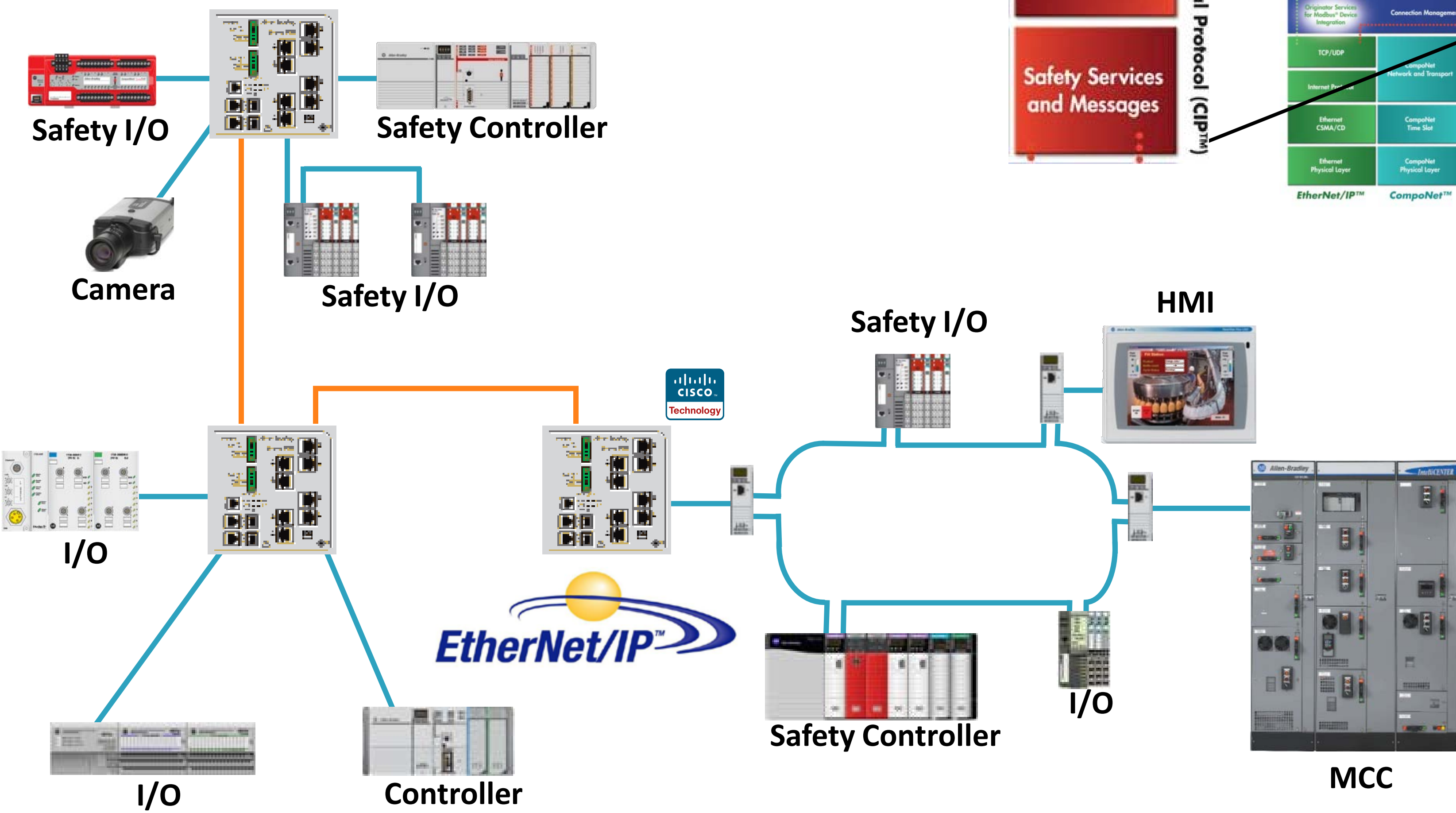
Layer 7 - Application

SIL 3 Safety Systems on Ethernet

CIP Safety™

- High-integrity Safety Services and Messages
- IEC 61508 – SIL3 and EN 954-1



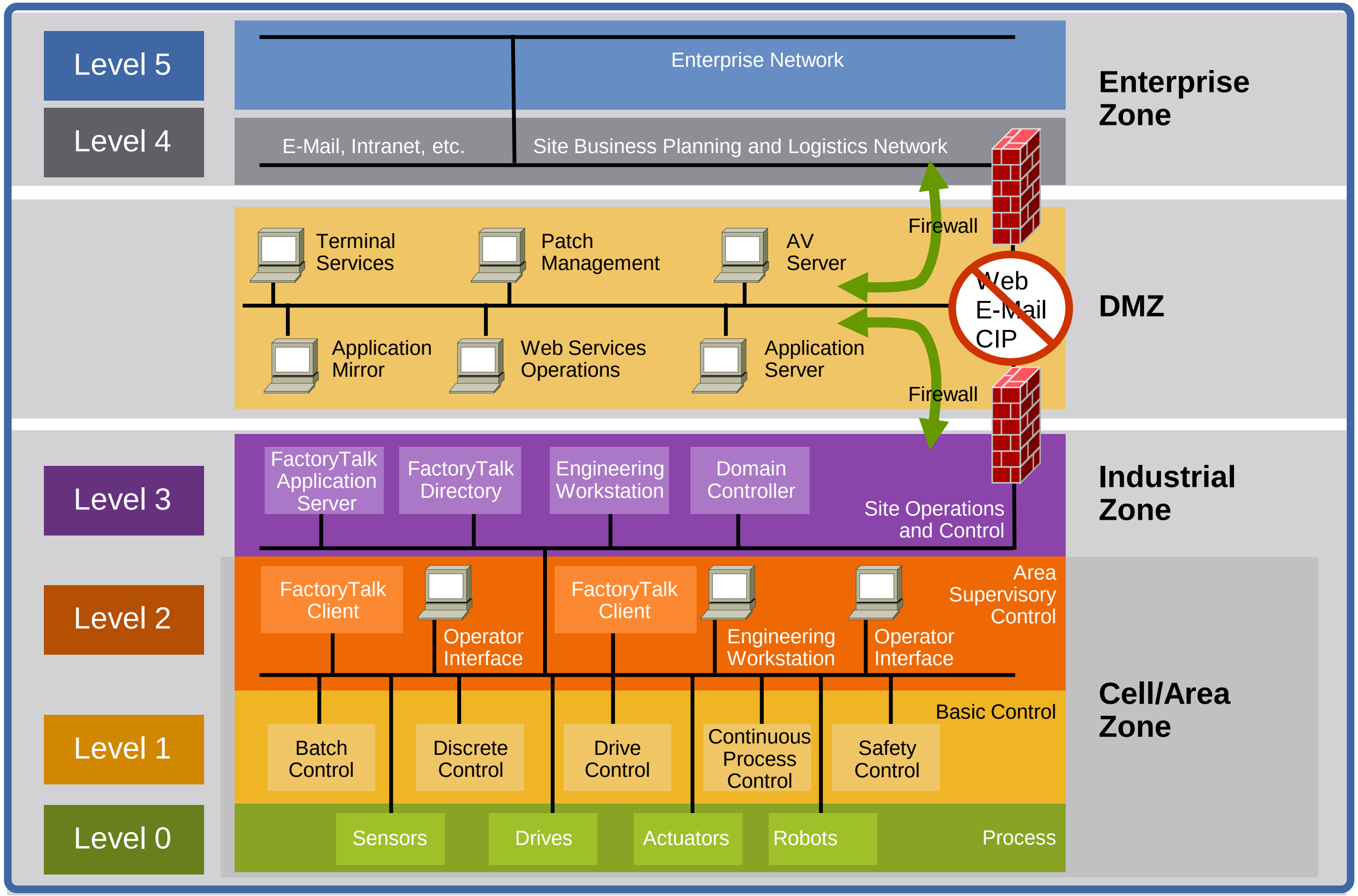


Networking Best Practices

Best practices for reducing **Latency** and **Jitter**, and to increase data **Availability**, **Integrity** and **Confidentiality**

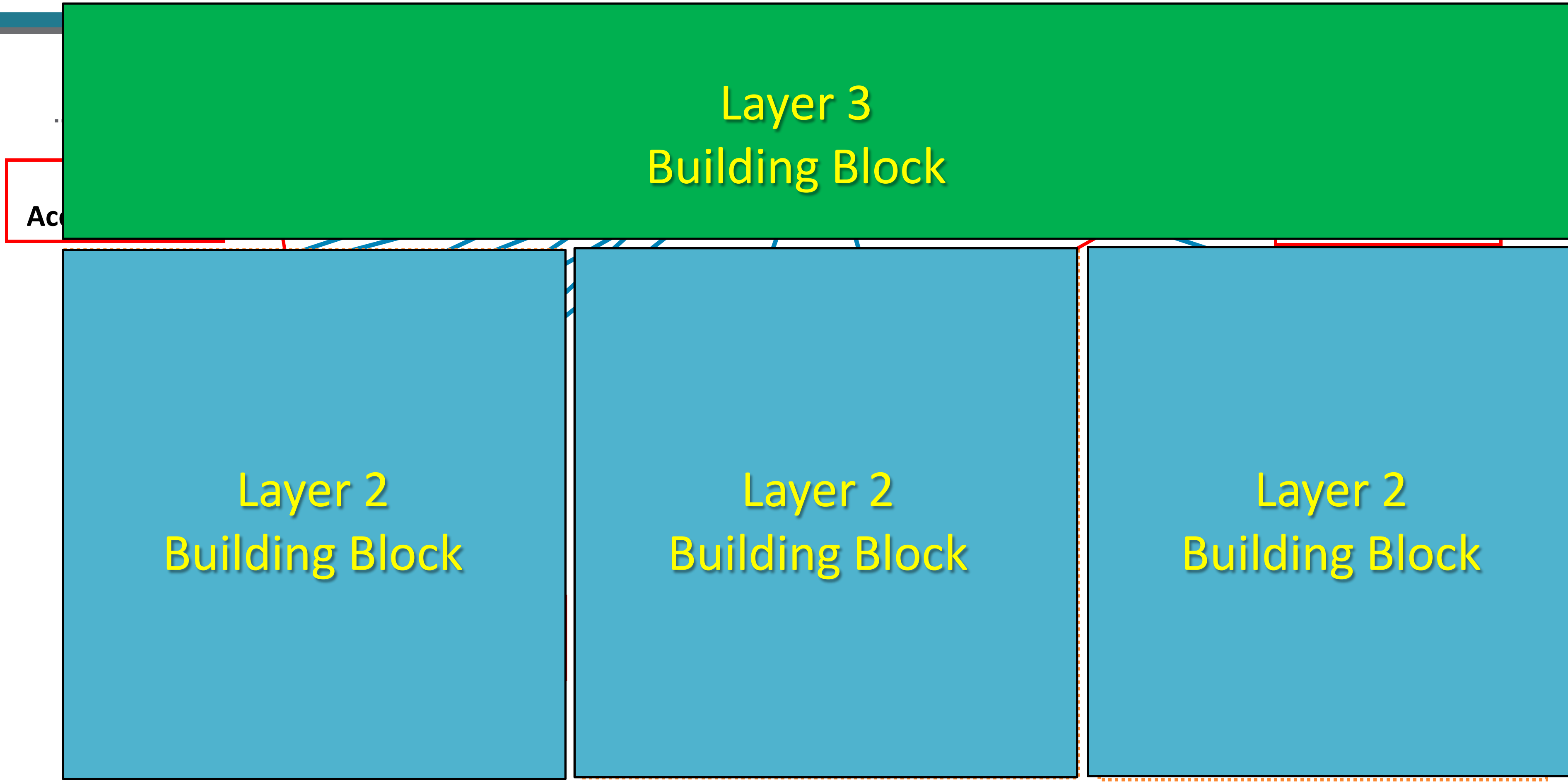
- **Segmentation**
  - Multi-tier Network Model
  - Topology
  - Virtual LANs (VLANs)
- **Prioritization**
  - Quality of Service (QoS)
- **Resiliency Protocols and Redundant (multipath) Topologies**
  - Use Fiber-media uplinks for fast convergence
- **Security**
  - DHS CSSP

Industrial and IT Network Convergence
Logical Framework



- Network Segmentation
- **Demarcation Line** for: Security Policies, Quality of Service Policies, Multicast Groups

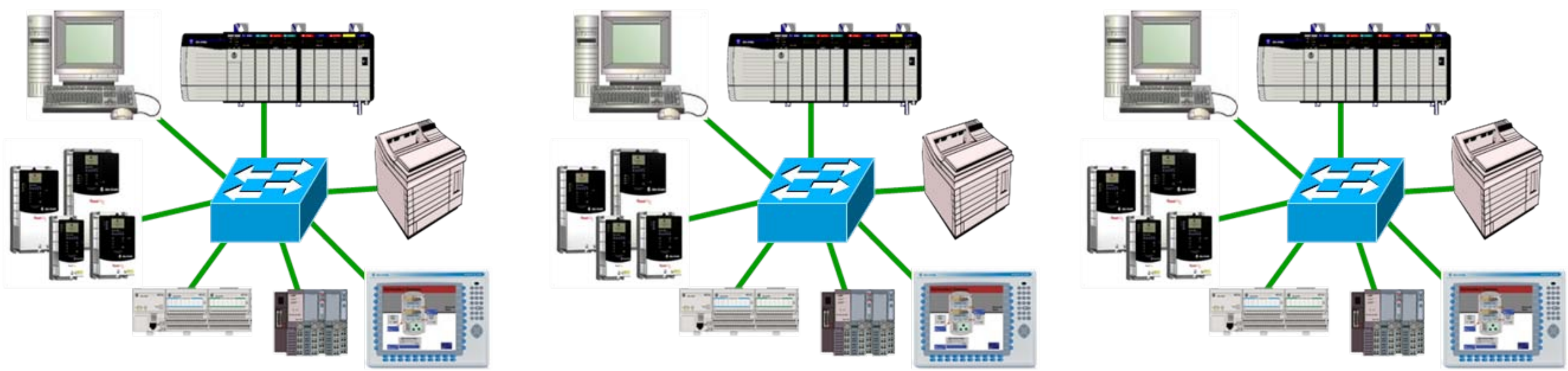
Structure and Hierarchy
Logical Framework



- The Cell/Area zone is a Layer 2 network for a functional area of the plant floor. Key network considerations include:
  - Structure and hierarchy using smaller Layer 2 building blocks
  - Logical segmentation for traffic management and policy enforcement to accommodate time-sensitive applications

Segmentation
Physical Isolation

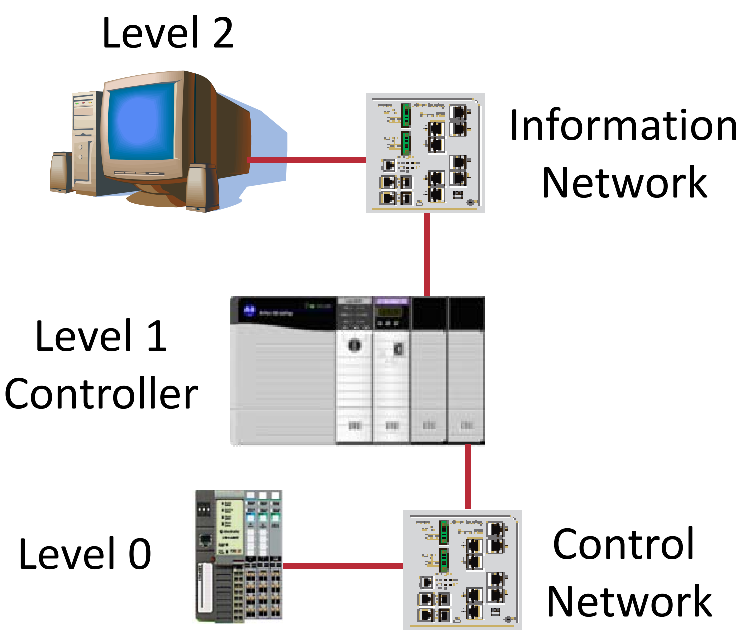
- Segmentation by physical isolation
  - Physically isolating networks
  - Each network is a separate subnet creating clusters of control
  - Limited to no IT involvement



Subnet #1 **Subnet #2** **Subnet #3**

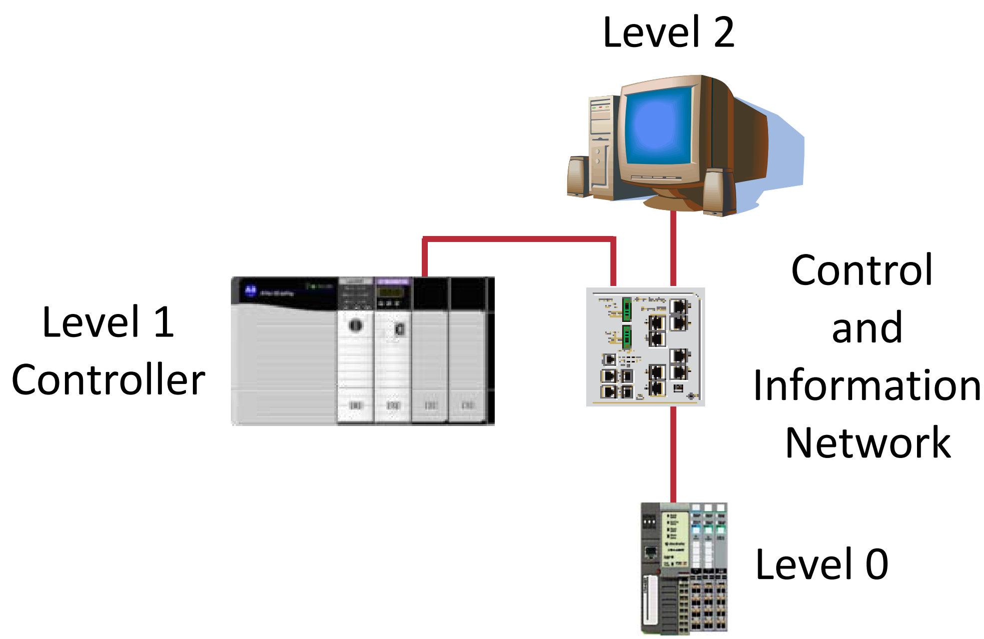
Segmentation
Physical – Multiple NICs

- 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

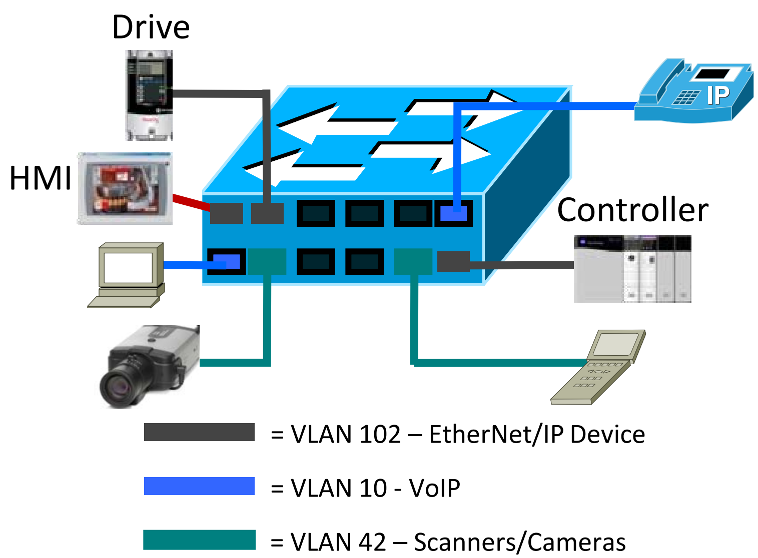
- Converged networks - logical segmentation



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

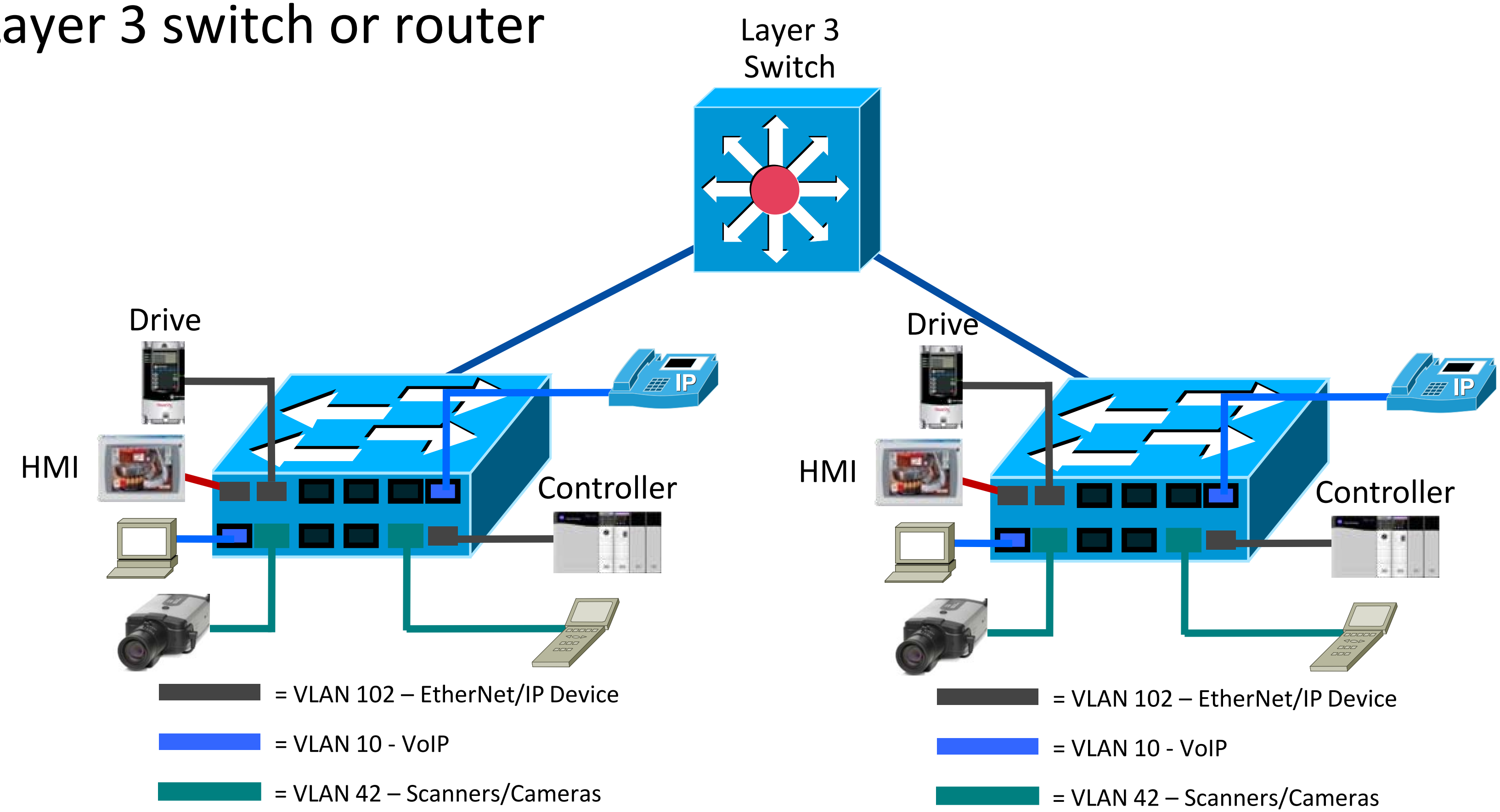
Segmentation
Virtual Local Area Networks - VLANs

- 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



Segmentation
Virtual Local Area Networks - VLANs

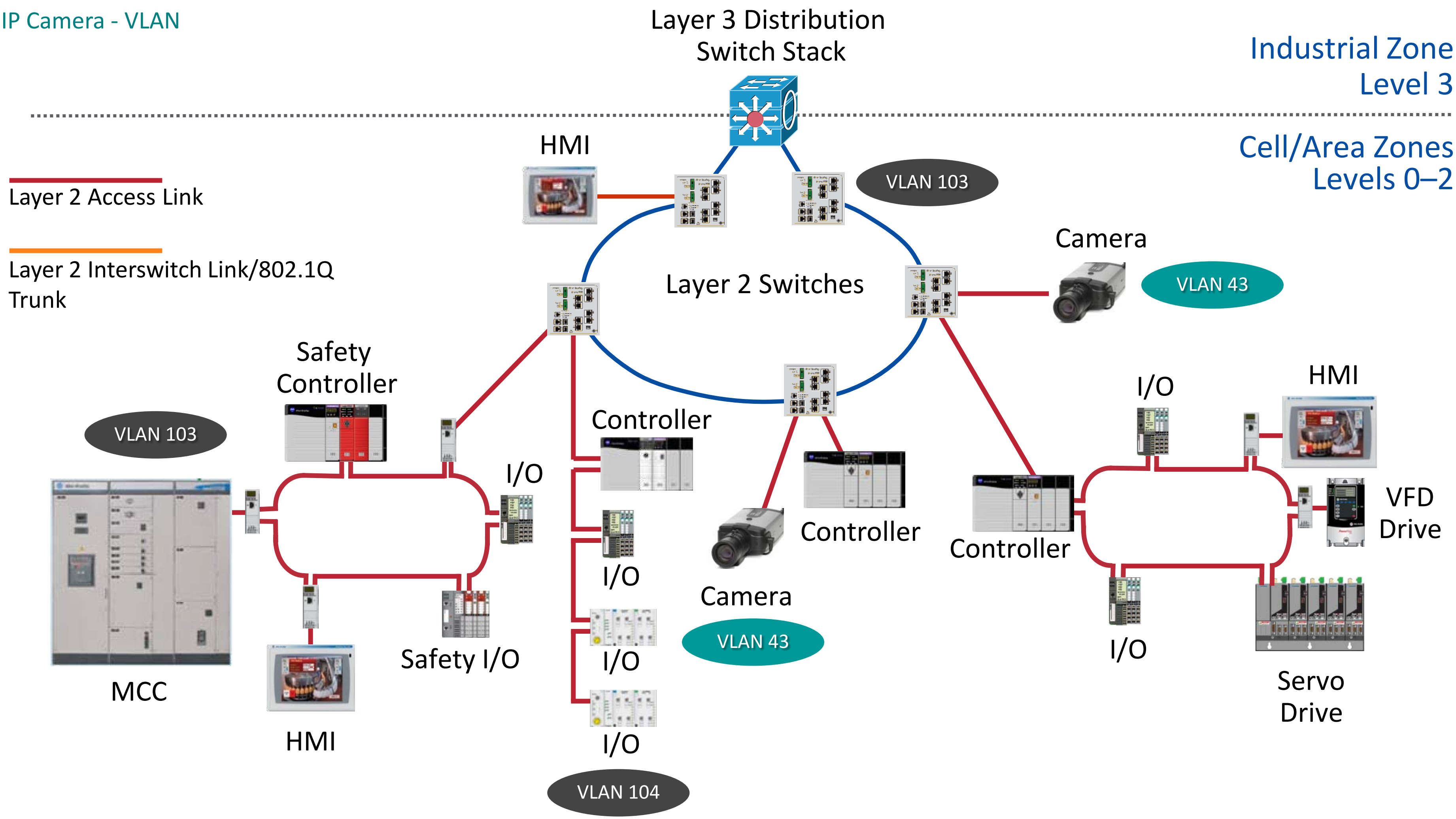
- Inter-VLAN routing
- Layer 3 switch or router



Segmentation
VLANS - Representative Example

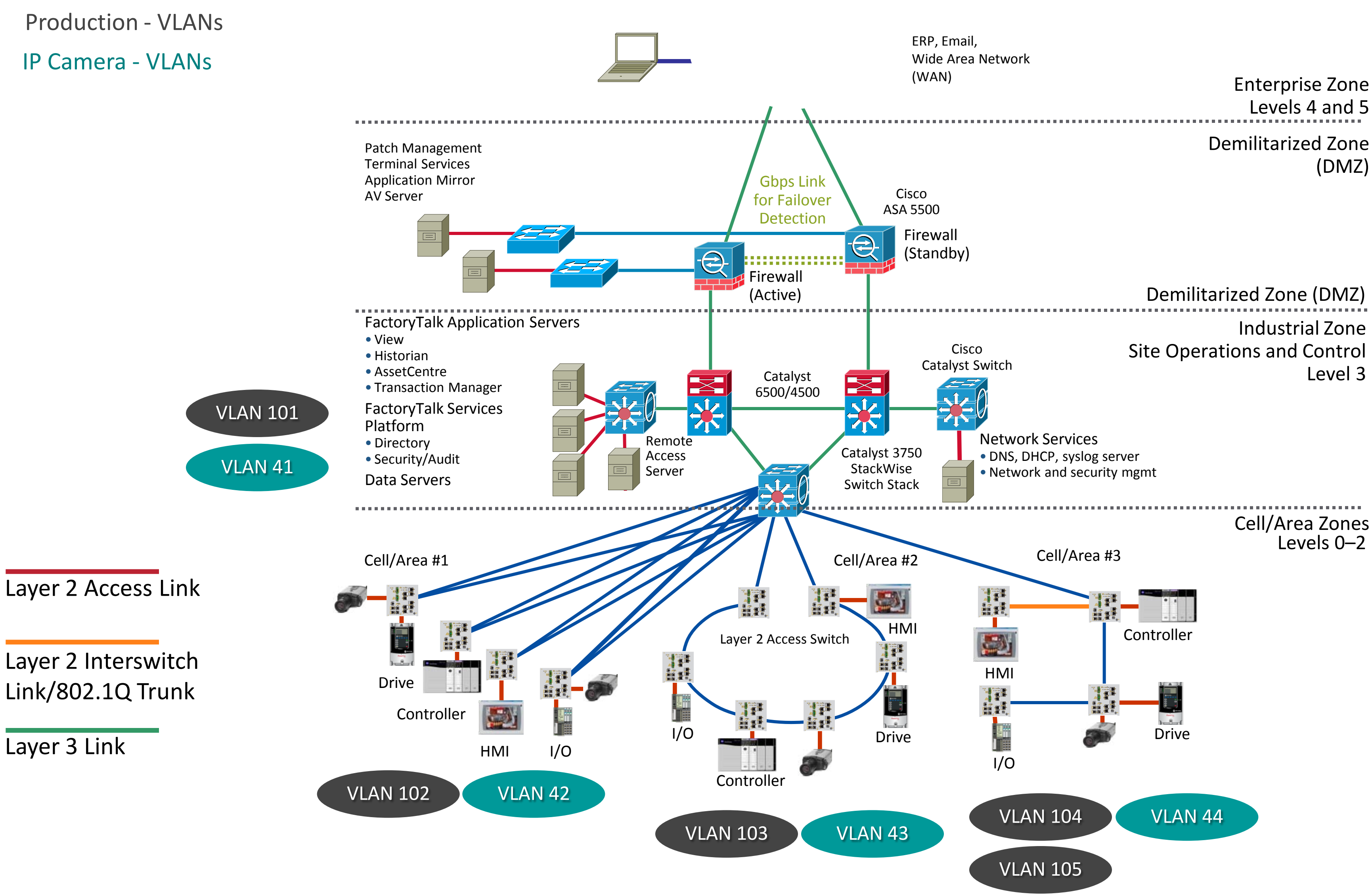
Production - VLANs

IP Camera - VLAN



Segmentation in the Framework

VLANs throughout Converged Plantwide Ethernet Network



Segmentation

VLANs – Design and Implementation Considerations

- Design small Cell/Area zones, segment traffic types into VLANs and IP Subnets to better manage the traffic and establish domains of trust
- Assign different traffic types to a unique VLAN, other than VLAN 1. Traffic types such as control, information, management, native
- Within the Cell/Area zone use Layer 2 VLAN trunking between switches with similar traffic types
- Use Layer 3 Inter-VLAN routing between zones and between switches with different traffic types within the Cell/Area zone

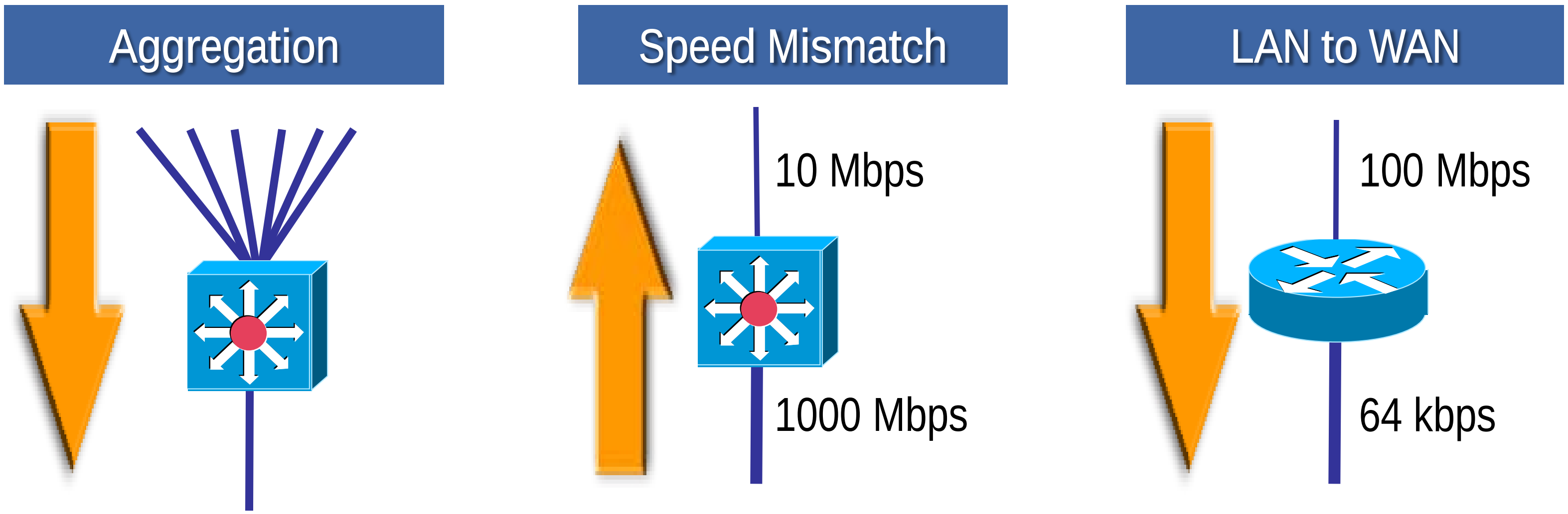
Prioritization

Traffic is Not Created Equal

	Control	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

Industrial Automation and Control System (IACS) Networks **Must** Prioritize Control Traffic over Other Traffic Types to Ensure Deterministic Data Flows with Low Latency and Low Jitter

Prioritization
Quality of Service (QoS)



- 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

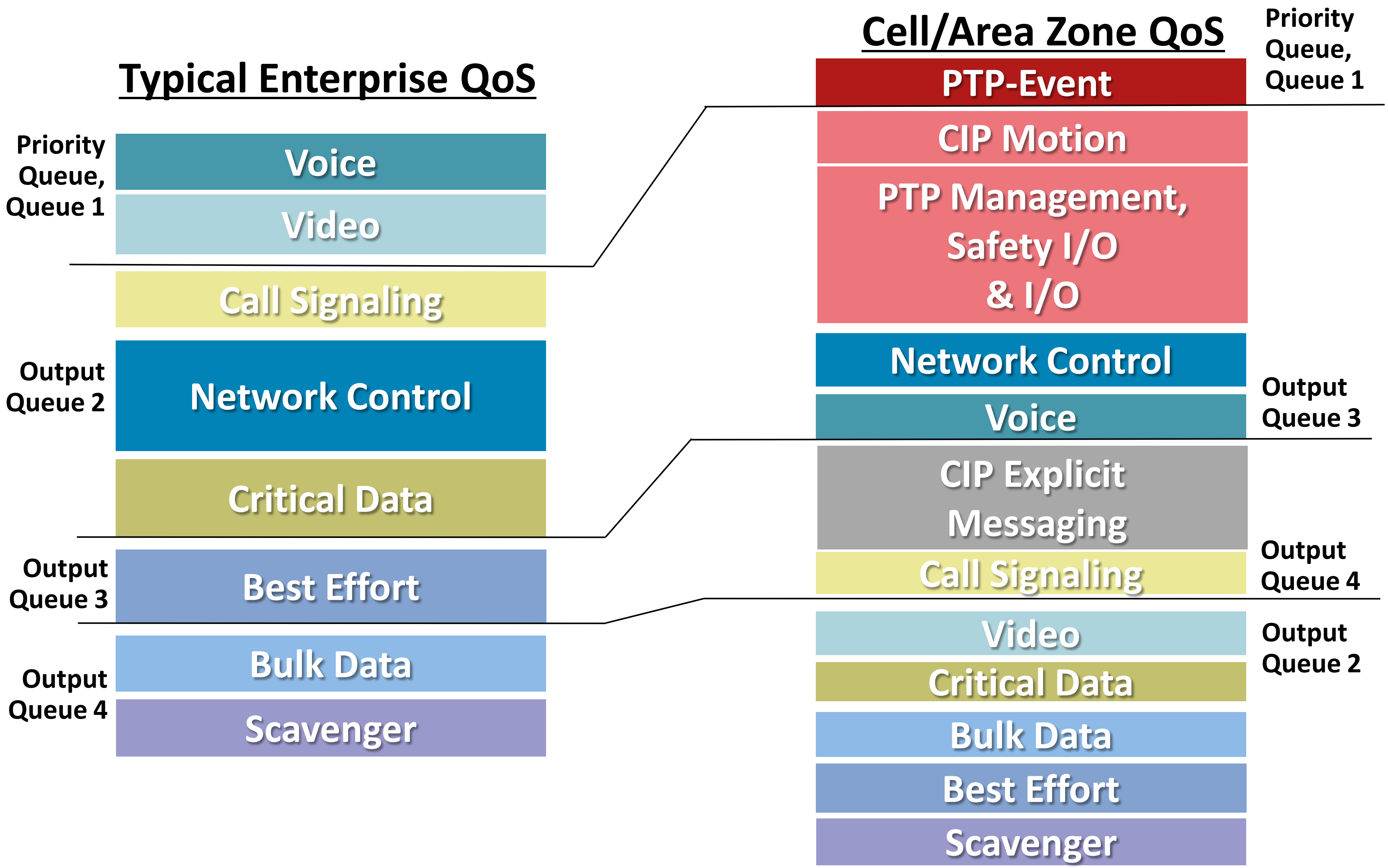
Prioritization
QoS - Operations

Classification and Marking

Queuing and (Selective) Dropping

Post-Queuing Operations

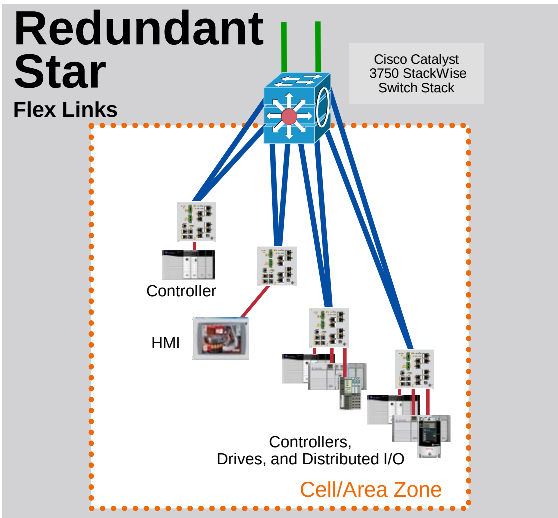
Prioritization
QoS – Cell/Area Zone Priorities

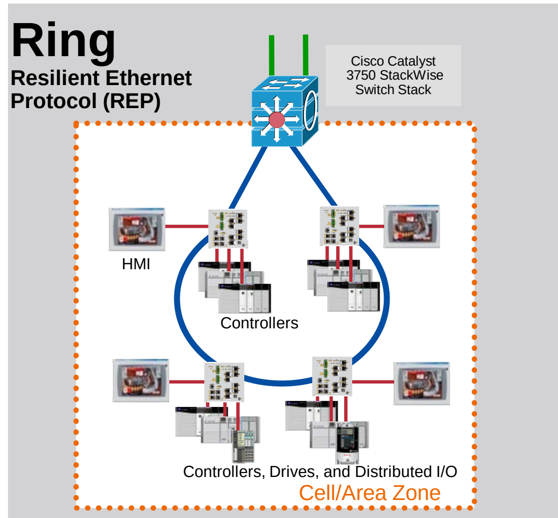


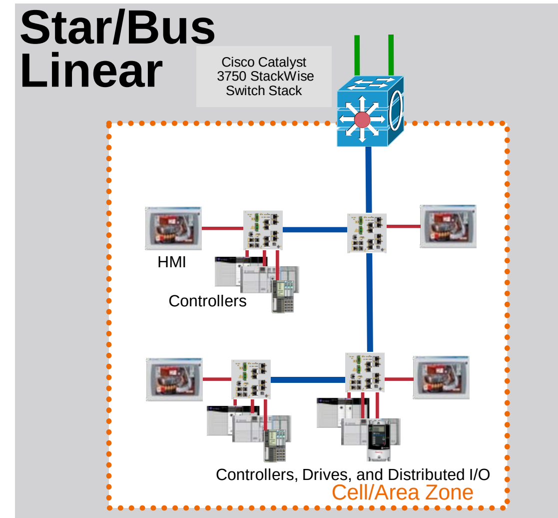
Prioritization
QoS – Design and Implementation Considerations

- Quality of Service does not increase bandwidth.
- QoS gives preferential treatment to Industrial Automation and Control System Network traffic at the expense of other network traffic.
- Deploy QoS consistently throughout Industrial Automation and Control System Network.

Redundant Topologies
Application Considerations

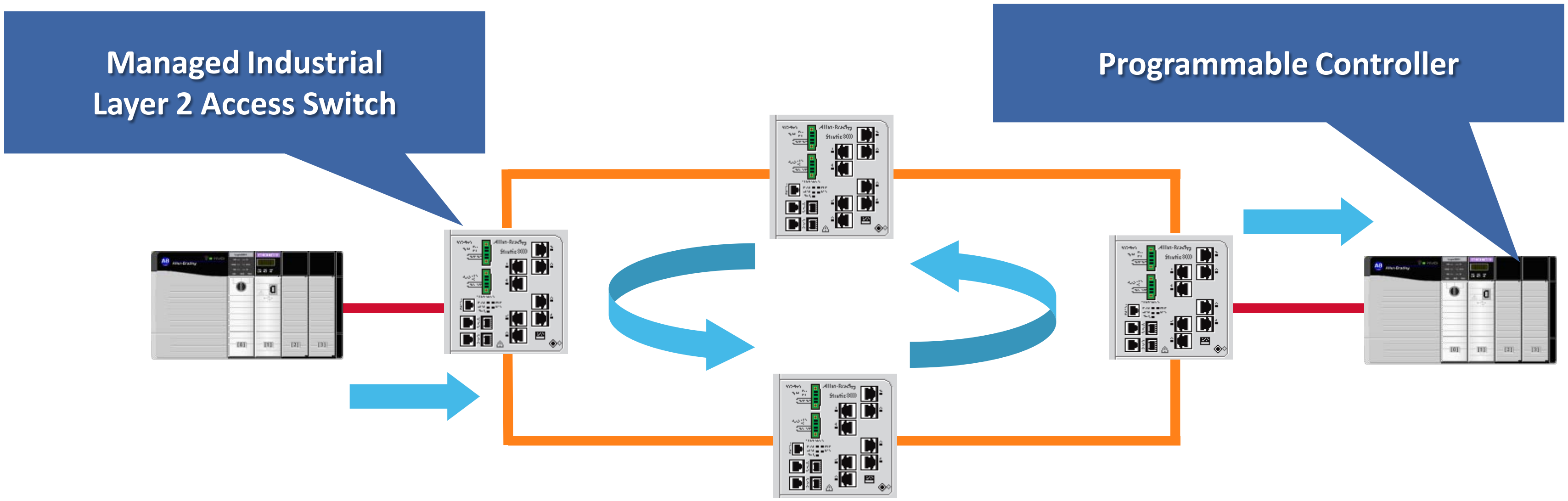






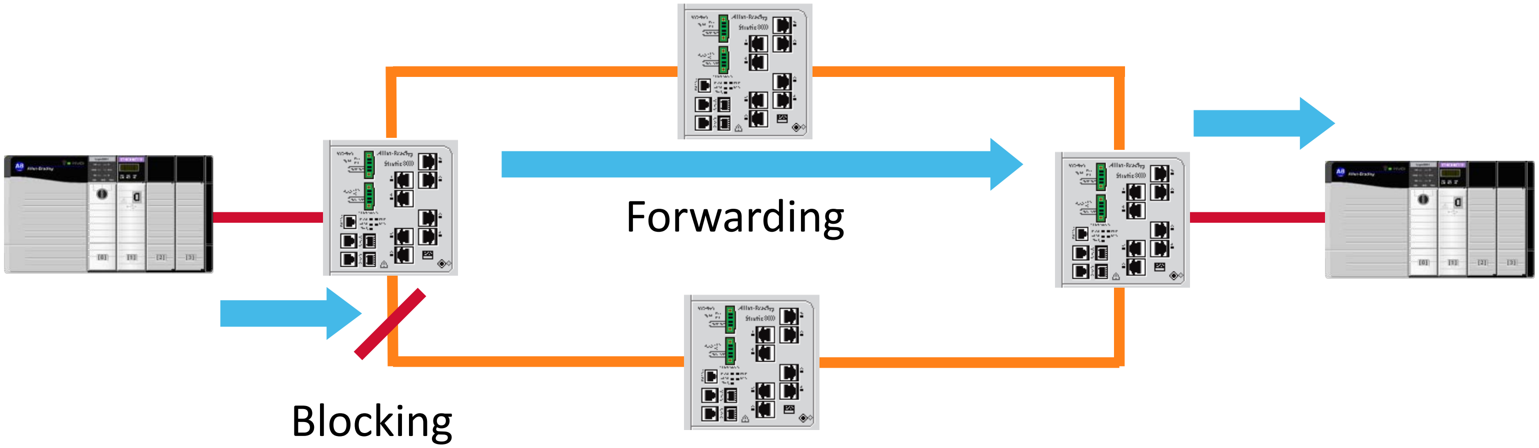
	Redundant Star	Ring	Linear
Cabling Requirements			
Ease of Configuration			
Implementation Costs			
Bandwidth			
Redundancy and Convergence			
Disruption During Network Upgrade			
Readiness for Network Convergence			
Overall in Network TCO and Performance	Best	OK	Worst

Resiliency Protocols and Redundant Topologies
Layer 2 – Loop Avoidance



- Parallel links (paths) create a switching (bridging) loop
  - Layer 2 Ethernet frames do not have a time-to-live (TTL), a frame can loop forever
  - 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

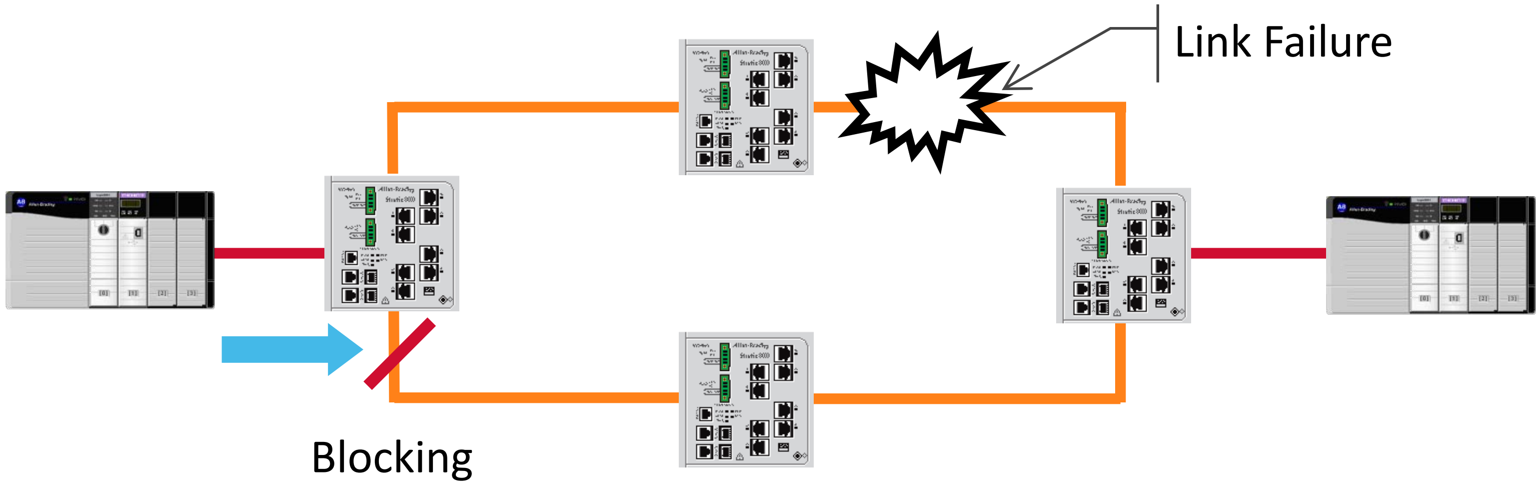
Resiliency Protocols and Redundant Topologies
Layer 2 – Loop Avoidance



- A resiliency protocol maintains parallel links for path redundancy while avoiding loops

Resiliency Protocols and Redundant Topologies

Layer 2 – Loop Avoidance



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

Resiliency Protocols and Redundant Topologies
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 table 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.

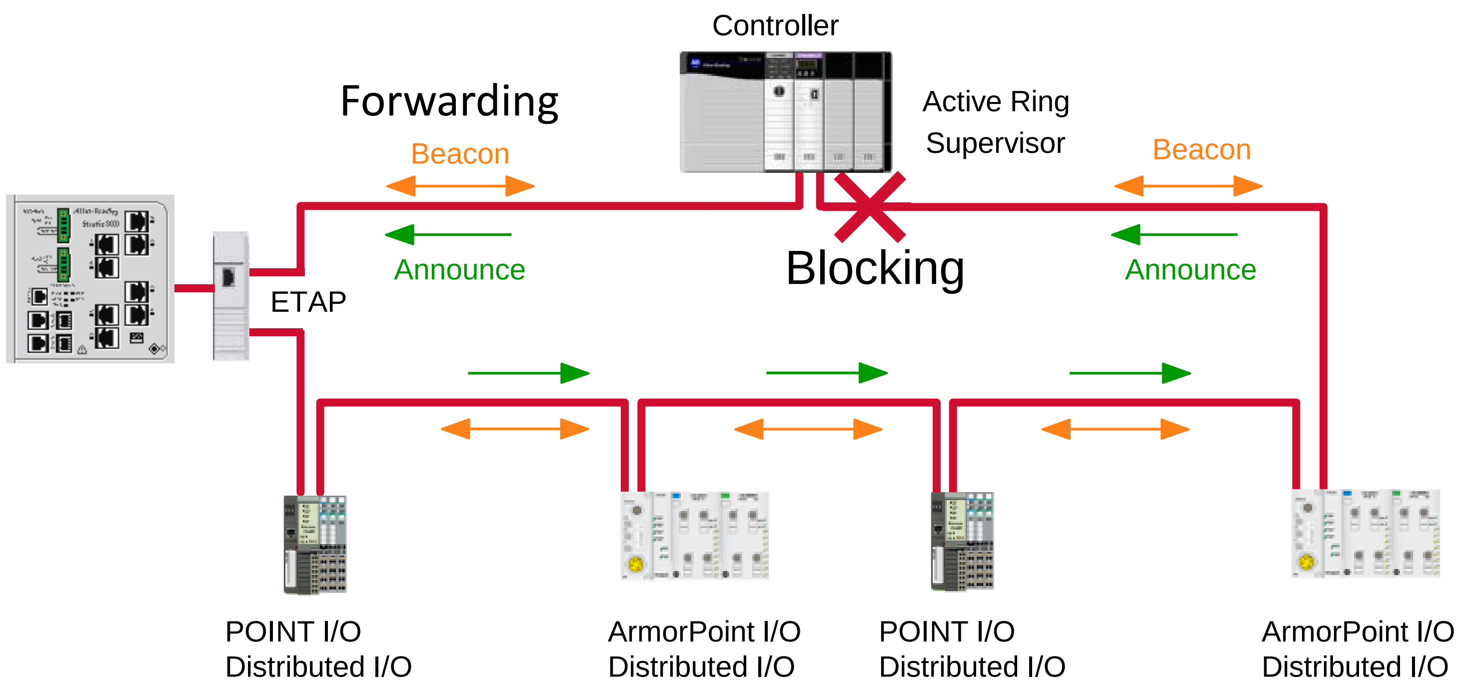
- If the convergence time is longer than the controller's connection timeout, the IACS Ethernet devices on the affected portion of the network may stop operating and <u>bring parts of the plant floor to a halt</u>.

Network Resiliency Protocols

Selection is Application Driven

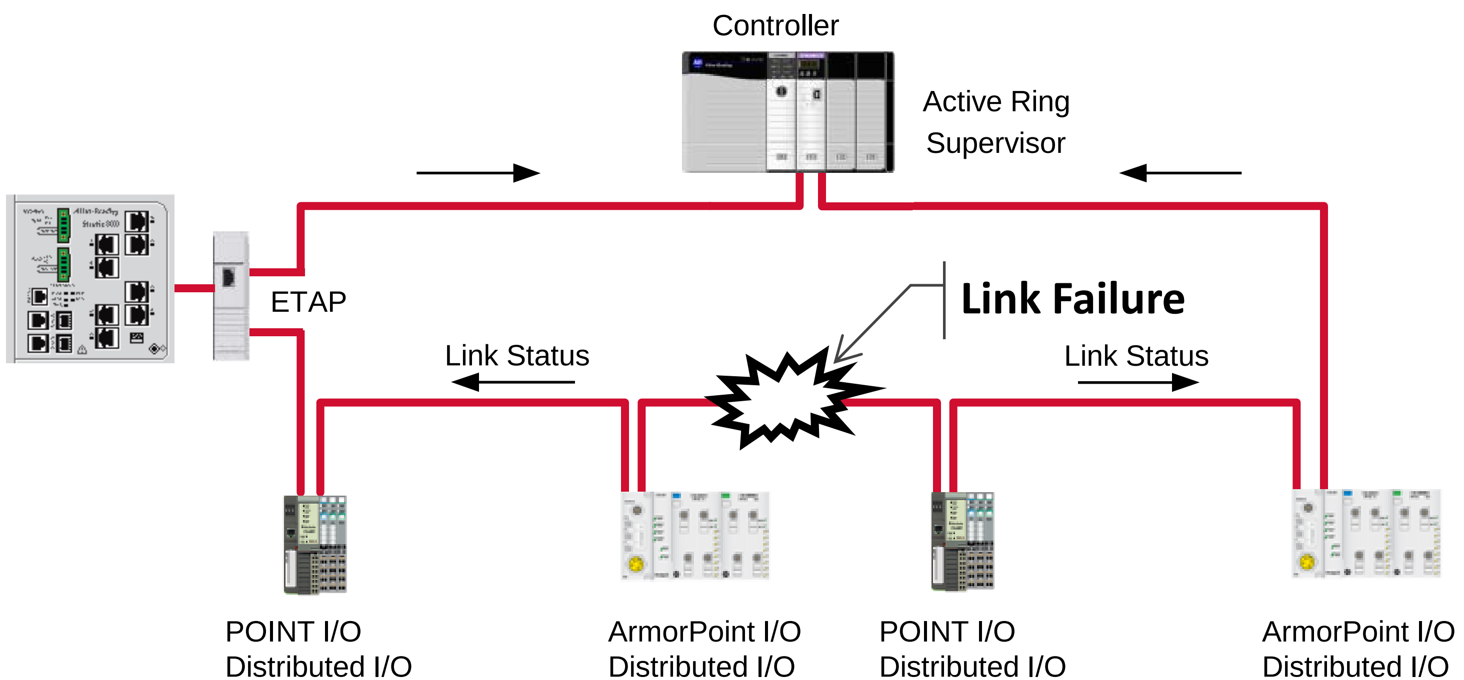
Resiliency Protocol	Mixed Vendor	Ring	Redundant Star	Network Convergence > 250 ms	Network Convergence 60 - 100 ms	Network Convergence 1 - 3 ms	Layer 3	Layer 2
STP (802.1D)	X	X	X					X
RSTP (802.1w)	X	X	X	X				X
MSTP (802.1s)	X	X	X	X				X
rPVST+		X	X	X				X
REP		X			X			X
EtherChannel (LACP 802.3ad)	X		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	

Device Level Ring (DLR)
Control Level Resiliency



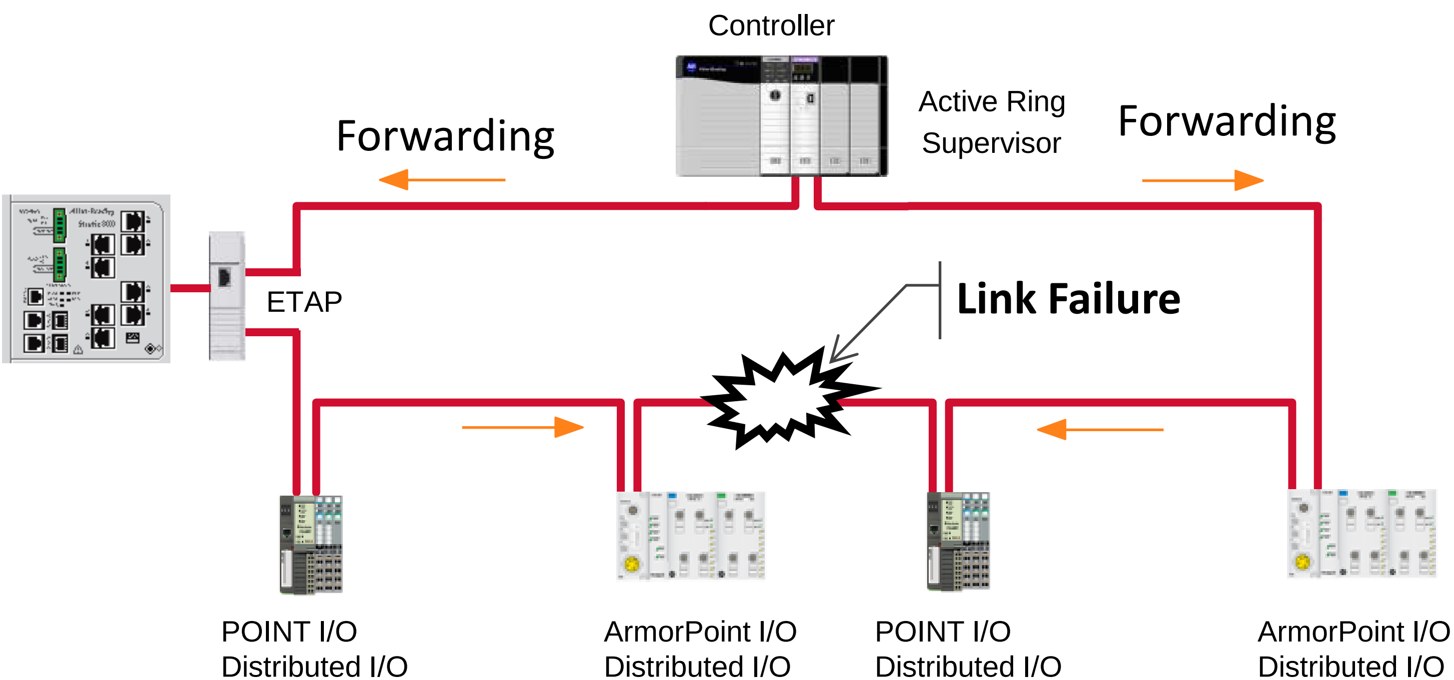
- Supervisor blocks traffic on one port
- Sends Beacon frames on both ports to detect break in the ring
- Sends Announce frames on unblocked port

Device Level Ring (DLR)
Physical Layer Failure



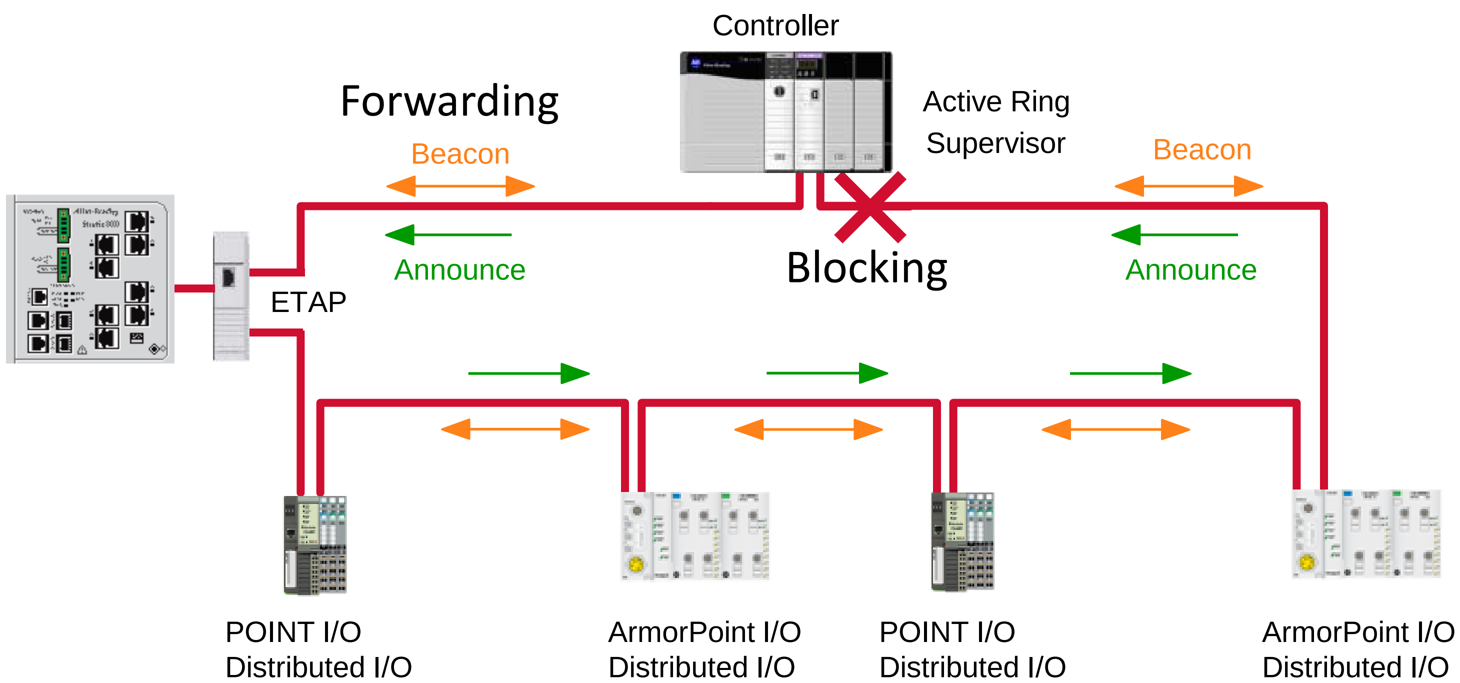
- All faults that are detectable at physical layer
- Physical layer failure detected by protocol-aware node
- Status message sent by ring node and received by ring supervisor

Device Level Ring (DLR)
Network Convergence



- After failure detection, ring supervisor unblocks blocked port
- Network configuration is now a linear topology
- Fault location is readily available via diagnostics

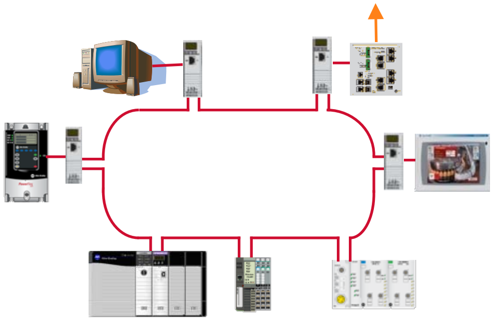
Device Level Ring (DLR)
Control Level Resiliency



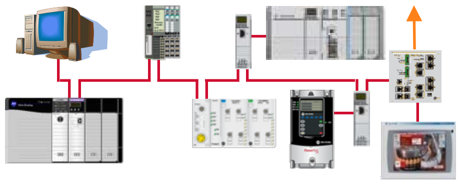
- Once ring is restored, supervisor hears beacon on both ports, and transitions to normal ring mode, blocking one port

Device Level Ring (DLR)
Control Level Resiliency Summary

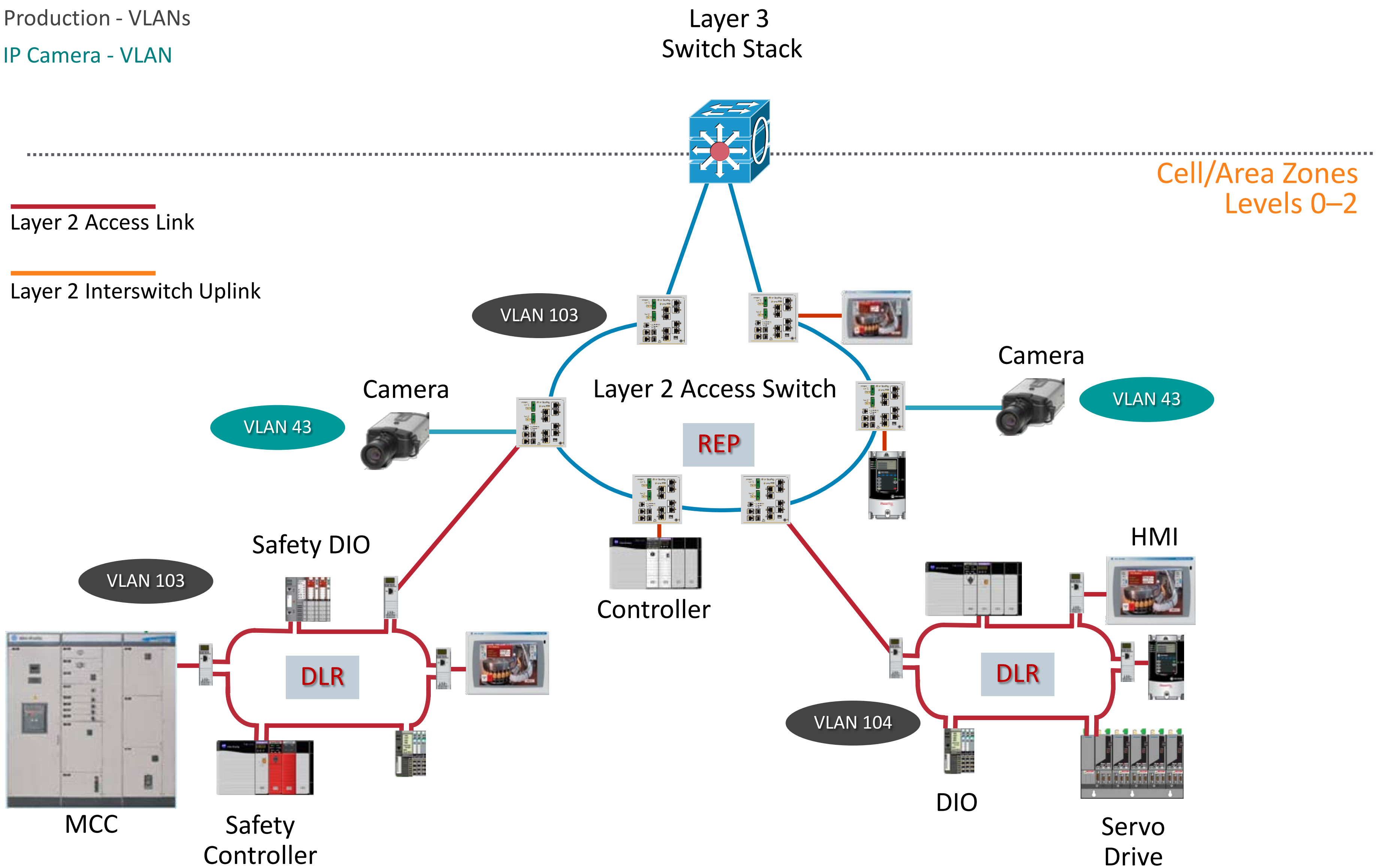
- Open standard (ODVA)
- Network traffic is managed to ensure timely delivery of critical data (Quality of Service, IEEE-1588 Precision Time Protocol, Multicast Management)
- 1-3 ms convergence time for Industrial Automation and Control System (IACS) device networks



- Ring and linear topologies
- Single fault tolerant Ethernet network



Redundant Topologies and Resiliency Protocols
Example: Industrial Automation and Control System



Physical Layer
Installation Pitfalls

It’s strange to think that the same people that demand organization, efficiency, and strict adherence to application requirements…

Yet it happens all the time, in most industrial automation facilities.

… wouldn’t demand the same standards in their plant floor level communication systems.

Physical Layer

More Installation Pitfalls

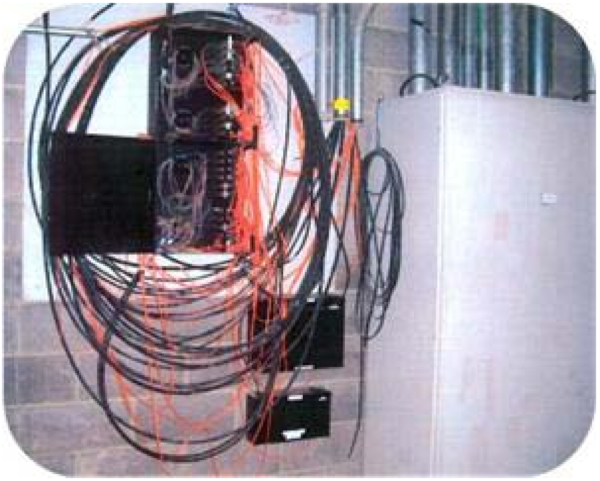
Proper cable installation is critical

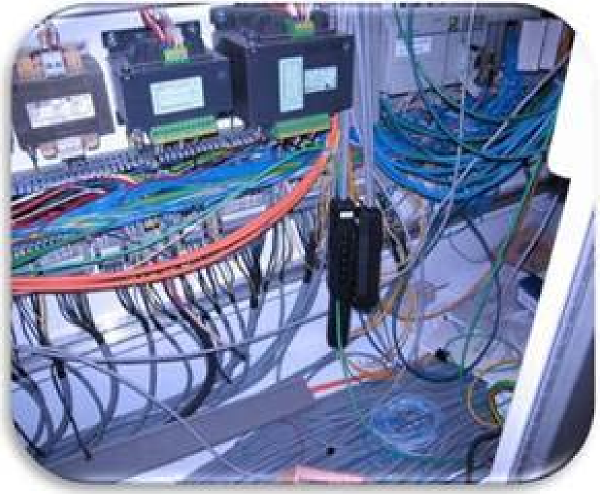
No matter the hardware, shoddy cable installation will result in a poor network

This makes it impossible to manage, maintain and troubleshoot

Critical Manufacturing Assets are at Risk

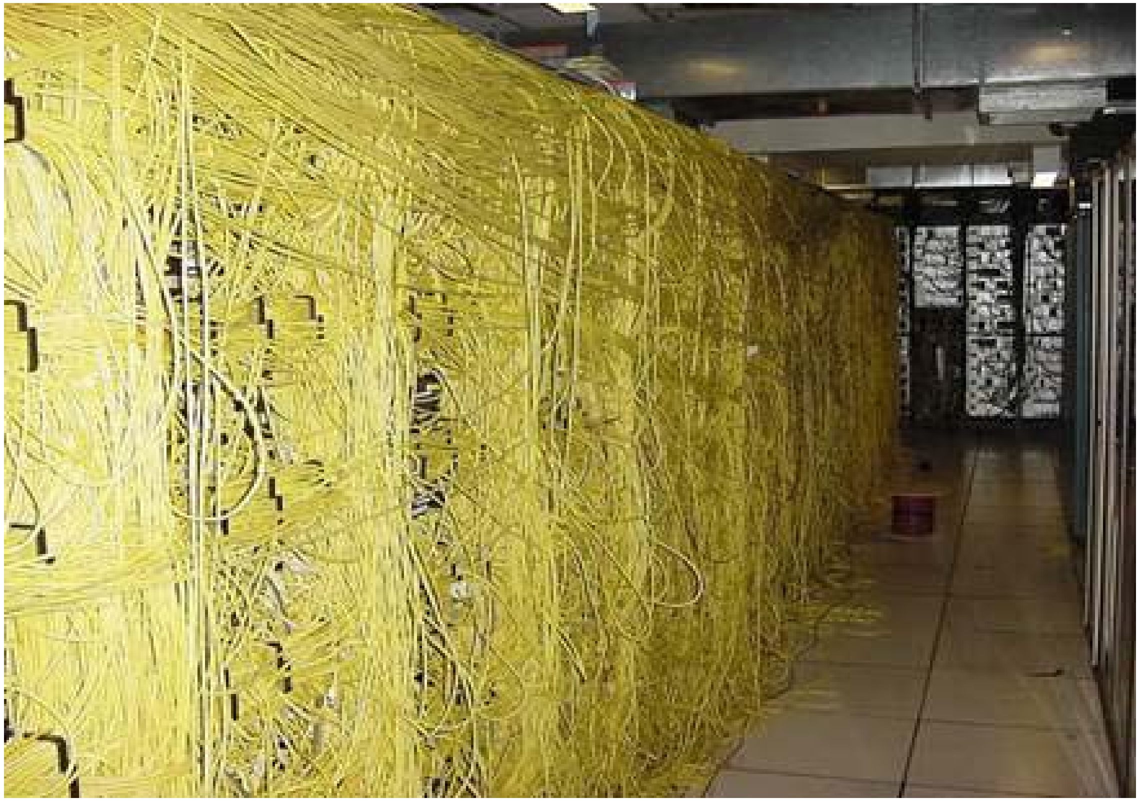
Downtime, Security, Performance issues!



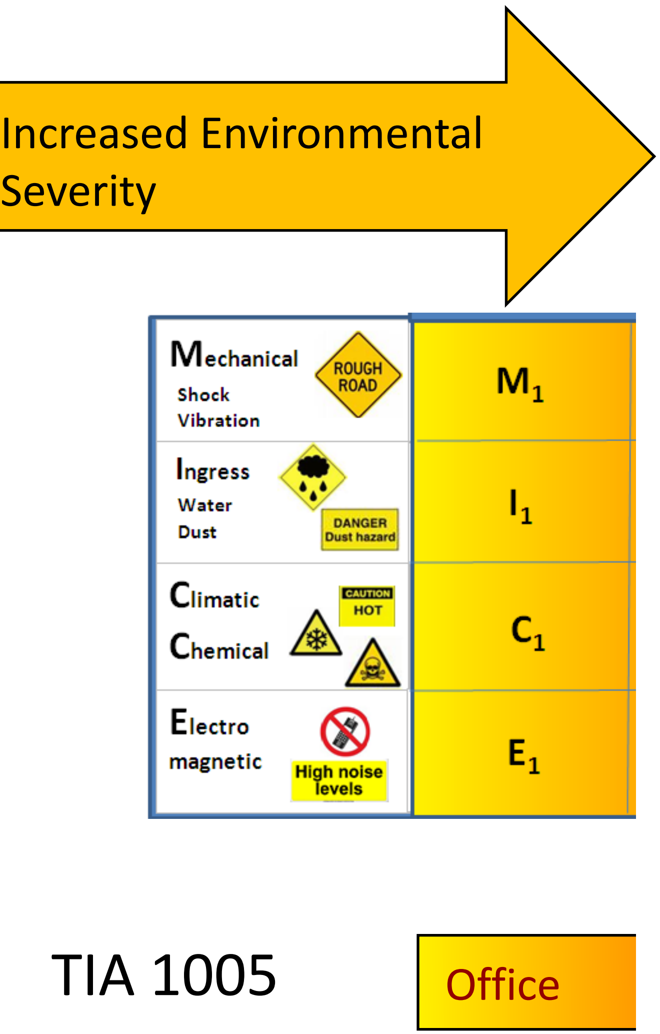


Network Infrastructure

- 80%+ of network problems are physical installation issues



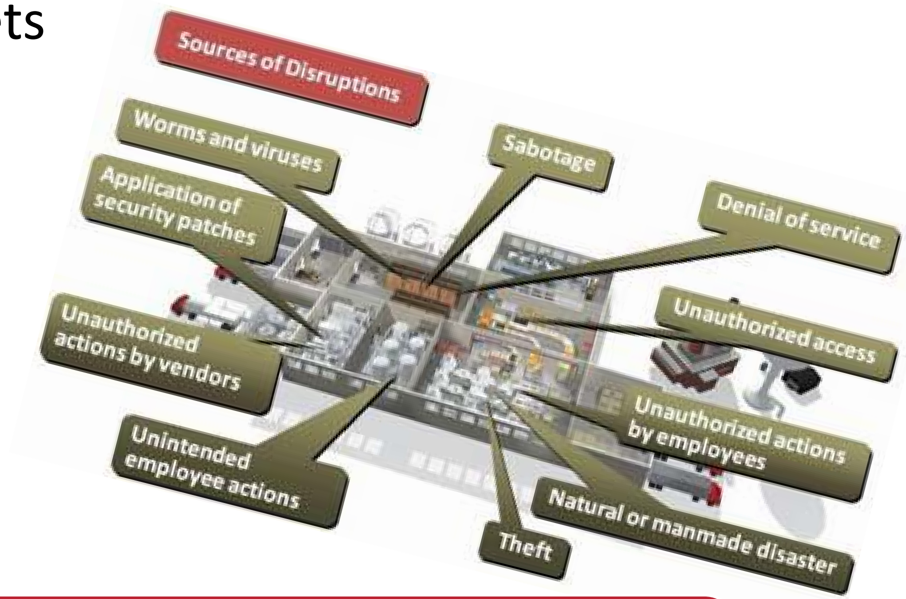
Environmental Focus – M.I.C.E.



- M.I.C.E. provides a method of categorizing the environmental classes for each plant Cell/Area zone.
- This provides for determination of the level of “hardening” required for the network media, connectors, pathways, devices and enclosures.
- 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
- Examples of rating:
  - Cable Media : $M_3I_3C_3E_3$
  - M12: $M_3I_3C_3E_3$
  - RJ-45: $M_1I_1C_2E_2$

Security – Overview

- Threat: An item (person or code in this context) with the intent and capability to exploit a vulnerability in an asset.
  - Malicious hacker, a disgruntled employee, accidental incident or code
- Vulnerability: Weakness in an asset that can be exploited
- Risk: Probability of negative impacts resulting from the interactions between threats and vulnerable assets
  - Impact = Threat + Vulnerability
  - Risk = Severity x Likelihood (of impact)
- Managing risk
  - Accept
  - Transfer
  - Mitigate
  - Avoid



Risk exists in manufacturing IT environment

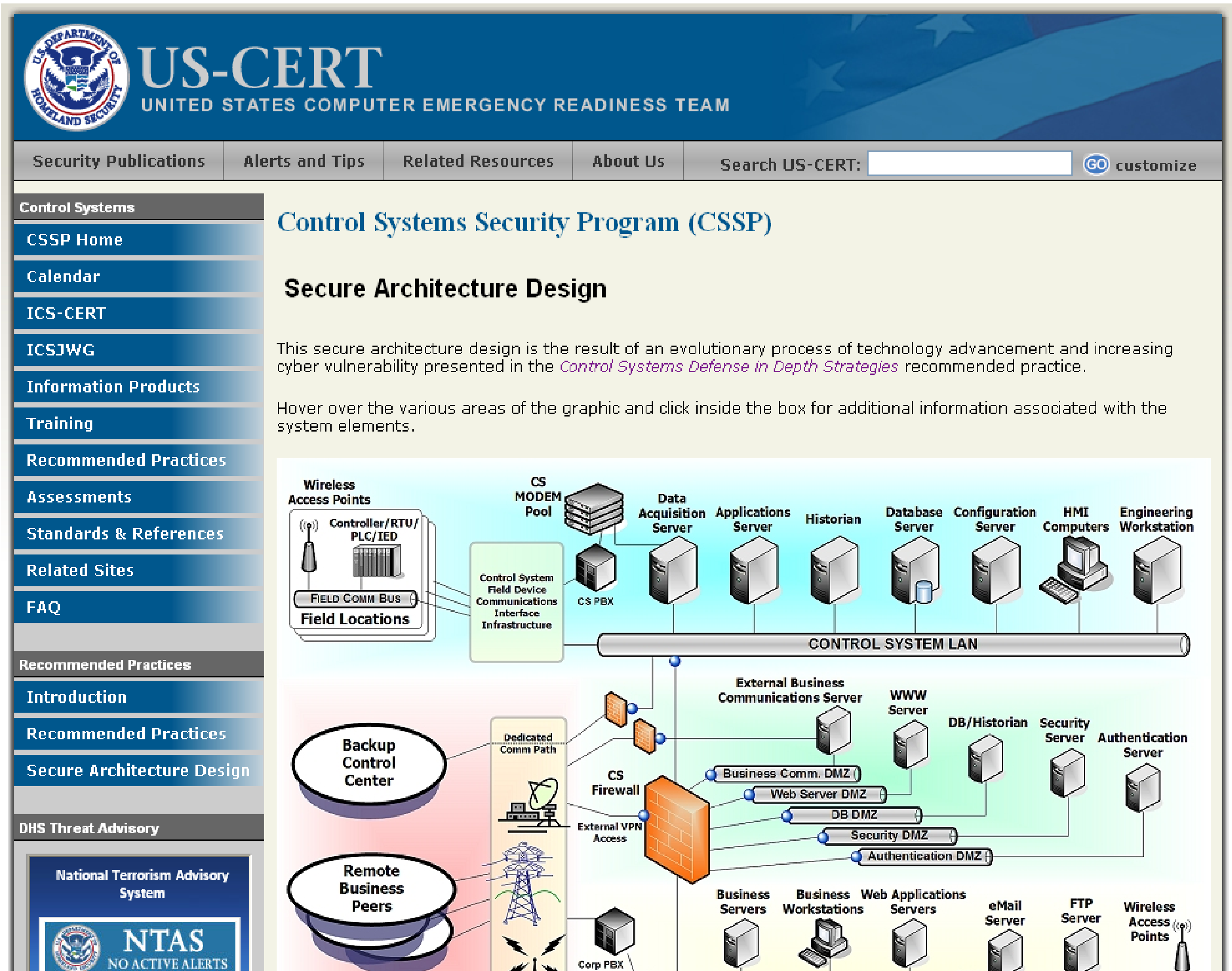
Different Goals and Objectives

Security Policies	IT Network	Controls Network
Focus	Protecting Intellectual Property and Company Assets	24/7 Operations, High OEE
Priorities	**Confidentiality** **Integrity** **Availability**	**Availability** **Integrity** **Confidentiality**
Types of Data Traffic	Converged Network of Data, Voice and Video	Converged Network of Data, Control, Information, Safety and Motion
Access Control	Strict Network Authentication and Access Policies	Strict Physical Access Simple Network Device Access
Implications of a Device Failure	Continues to Operate	Could Stop Operation
Threat Protection	Shut Down Access to Detected Threat	Potentially Keep Operating with a Detected Threat
Upgrades	ASAP During Uptime	Scheduled During Downtime

DHS National Cyber Security Division

Control System Security Program

http://www.us-cert.gov/control_systems/



The foundation of every network is the physical layer

Thank You!