Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

Industrial Networking Concepts, Design, Resilience and Security

BRKRST-2661

Housekeeping

- We value your feedback- don't forget to complete your online session evaluations.
- Please remember this is a 'non-smoking' venue!
- Please make use of the recycling bins provided
- Please switch off your mobile phones
- Please remember to wear your badge at all times
- Informational slides may not be presented





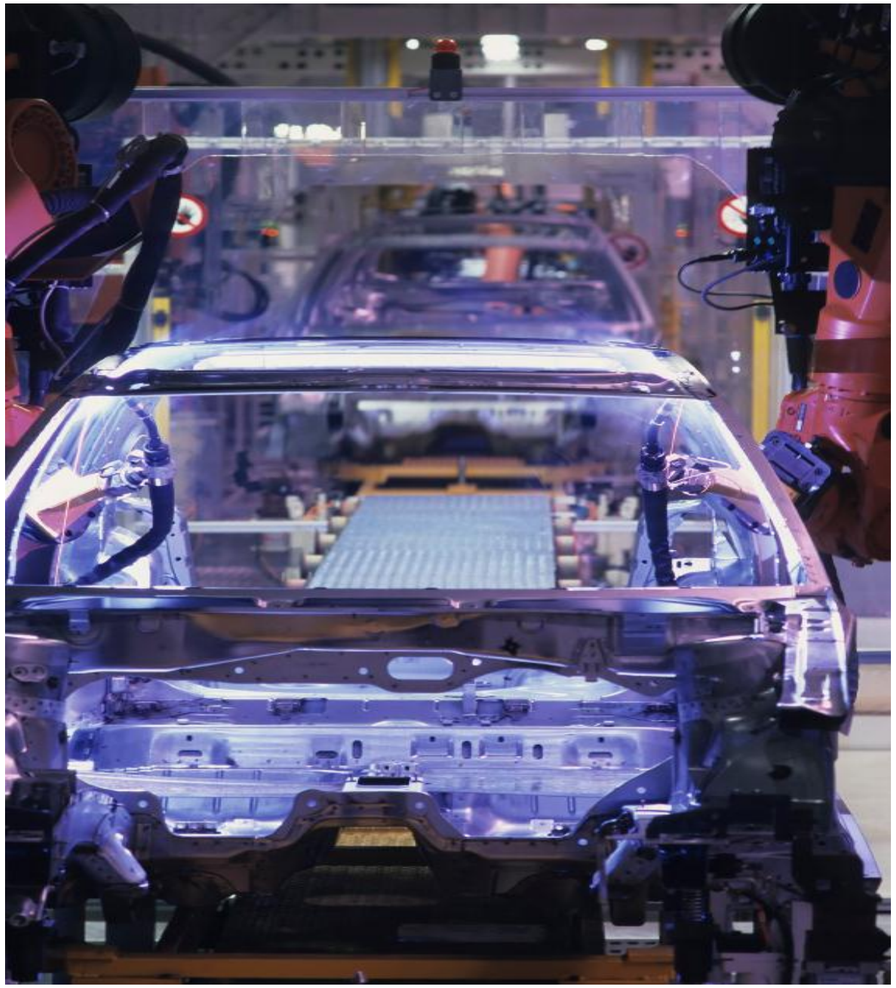

Session Abstract

Session Title: Connected Industry Architectures and Technologies

- This 90min session is an introduction to Industrial Networking including industry trends, commonly used products, protocols and associated technologies. The speaker will also introduce Cisco's Converged Plant-wide Ethernet architecture for Industrial Networking and will discuss design considerations including industrial applications, network topology choices, performance considerations, network resilience and redundancy, security trends and defence in depth for industrial networks including secure remote access solutions.

Agenda

- Industry Trends
- Connected Industry Architectures
- Design Considerations
- Q&A
- Recommended Resources



The Evolution of IP Networks

The Internet of Everything - The Third Great Era

Industrial and Enterprise Networks Are Converging

Connected Industries Business Unit

Born Jan 2012 - Driving IT and OT Convergence

Verticals

- Process Mfg. Oil & Gas
- Discrete Mfg.
- Transportation
- Machine to Machine
- Connected Vehicle

Smart Solution

- Converged Plant
- Machine Builder
- Road & Rail Network Infrastructure
- Connected Machine
- Connected Vehicle

Industry Partners

- Rockwell Automation
- Honeywell
- EMERSON Process Management

\+ Cisco Advanced Services

IoE Enablers

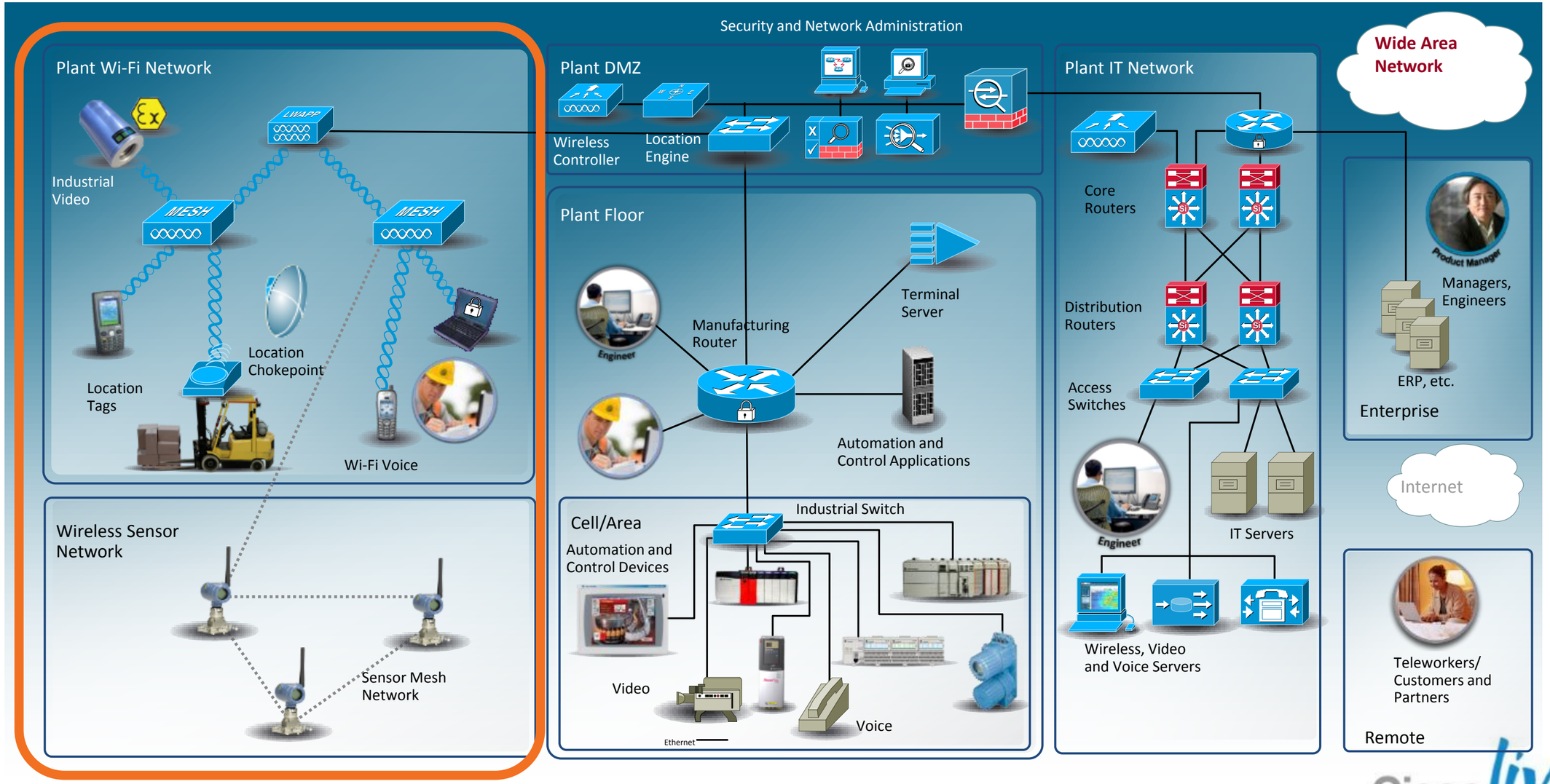
- Time Sync
- Pervasive Security
- Scalable Routing
- Deterministic Ethernet
- Guaranteed Delivery
- Big Data Management

Ruggedized Products

- Ruggedized Wireless AP
- Industrial Routers & Switches
- Industrial Security
- Hardened Mobile M2M Gateway

Converged Plant Floor Architecture

Plant Floor Safely and Securely Connected with the Enterprise



Renewed Focus On Industrial Network Security

Commonly Reported Business Disruptions

Application of Security patches

Natural or Man-made disasters

Worms and viruses

Theft

Sabotage

Denial of Service

Unauthorised access

Unauthorised actions by employees

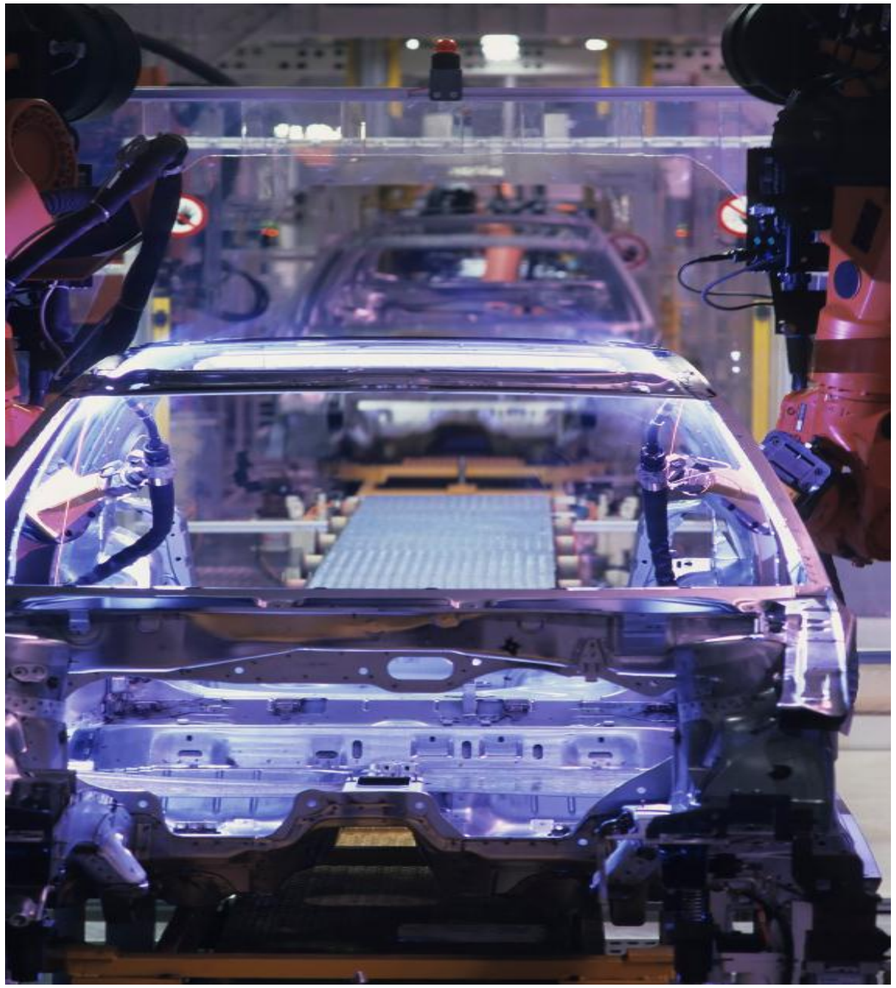
Unauthorised remote access

Unintended employee actions

Unaddressed security risks increase potential for disruption to control system's uptime and safe operation

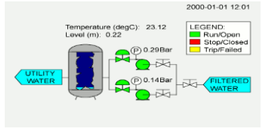
Agenda

- Industry Trends
- Connected Industry Architectures
  - Applications and Protocols
  - Architectures
  - Solutions and Technologies
- Design Considerations
- Q&A
- Recommended Resources



Typical Applications and Systems

MES - Manufacturing Execution System



SCADA - Supervisory Control and Data Acquisition

Historian

PLC/PAC - Programmable Logic (Automation) Controller

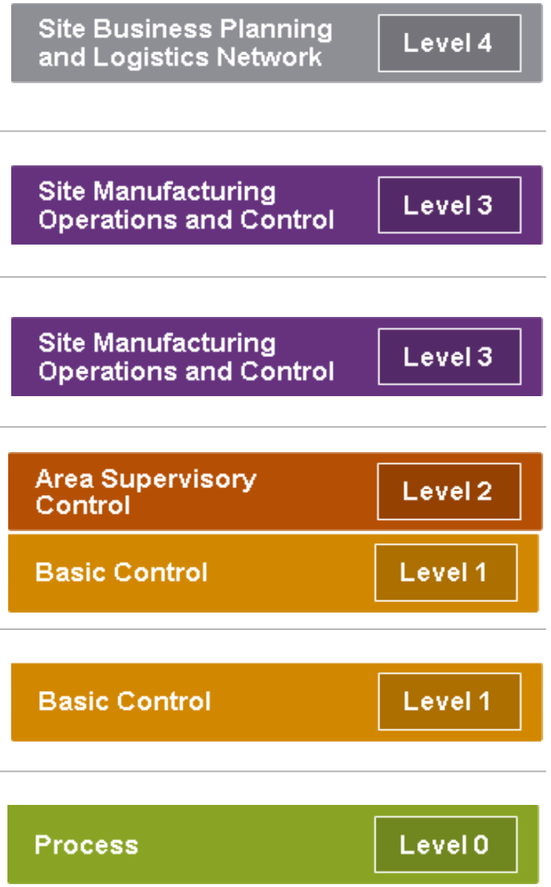
HMI - Human Machine Interface

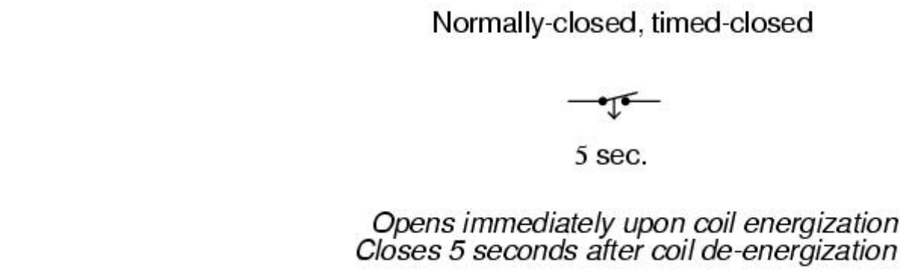
I/O - Input / Output

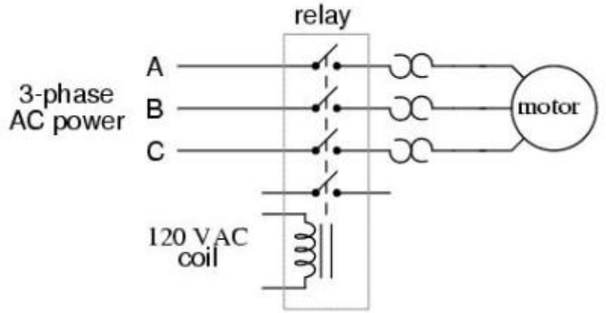
Industrial Lexicon 101

Typical Applications and Systems

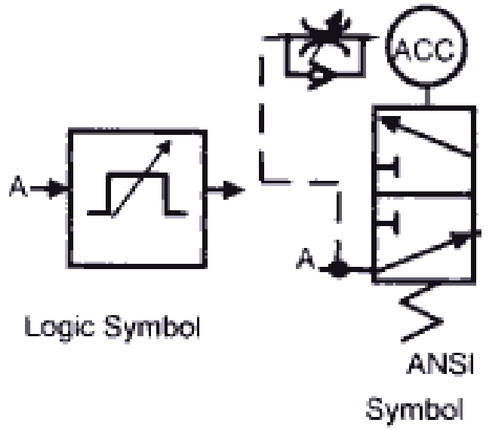
- MES—Manufacturing Execution System measures and controls production facilities; it tracks and measures key operational criteria such as product, equipment, labor, inventory, defects, etc.; a key interface to the Enterprise-level applications
- Historian—Collects historical data from the factory floor applications and reports or displays them in various report formats. Level 3
- SCADA—Supervisory Control and Data Acquisition; large scale distributed measurement and control systems, usually covers a geographical area
- PAC (a.k.a. PLC)—Programmable Automation Controller or Programmable Logic Controller; controls a subset (cell/area) of manufacturing, e.g. a line or function, as well as the relevant devices in that cell/area
- HMI—Human Machine Interfaces display operational status to manufacturing personnel and may allow them to perform basic functions (e.g. start/stop a process)
- I/O—Input/Output device; a device that measures or controls key functions or aspects of the manufacturing process; Level 0

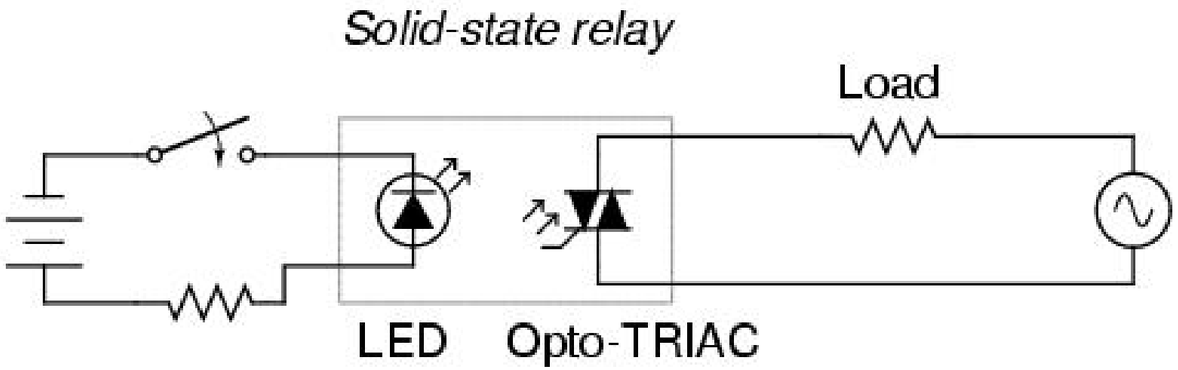


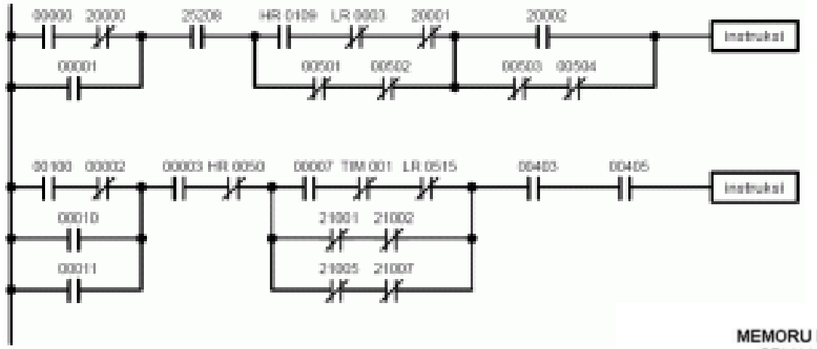




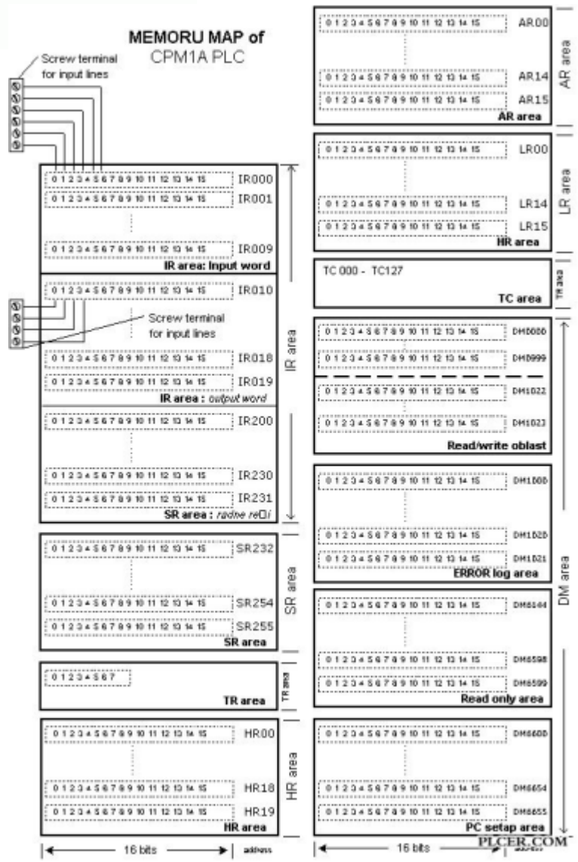
In the beginning



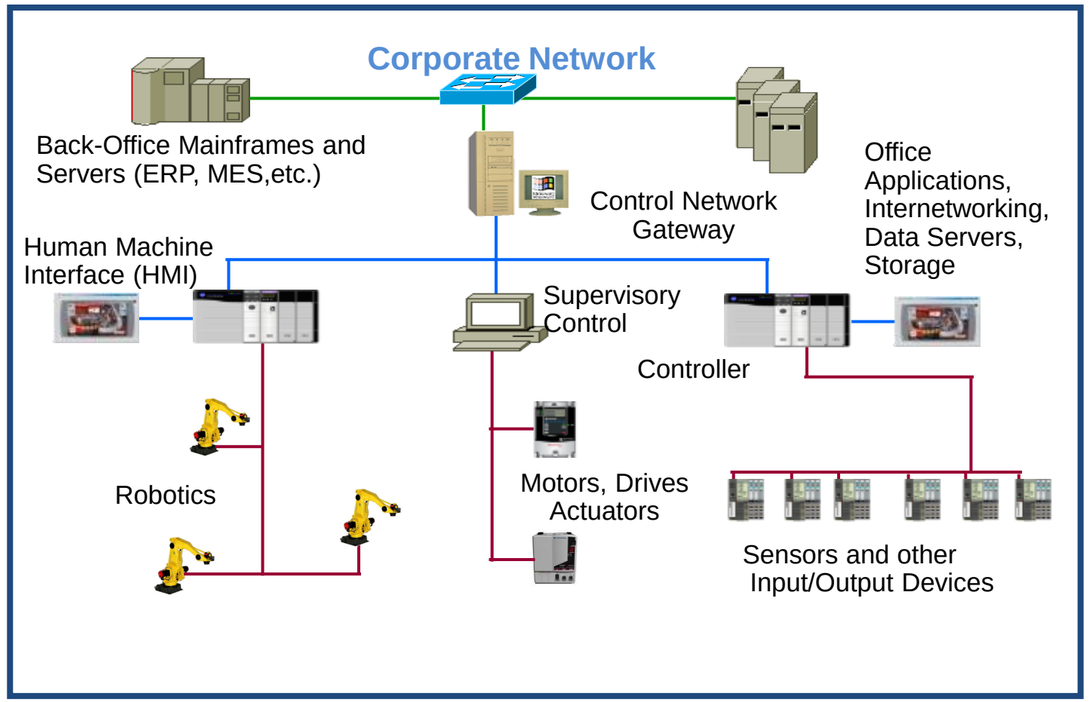




…then along came the PLC…



…which could be “networked” (sort of!)



Common Industrial Automation Protocols

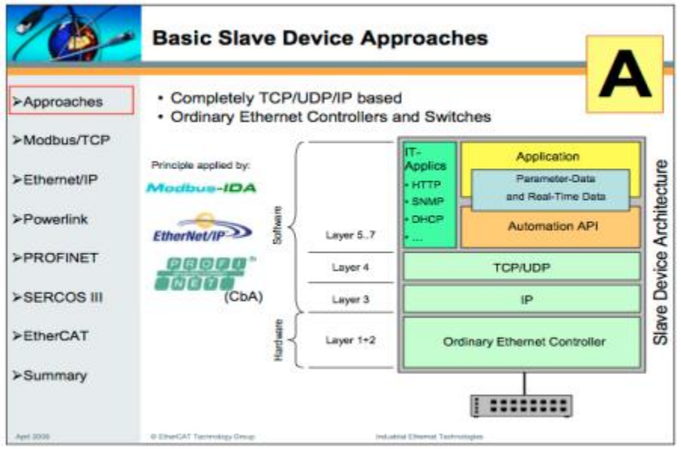
Not exhaustive, see: http://en.wikipedia.org/wiki/List_of_automation_protocols

- CIP - application layer common to DeviceNet, CompoNet, ControlNet and EtherNet/IP
- EtherCAT - an open high performance Ethernet-based fieldbus system.
- EtherNet/IP - IP stands for "Industrial Protocol". An implementation of CIP.
- Ethernet Powerlink – a deterministic open protocol managed by the Ethernet POWERLINK Standardization Group.
- FOUNDATION fieldbus – H1 & HSE – L2 serial standard to coincide with Profibus/Modbus etc.
- HART Protocol - Used to communicate over legacy 4-20 mA analogue instrumentation wiring.
- Modbus RTU or ASCII or TCP
- Profibus/Profinet – by PROFIBUS International, Siemens centric.
- SERCOS – Primarily used by drive systems. Ethernet-based version is SERCOS III
- OPC – OLE for Process Control. A “babel-fish” for control systems.
- CC-Link Industrial Networks, supported by CC-Link Partner Association. CC-Link IE is Ethernet based.
- DNP3 – Distributed Network Protocol. Used in large scale process networks, e.g. water and electricty.
- IEC 61850 - A standard for the design of electrical substation automation, including protocols.

A Plethora of Standards and Protocols

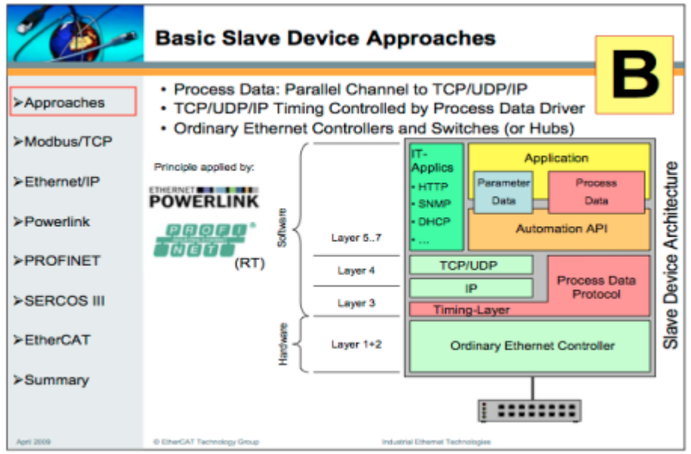
Familiar story – drive to consolidate standards and protocols

Standard Network Stack



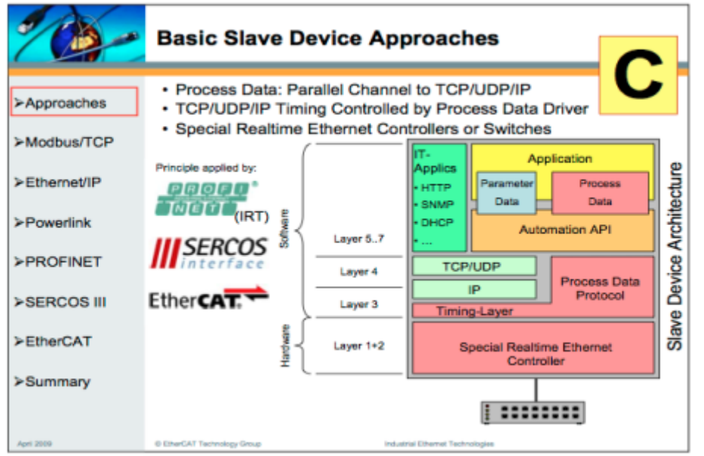
- Based on Open Standards at layers 1-4
- Use of IEEE 1588 Precision Time Protocol (PTP) for further determinism
- Viewed as slow or non-deterministic

Modified Network Stack



- Modify layers 2 & 3
- Carries normal IP traffic with lower priority
- Schedules IACS traffic
- All network infrastructure must support the enhancements
- Uses enhanced switches

Encapsulated Ethernet

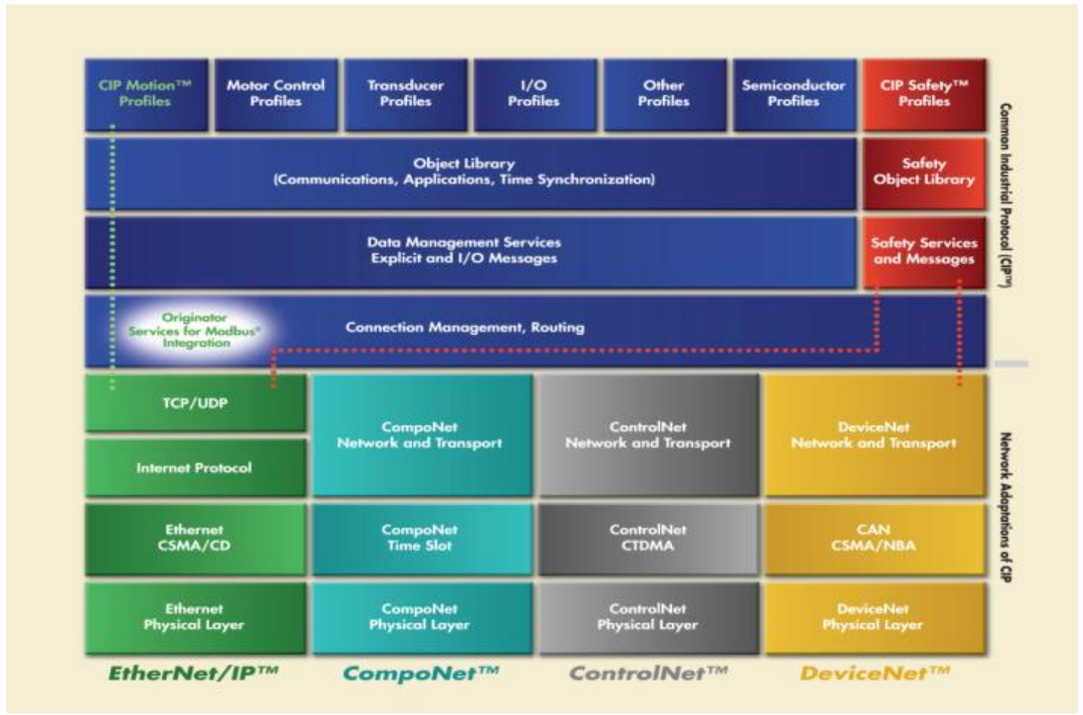


- Often not a “switched” network
- Modify layers 1 - 3 – scheduling and timing
- Encapsulates Ethernet - IP traffic
- Gateway required to interconnect with standard network
- All network infrastructure for IACS must support the protocol

What is EtherNet/IP and CIP

Common Industrial Protocol

- Standard to integrate I/O control, device configuration and data collection in automation and control systems
- Supports three network protocols. EtherNet/IP is based on Ethernet, IP and TCP/UDP
- Supported by the Open Device Vendor Association
- Key communication includes:
  - CIP: Control traffic (a.k.a. Implicit traffic)
    - I/O control, drive control, Produced/Consumed tags
    - Uses UDP protocol (multi-cast and uni-cast)
  - CIP: Information traffic (a.k.a. Explicit traffic)
    - HMI, MSG's, Program upload/download
    - Uses TCP protocol
  - Other common traffic
    - HTTP, Email, SNMP, etc.



ODVA: www.odva.org

What are Profinet IO, Profinet RT and Profinet IRT

Input/Output, Real-time and Isochronous Real-time

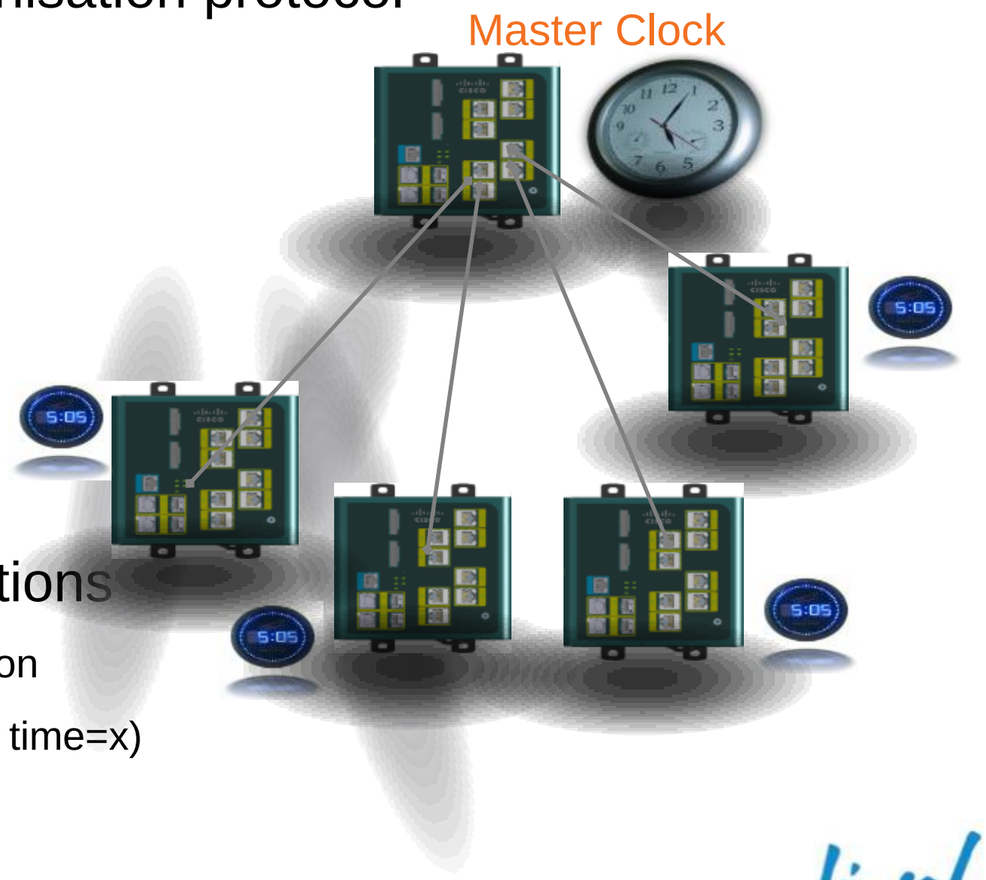
- PROFINET IO defines fast data exchange between distributed field devices and follows the provider-consumer model
- PROFINET RT – Communication class of PROFINET IO
  - Transmission of data and alarms
  - Cycle times of 5-10ms
  - Uses standard Ethernet
- PROFINET IRT – Communication class of PROFINET IO
  - High speed multi-axis motion control
  - IRT capable devices have integrate switches
  - Data cycle times of few 100µs to a few ms
  - High degree of determinism. Start of cycle can only deviate 1µs
  - Uses non-standard Ethernet and proprietary silicon
- PROFINET uses GSD file (General Station Description) to describe properties and functions of field devices.

PROFI INDUSTRIAL ETHERNET NET

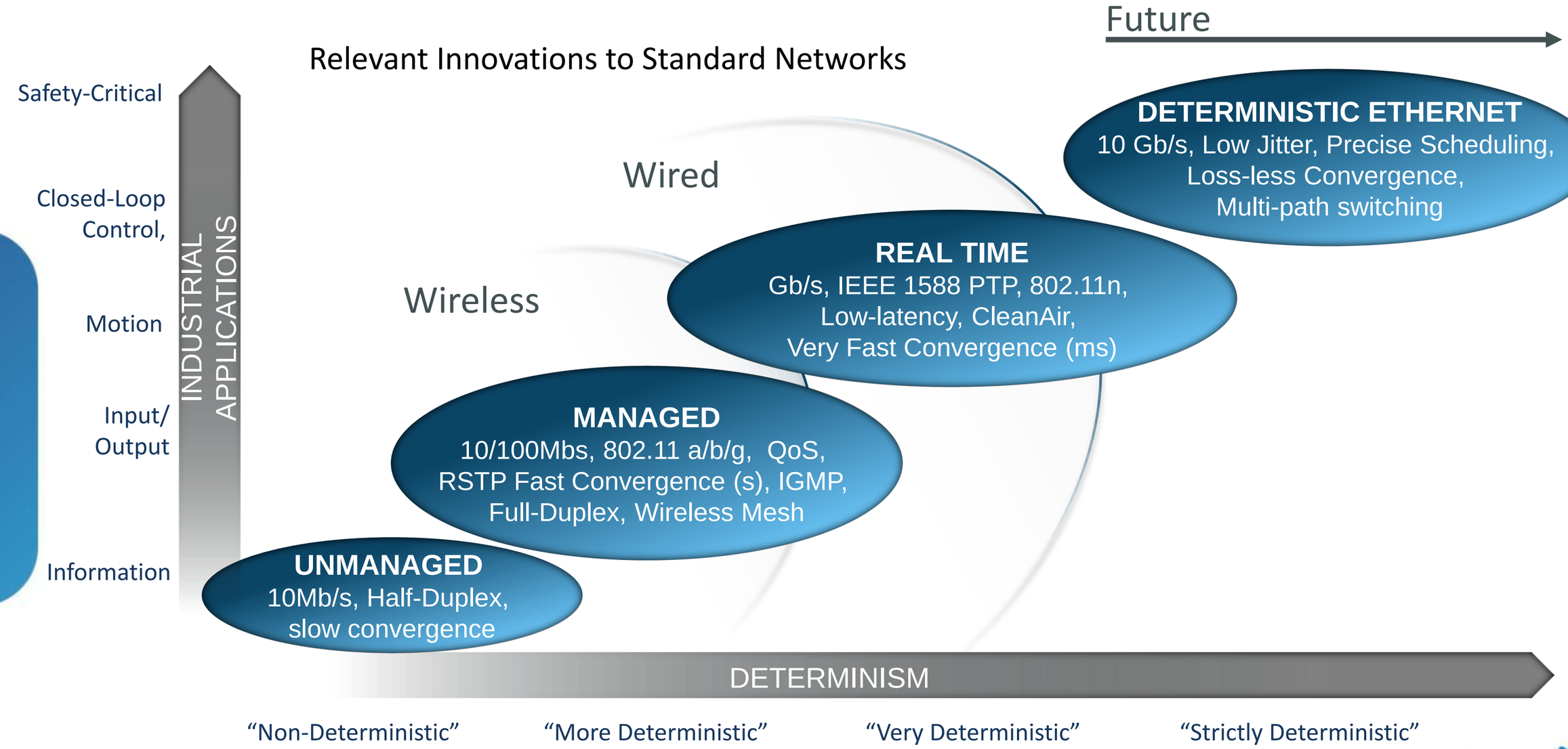
www.profibus.com

Industrial Time Synchronisation

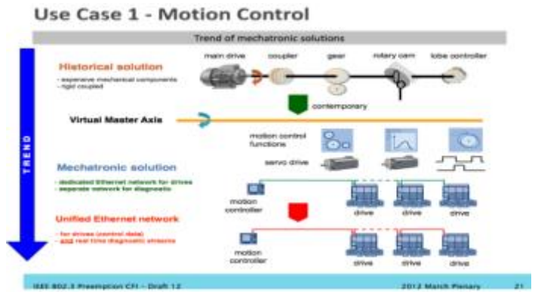
- Distributed control components to share a common notion of time
- Implements IEEE-1588 precision clock synchronisation protocol
  - Provides +/- 100 ns synchronisation (hardware-assisted clock)
  - Provides +/- 100 µs synchronisation (software clock)
- Time Synchronised Applications such as:
  - Input time stamping
  - Alarms and Events
  - Sequence of Events recording
  - Time scheduled outputs
  - Coordinated Motion
- Required in high performance industrial applications
  - Motion control requires sub-micro second accuracy and precision
  - The high-precision activity is scheduled (ex: all systems stop at time=x)
  - Also used within the Finance Arena to time stamp transactions.

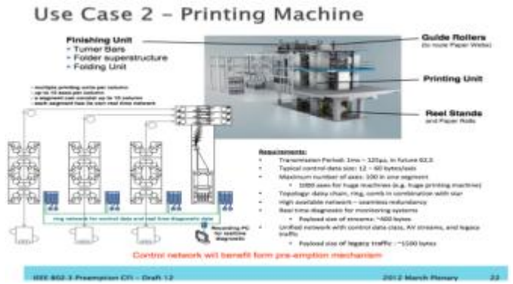


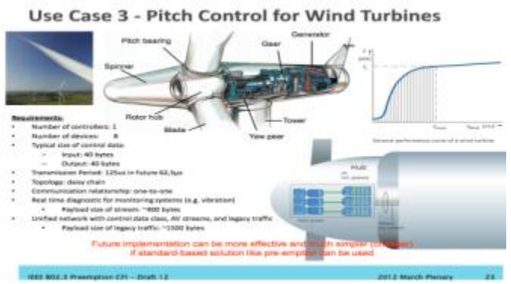
Industrial Communications Requires Evolution

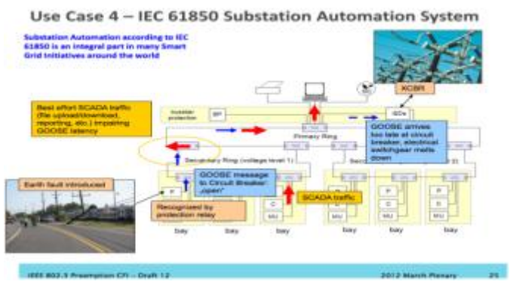


Deterministic Ethernet Standards





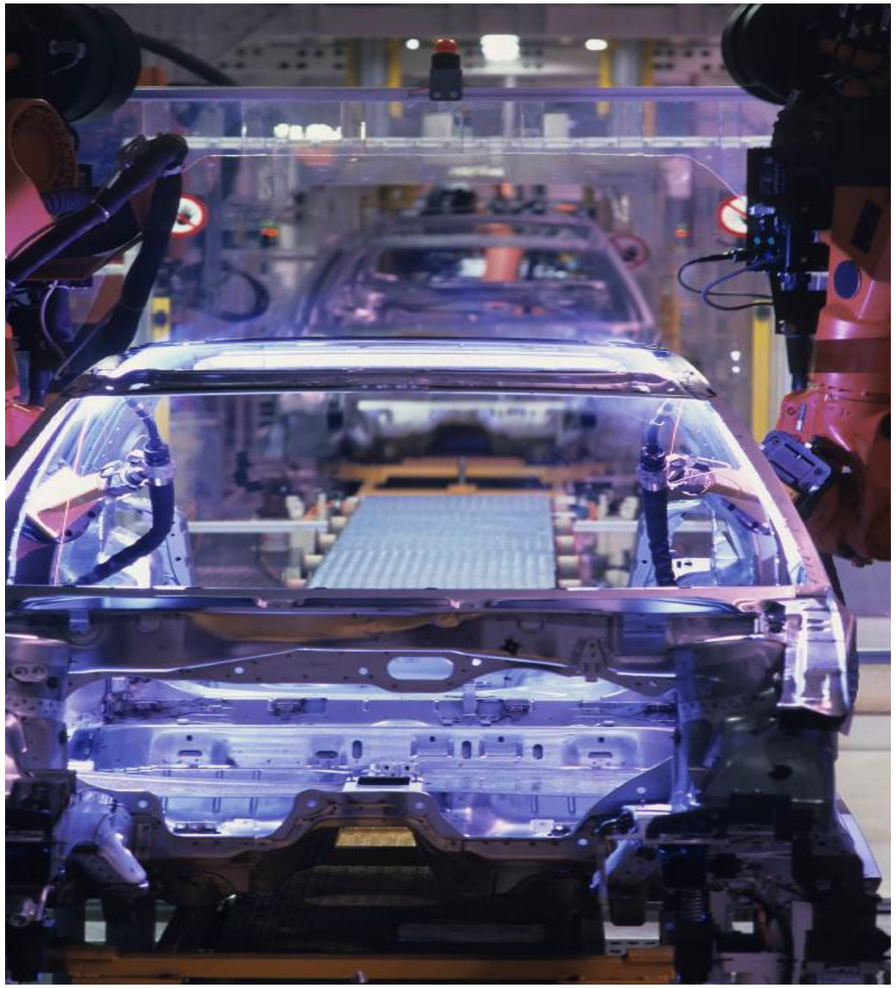




- IEEE 802.1 & 802.3 is undertaking efforts to make Ethernet deterministic including:
  - Guaranteed Delivery over a variety of multi-path topologies
  - Scheduled Delivery; Low-latency (< x µs), low-jitter
  - Time synchronisation across end-devices and the network (<100ns drift)
  - Converge critical application, Audio-Visual and best-effort data traffic
- Deterministic Ethernet proven for highly critical applications (Aviation, SIL, etc.)

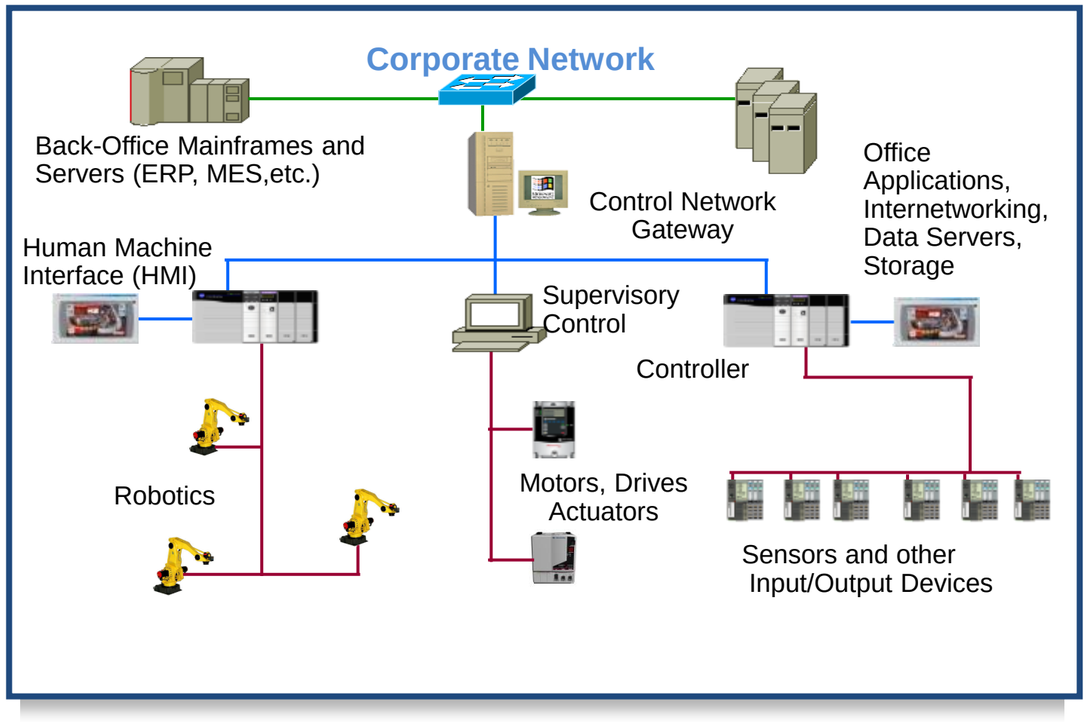
Agenda

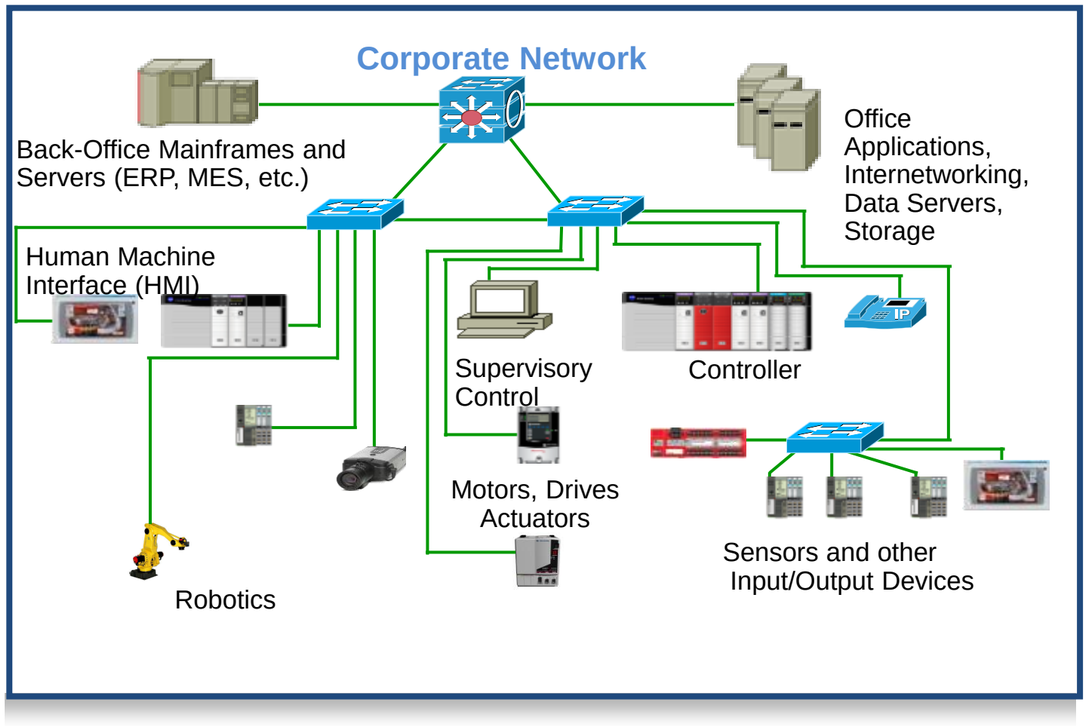
- Industry Trends
- Connected Industry Architectures
  - Applications and Protocols
  - Architectures
  - Solutions and Technologies
- Design Considerations
- Q&A
- Recommended Resources



Industrial Network Convergence

The Journey Towards IP Everywhere

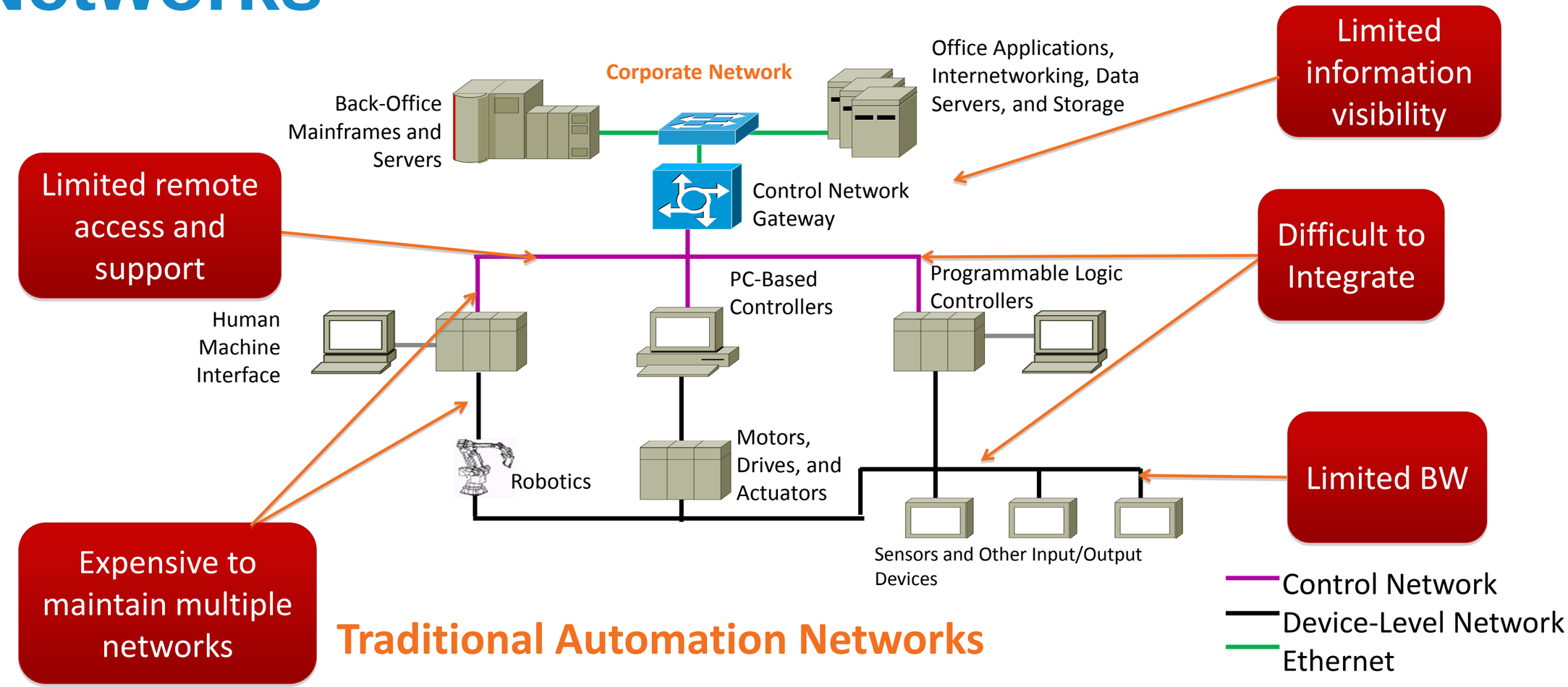




Traditional

Converged Ethernet

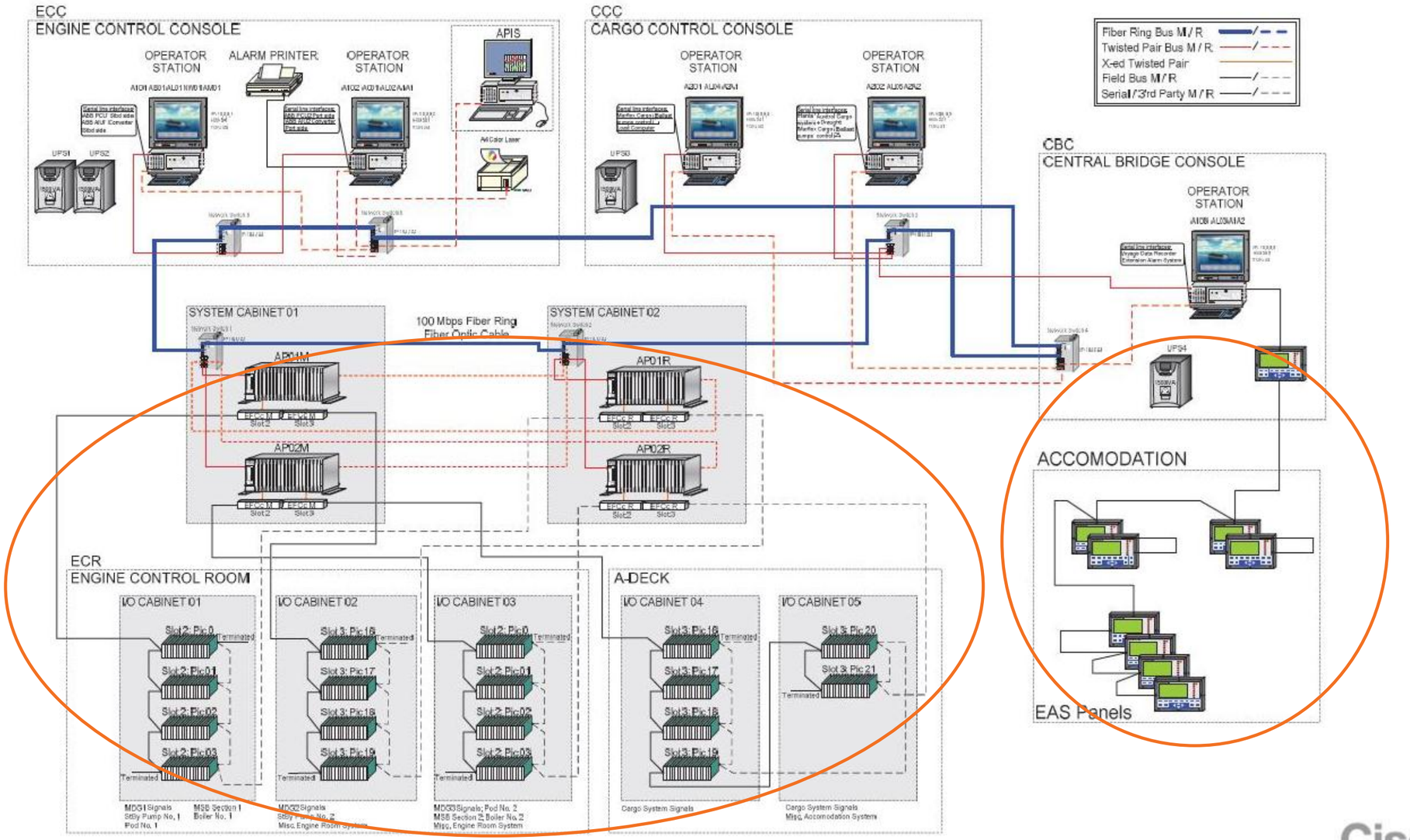
Traditional Industrial Automation Networks



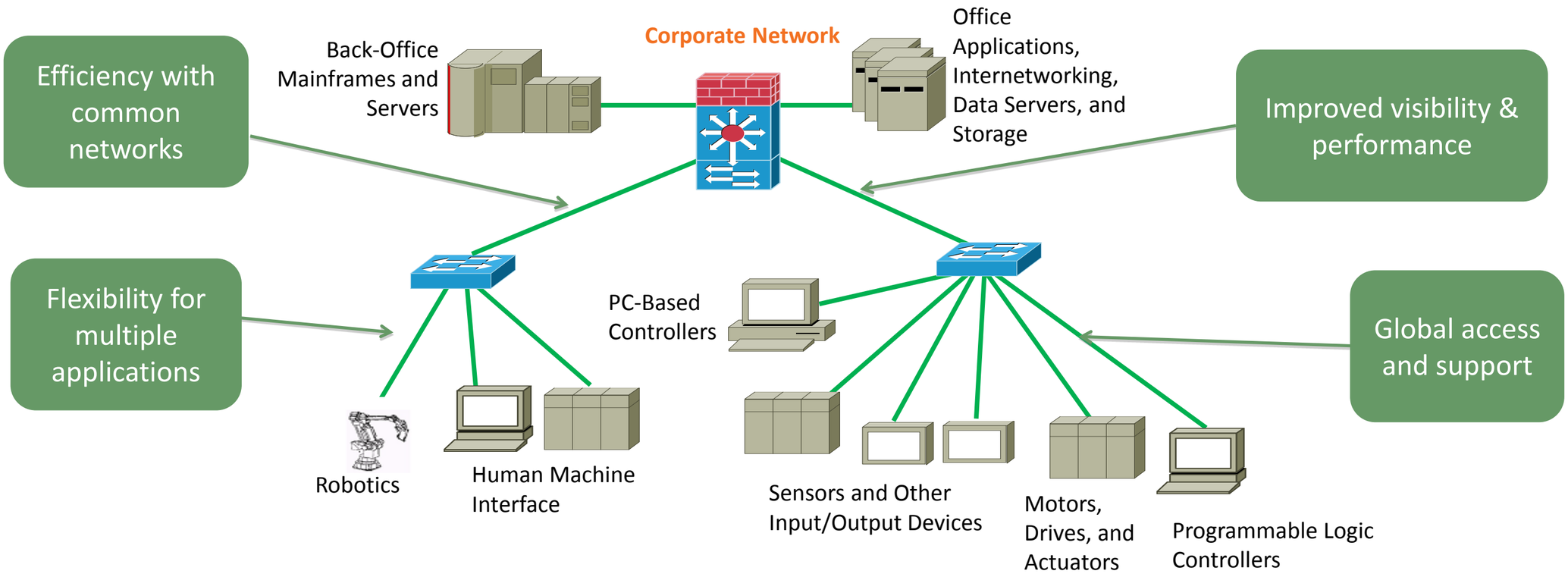
Traditional Automation Networks

Traditional Automation Network Example

Cargo Ship Control System

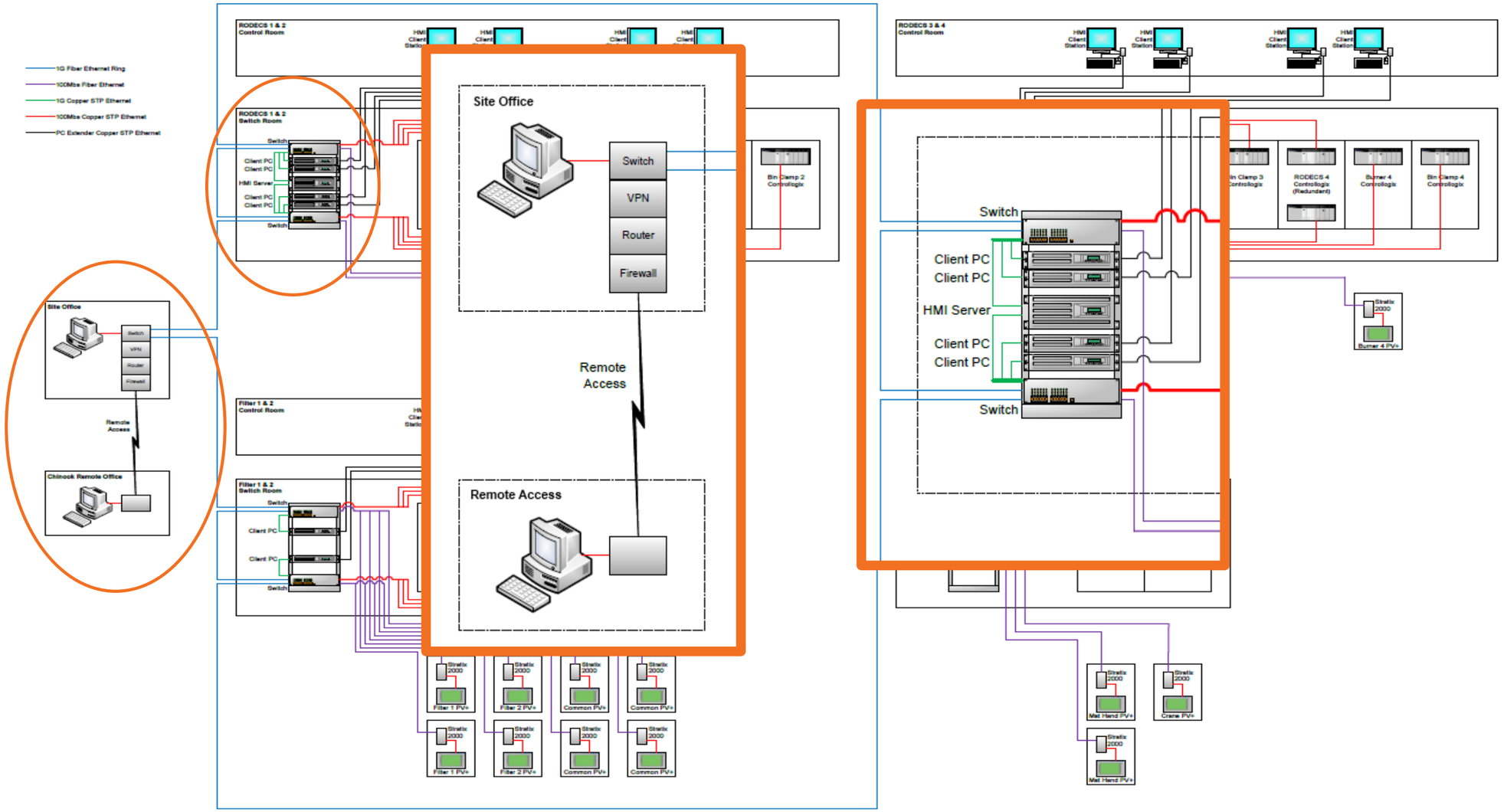


Ethernet & IP Based Industrial Automation Networks

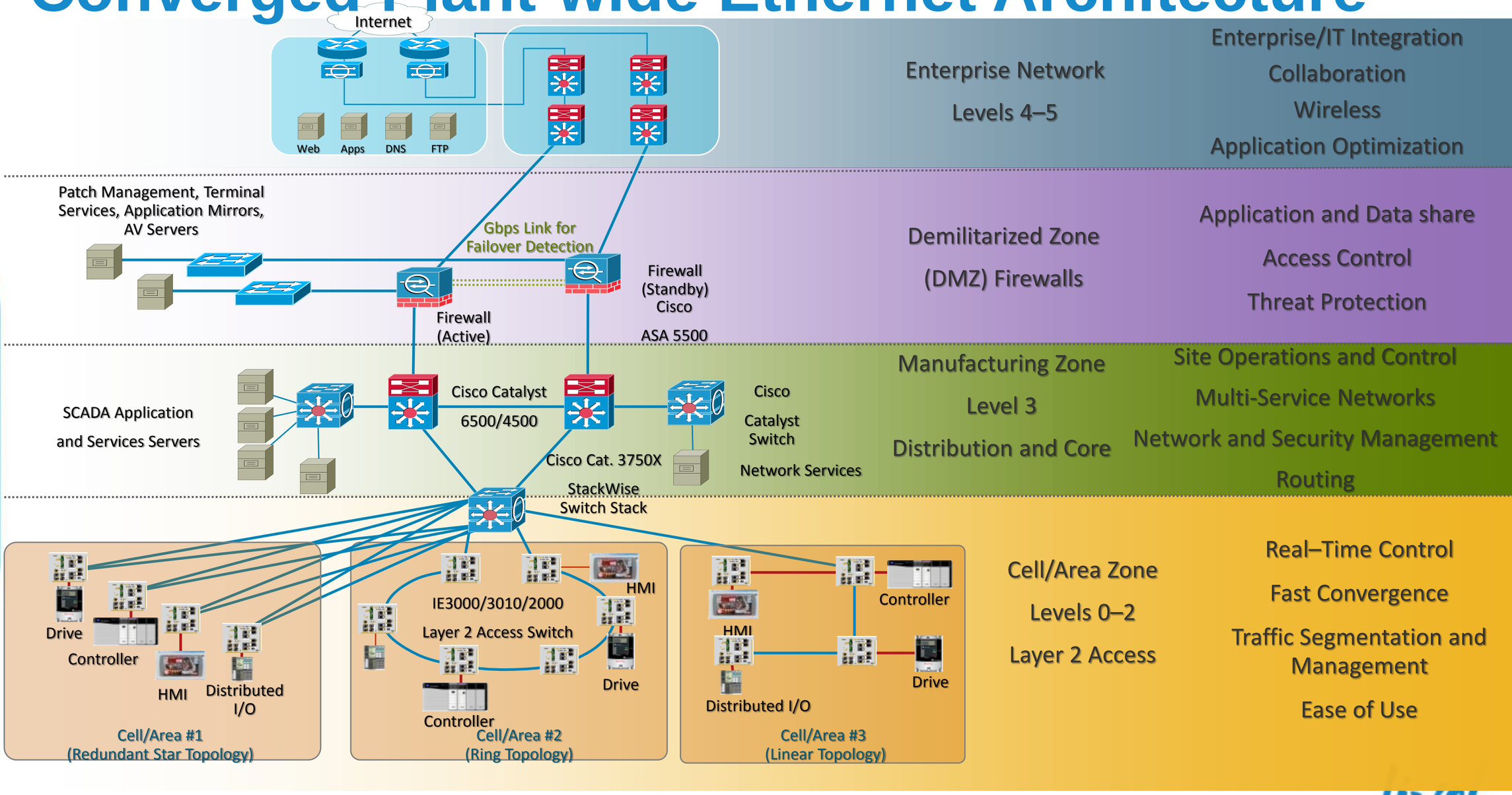


Ethernet and IP Automation Network Example

Material Recycling Plant Control System

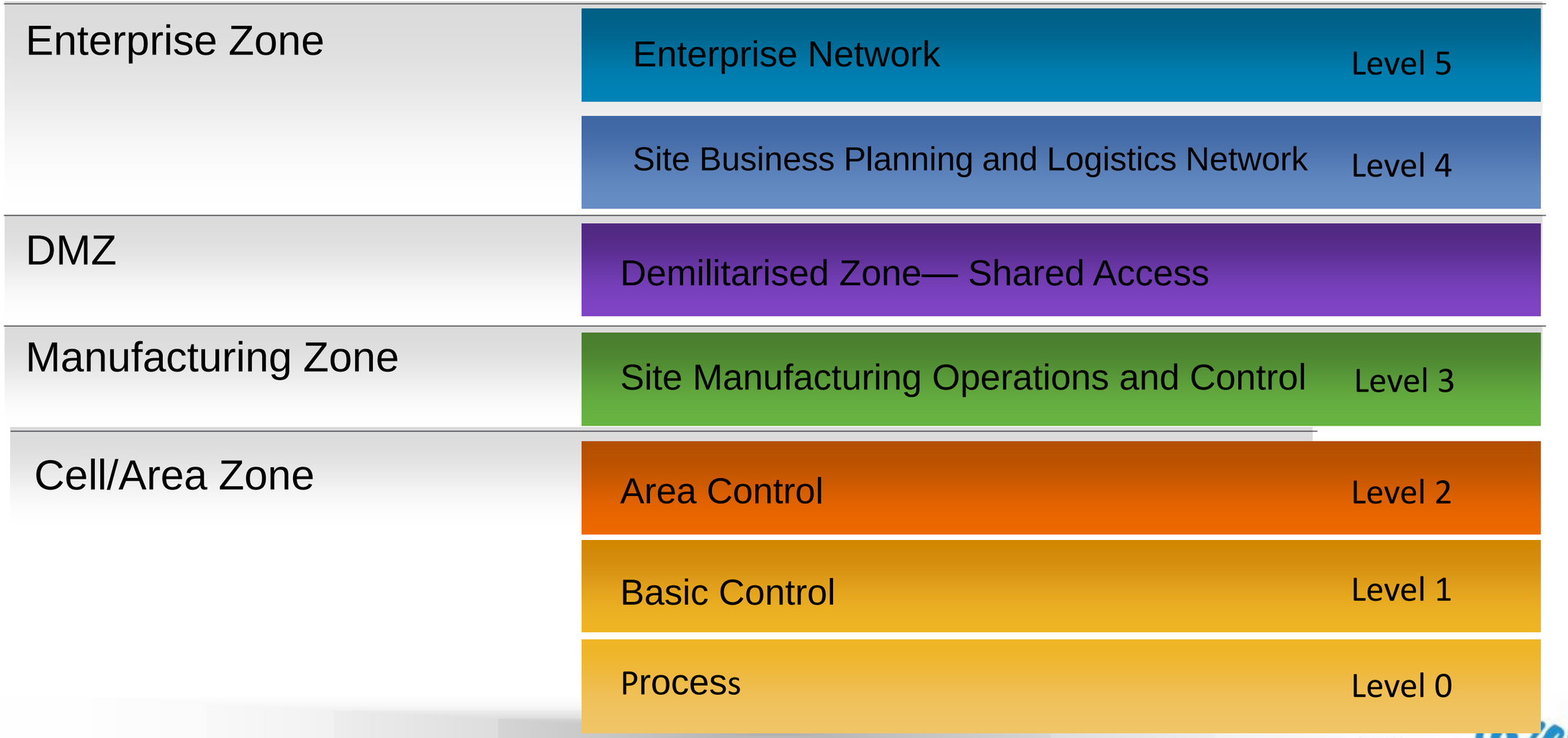


Converged Plant-wide Ethernet Architecture



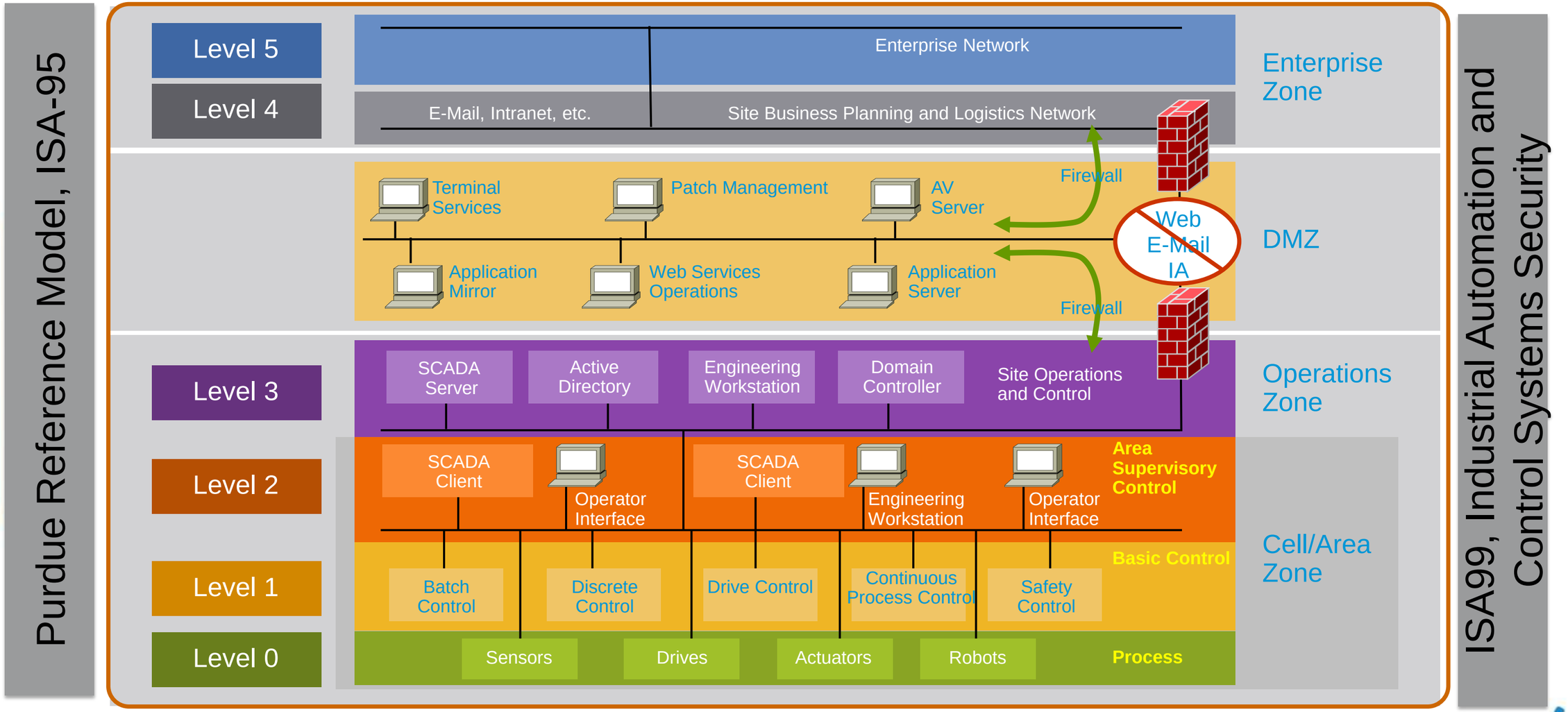
Built on Industry Standards

Purdue Reference Model, ISA95



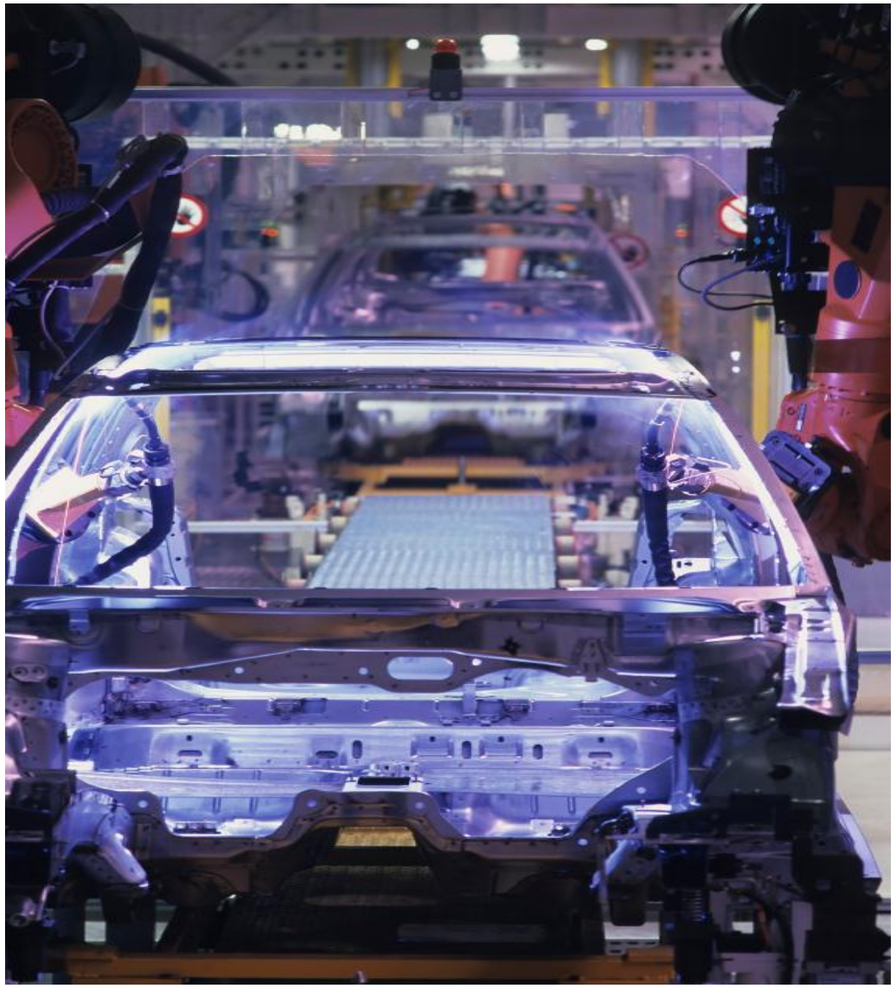
Security Framework

Strong Segmentation



Agenda

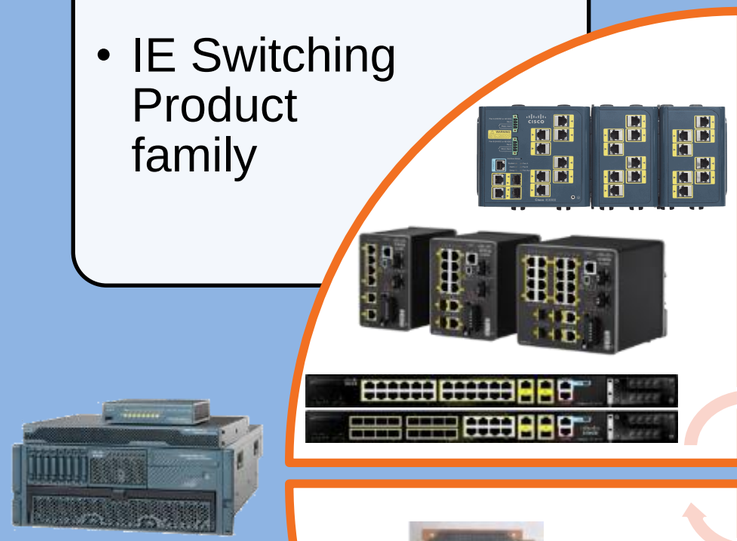
- Industry Trends
- Connected Industry Architectures
  - Applications and Protocols
  - Architectures
  - Solutions and Technologies
- Design Considerations
- Q&A
- Recommended Resources



Cisco Connected Industries Product Portfolio

Security

- IE Switching Product family



- Industrial Wireless Family

- Embedded Routing and Switching

- M2M ISR Gateway Router

Industrial Switching Portfolio

- Industrial-grade, Catalyst-based switches
- IE SwapDrive for “Zero-Config” replacement
- Ideal for manufacturing, mass transit, oil and gas, mining, and more
- IE2000/IE3000 sold by Rockwell as Stratix-branded Allen Bradley switches

IE 3000

Modular/Scalable
L2/L3
Access/Aggregation
DIN Rail

IE 2000

Fixed/Compact
L2
Access
DIN Rail

IE 3010

Fixed
L2/L3
Access
1 RU
PoE and Fibre

Industrial Routing Portfolio

- Mobile routers enabling the Internet of Everything
- Rugged, small form-factor, ISR IOS routers
- Service Provide partnerships
- Typical Applications: fleet management, public safety, mass transit, ATM, vending, kiosk, temporary field office, remote asset monitoring,…

ISR 819H Hardened M2M Gateway

Feature rich
- GPS
- Mobile IP
- IPV6-Ready
- WAAS Express Option
- ScanSafe
- Dual SIM

Connection flexibility
- Serial
- Ethernet
- AP 3500 class, dual radio, mesh AP

Backhaul flexibility
- 4G
- 3G+Wi-Fi
- HSPA+
- EV-DO
- Wi-Fi
- Ethernet

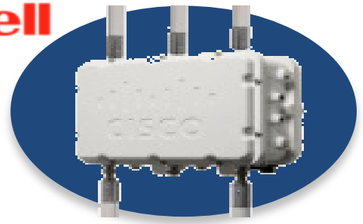
Industrial Wireless Portfolio

- Extension of 1550 Outdoor AP product line
- Converges industrial wireless access and sensor networks
- 802.11 a/b/g/n Mesh AP's
- Hazardous location qualified (Class 1, Div/Zone 2
- Ideal for mining, oil and gas, manufacturing, and process control applications

1552H

3 Antennae (2.4/5 GHz)
AC Power

Honeywell



1552S

3 Antennae (2.4/5 GHz)
AC and DC Power
ISA100 Sensor Gateway

EMERSON

New
2HCY13

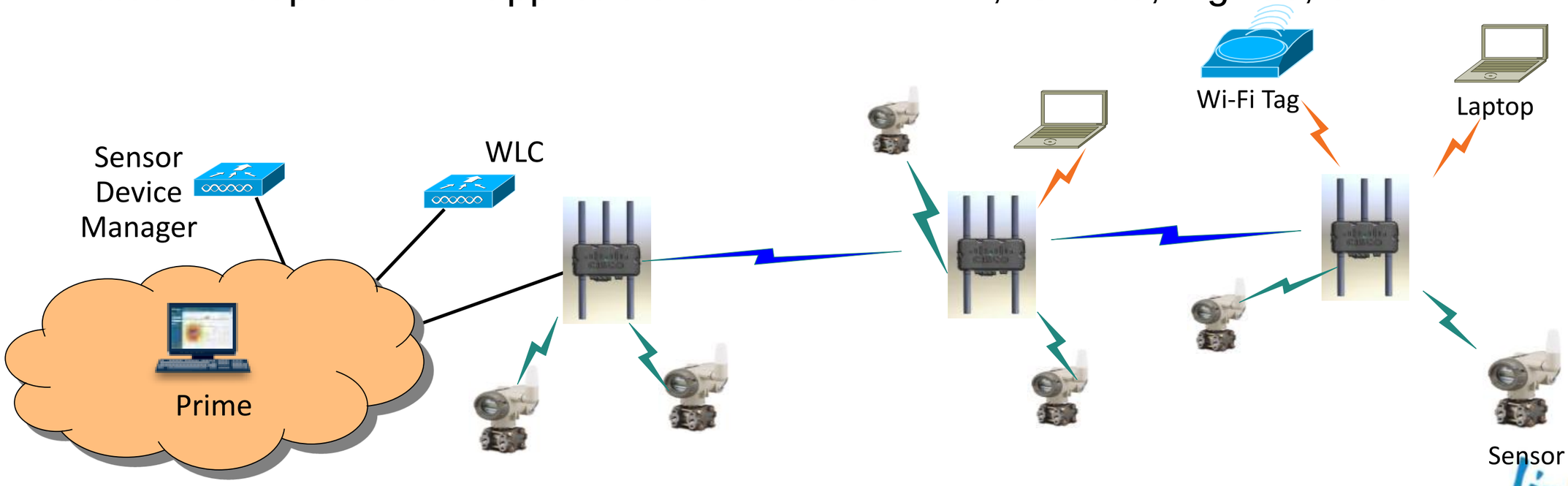
1552WU

6 Antennae (3x2.4, 3x2.5)
DC Power
WiHART Sensor Gateway

Wireless Sensor Networks

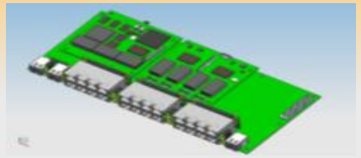
None-WIFI integration into Wireless

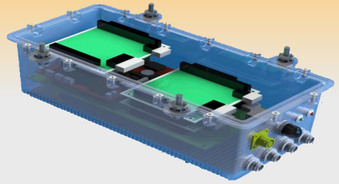
- WSN may share same spectrum as Wi-Fi
- Integrate sensor gateway into AP
- Field sensors communicate (IEEE 802.15.4 radio) to gateway & AP provides Wi-Fi access and backhaul connectivity
- Protocol independent – applicable to WirelessHART, ISA100, ZigBee, 6LoWPAN

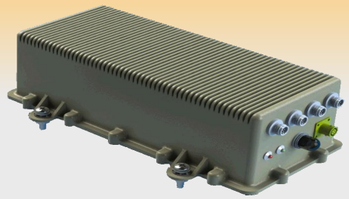


Embedded Industrial Networking Portfolio

- Cisco boards for integrating into custom enclosures
- For ruggedised custom networking products





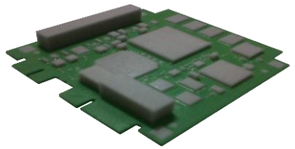


Military

Government Services

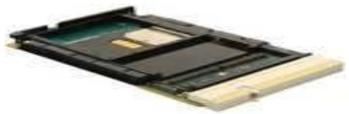
Transportation

Oil and Gas



C5915 ESR

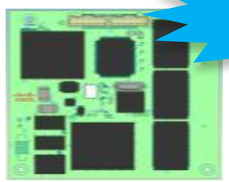
Mid Range Router
PC104 Form Factor



C5940 ESR

High End Router
cPCI Form Factor

New
2HCY13



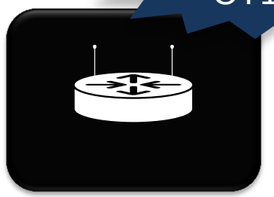
ESS 2020

IE2K-Based Switch
PC104 Form Factor
2GE + 8 FE ports
16FE Expansion Board

Industrial Security

- Security features are incorporated into industrial product lines
- Targeted industrial security products are on the roadmap

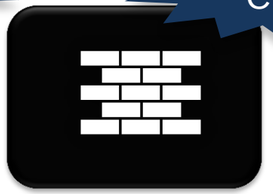
1H CY13



Secure Router

Provides secure remote access and zone segmentation for most industrial use cases

2H CY13



Industrial Firewall

Industry leading firewall, intrusion prevention, VPN, remote access, and other services. features

Industrial IPS

Defence against complex industrial network attacks

Wireless IPS

Increase mobility without compromising security with threat-protected WLAN services

Cisco TrustSec

Policy-based access control, identity-aware networking, and data integrity

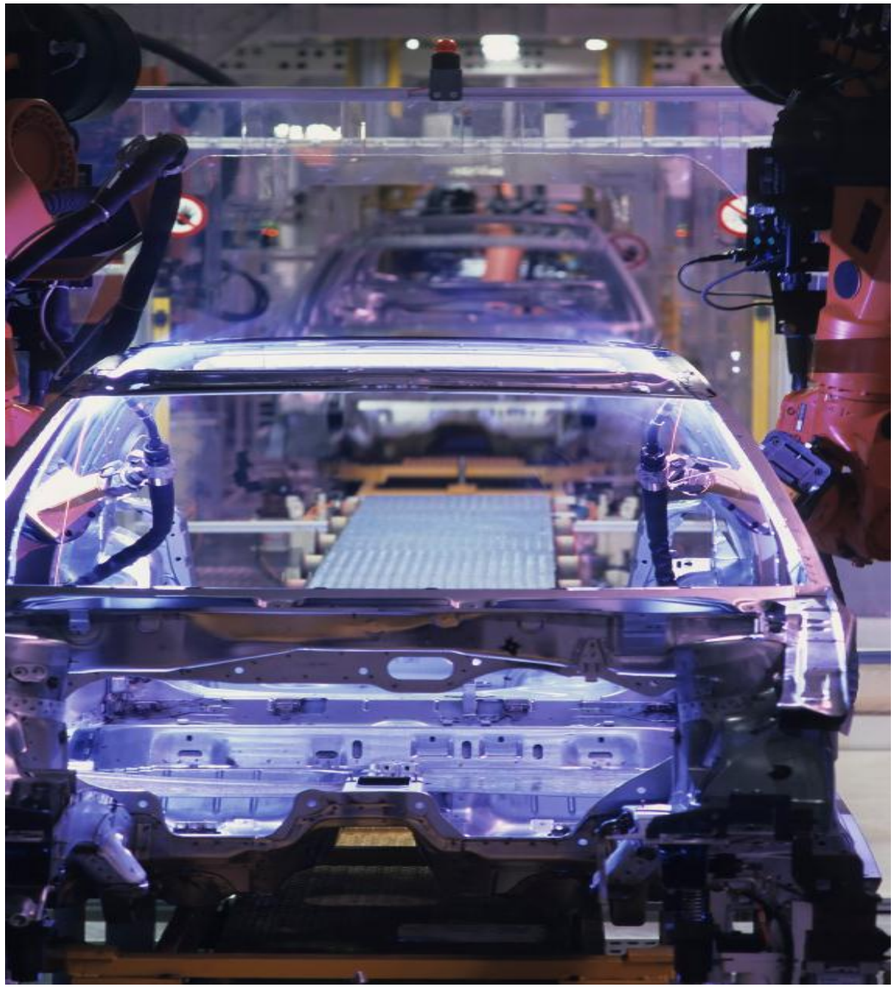
Network Portfolio for End-to-End Manufacturing Architecture

Cisco Differentiation

- Built on tried-and-tested Cisco Campus network
- Cisco IOS based
- Consistent Security including Identity Services (ISE)
- Cisco network management applications
- Resiliency and availability features
- Optimised delivery of critical traffic
- Scalable, converged network framework

Agenda

- Industry Trends
- Connected Industry Architectures
- Design Considerations
  - Traffic Flows and Topologies
  - Availability and Resilience
  - Segregation and VLANs
  - QoS
  - Security
- Q&A
- Recommended Resources

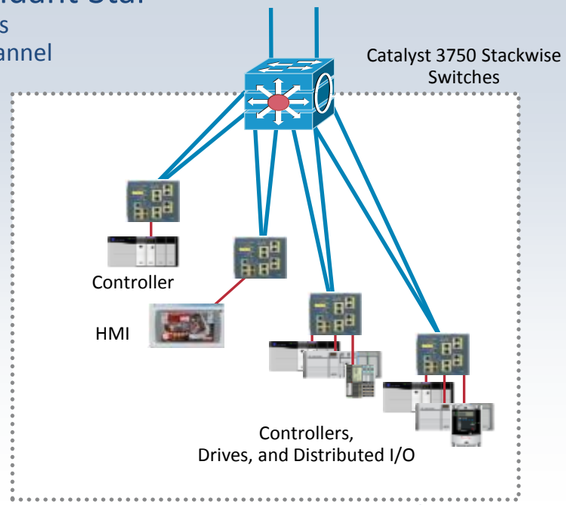


Industrial Network Topologies

Cell/Area Zone Topology Options

Redundant Star

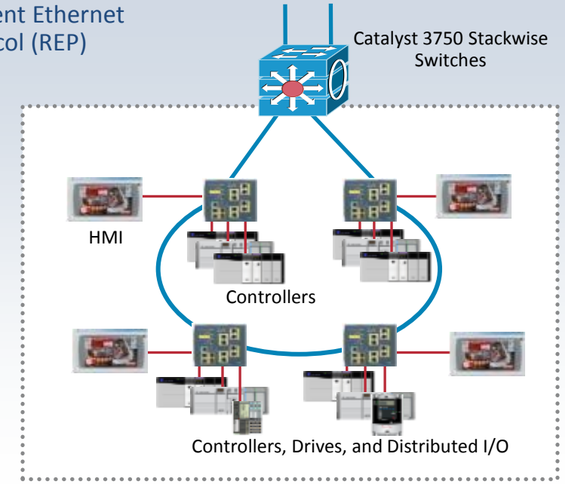
Flex Links
EtherChannel



Cell/Area Zone

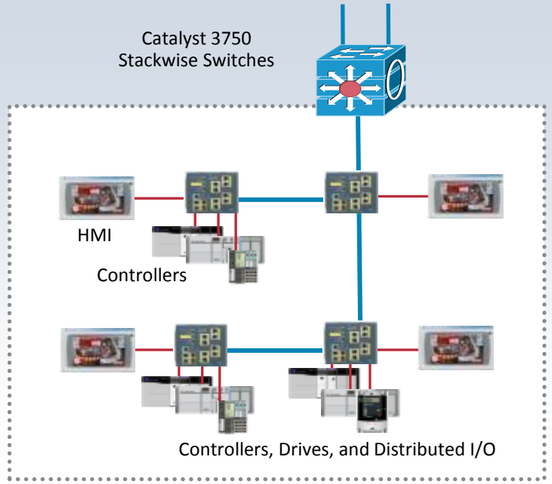
Ring

Resilient Ethernet Protocol (REP)



Cell/Area Zone

Star/Bus Linear

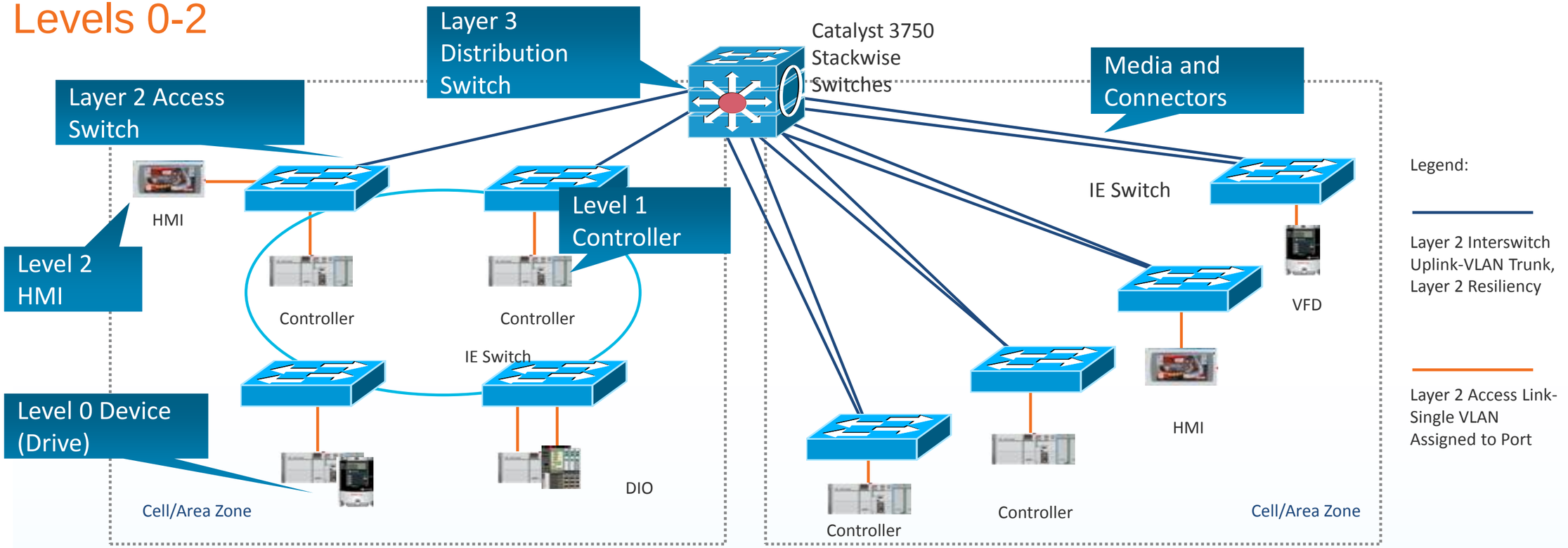


Cell/Area Zone

	Redundant Star	Ring	Linear
Cabling Requirements			
East 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

Cell/Area Zone Overview

Levels 0-2



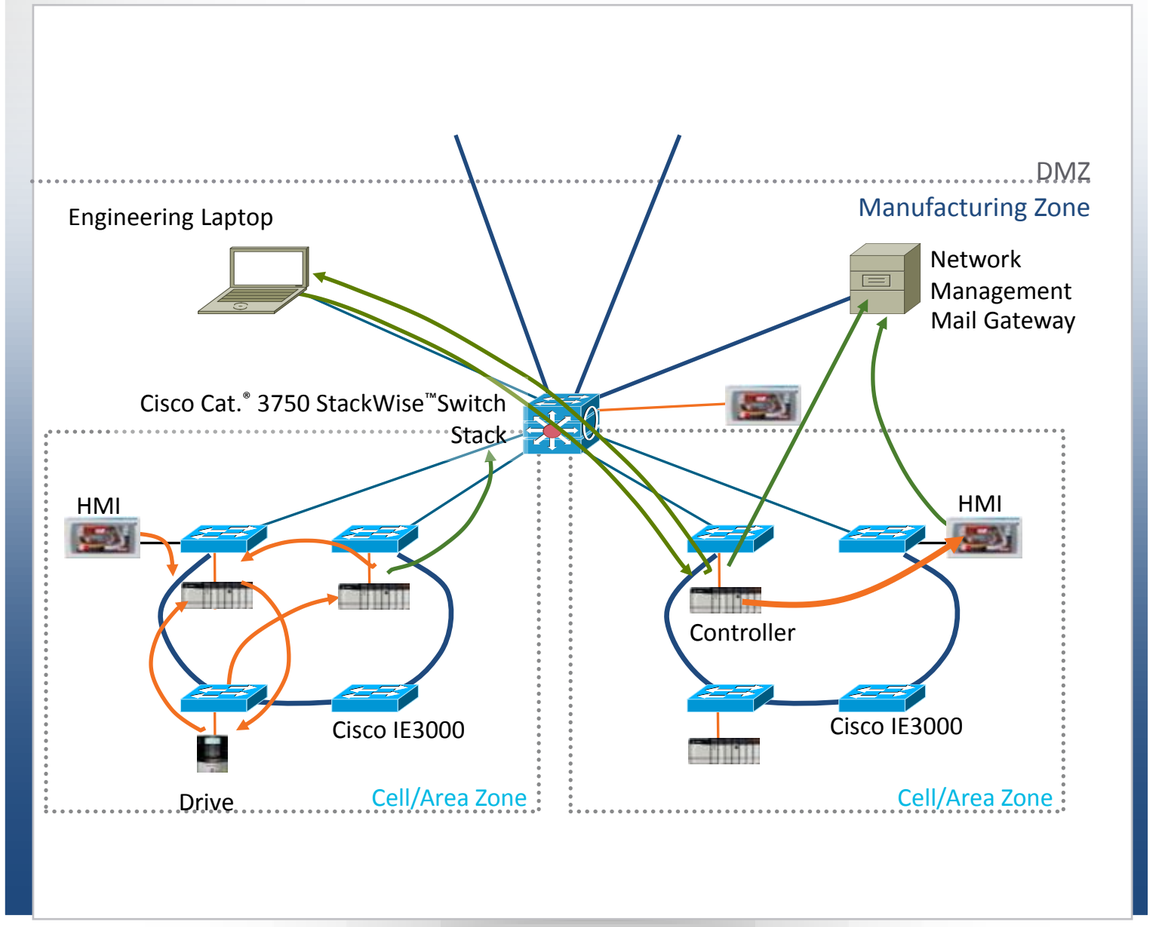
The Cell/Area Zone Is a Layer 2 Network for a Functional Area of a Production Facility.
Key Network Considerations Include:

- Environmental constraints
- Range of device intelligence
- Time-sensitive applications

Cell/Area Traffic Flows

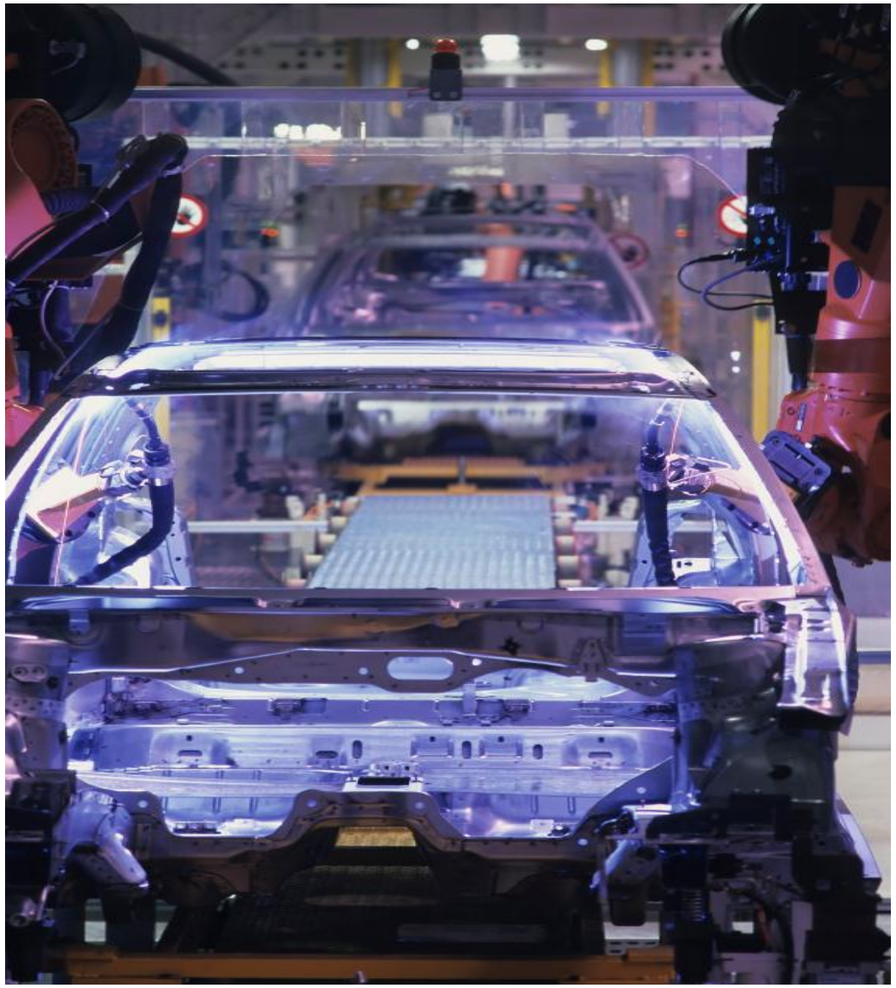
- Cell/area traffic is predominately (>80%) local, cyclical I/O (a.k.a. Implicit) traffic
  - Producers generate UDP multi-cast messages
  - Consumer generate UDP/TCP uni-cast messages
  - Packets are small: 100-200 Bytes, but communicated very frequently (every 0.5 to 10's of ms).
  - Typically un-routable (TTL=1 by application)

- The rest is informational control and administration (or Explicit) traffic flows intra- and inter-cell/area
  - Non-critical administrative or data traffic
  - Diagnostic information via HTTP/S
  - Status and fault warnings via SNMP or SMTP
  - Packets are larger, ~500 bytes but infrequent (100s of ms)



Agenda

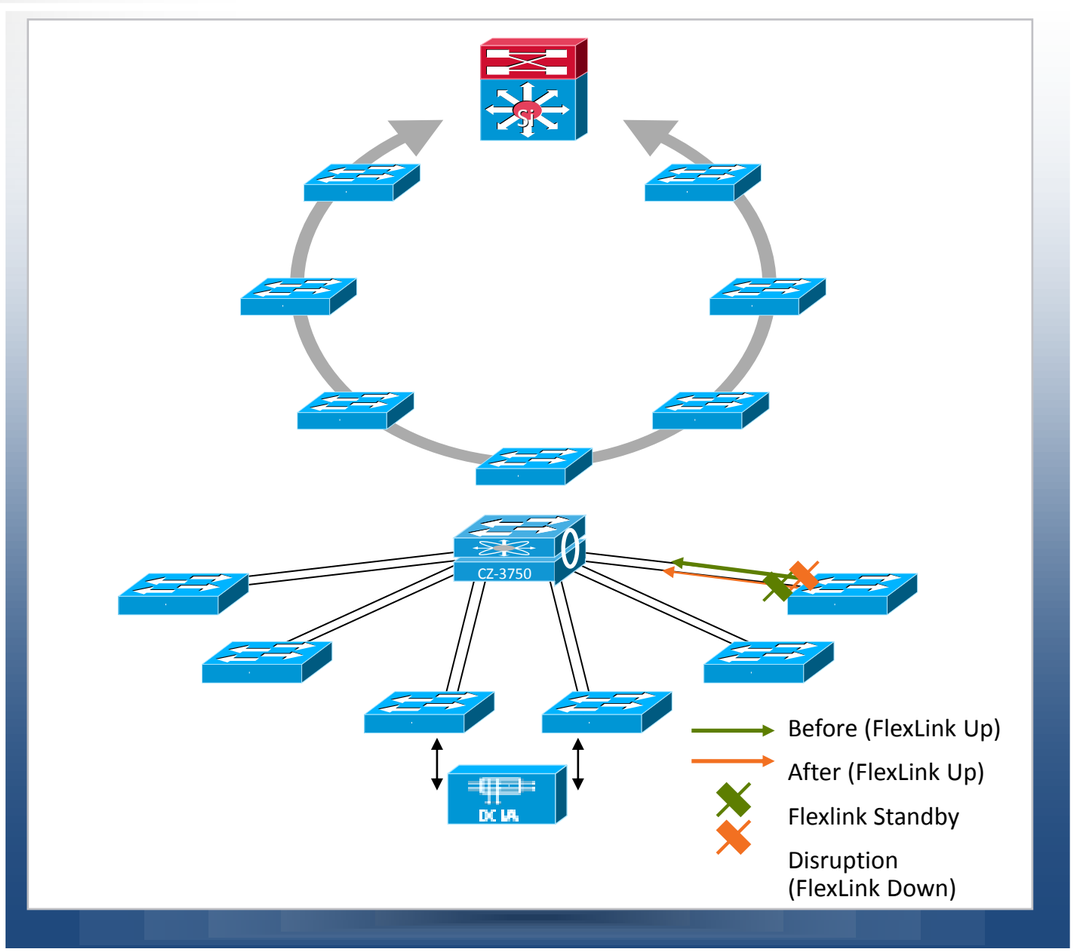
- Industry Trends
- Connected Industry Architectures
- Design Considerations
  - Traffic Flows and Topologies
  - Availability and Resilience
  - Segregation and VLANs
  - QoS
  - Security
- Q&A
- Recommended Resources



Resiliency for Industrial Applications

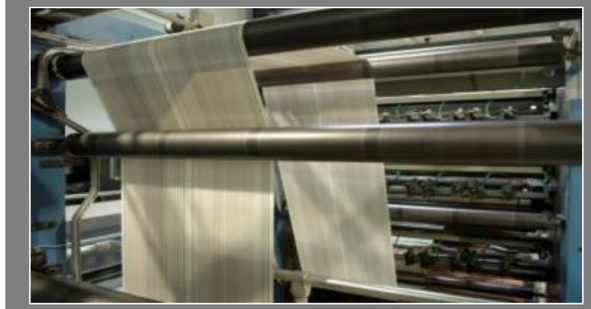
Supporting Multiple Topologies

- Ring Convergence
  - –Resilient Ethernet Protocol (REP)
  - –Achieves ~50 ms convergence in large, complex networks
- Redundant Star Convergence
  - –Multiple protocol options
  - –Convergence times of <100ms for Flexlinks and Etherchannel
- Tested with SCADA applications and multicast traffic
- Fast convergence avoids application reset and improves uptime
- Critical for industrial applications



Performance Requirements

Industrial Automation & Control Applications

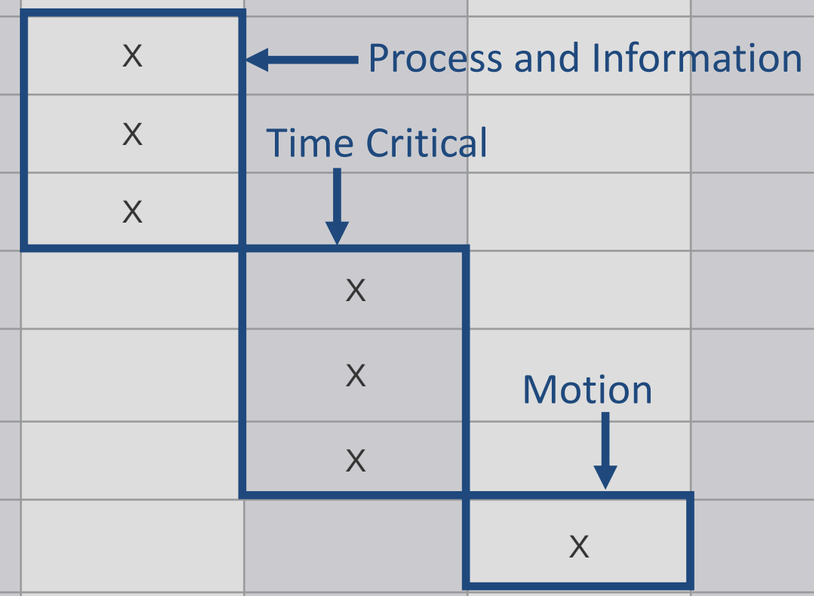
	Process Automation	Factory Automation	Motion Control
			
Function	Information Integration, Slower Process Automation	Time-critical Factory Automation	Motion Control
Comm. Technology	.Net, DCOM, TCP/IP	Industrial Protocols, CIP, Profinet etc.	Hardware and Software solutions, e.g. CIP Motion, PTP
Period	1 second or longer	10 ms to 100 ms	<1 ms
Industries	Oil & gas, chemicals, energy, water	Auto, food and bev, electrical assembly, semiconductor, metals, pharmaceutical	Subset of factory 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

Source: ARC Advisory Group

Network Resiliency Protocols

Selection Is Application Driven

Resiliency Protocol	Mixed Vendor	Ring	Redundant Star	Net Conv >250 ms	Net Conv 50-100 ms	Net Conv > 1 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
PVST+		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	

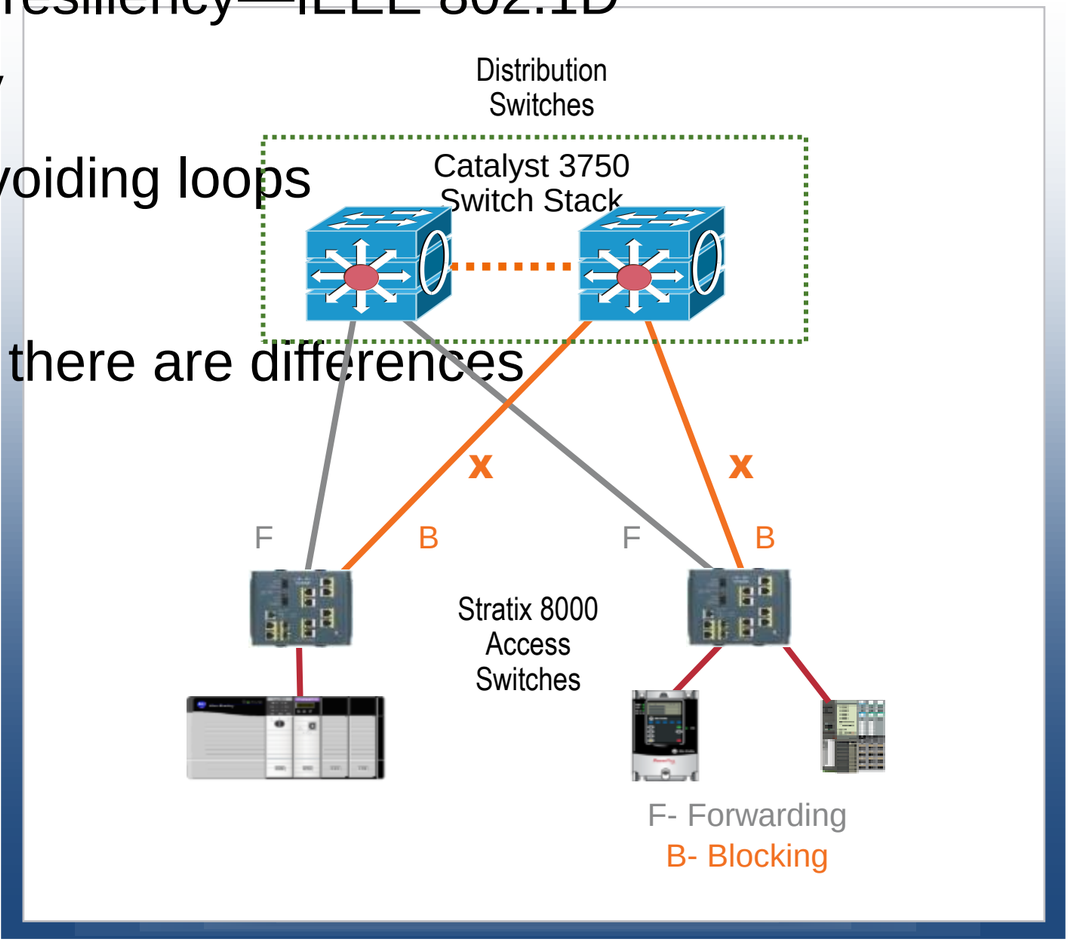


Net Conv: Network Convergence

Spanning Tree Protocol (STP)

Often required for interoperability

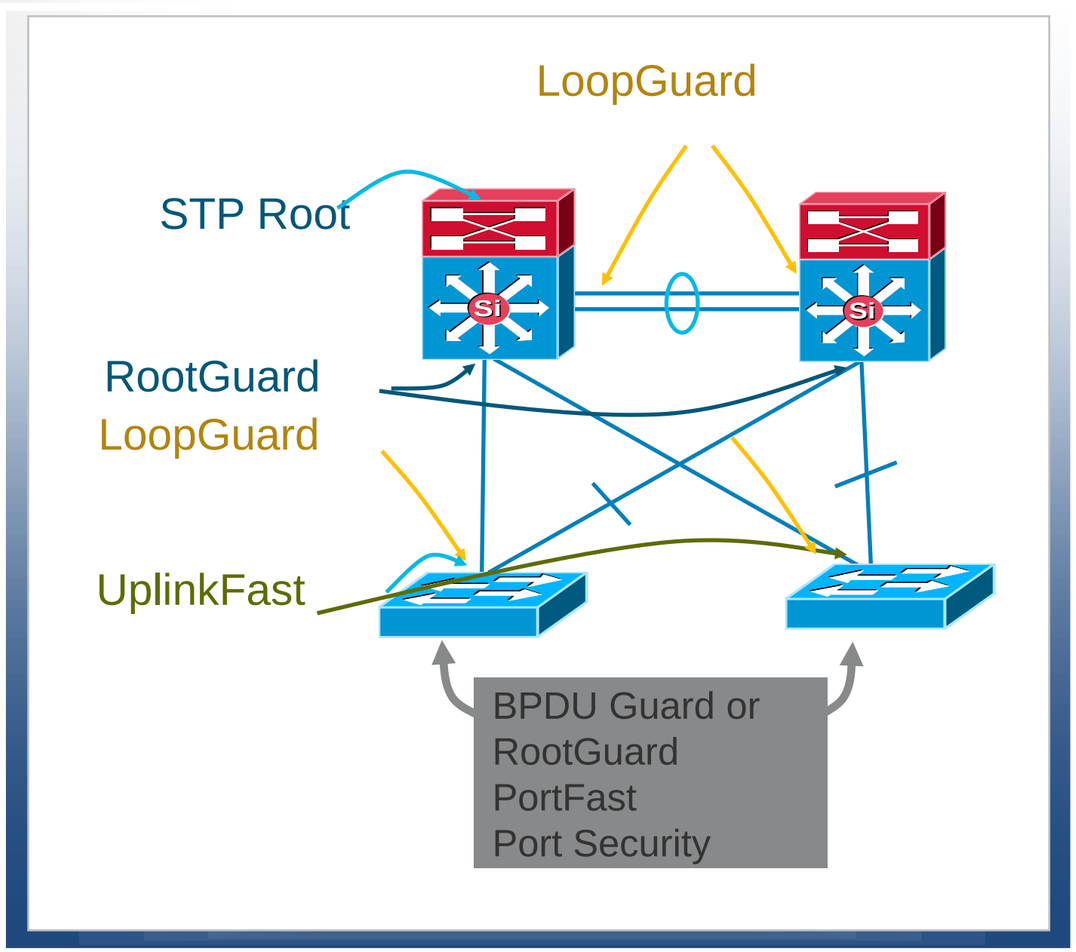
- Most common standard protocol for network resiliency—IEEE 802.1D
- Supports Redundant Star and Ring Topology
- Provides alternate path in case of failures, avoiding loops
- Unmanaged switches don’t support STP
- Versions: STP, RSTP, MSTP and RPVST+ - there are differences
- Coordinate with IT before implementing



Layer 2 Hardening

Spanning Tree Should Behave the Way You Expect

- Place the root where you want it
  - Distribution Switch
- The root bridge should stay where you put it
  - RootGuard
  - LoopGuard
  - UplinkFast
  - UDLD
- Only end-station traffic should be seen on an edge port
  - BPDU Guard
  - RootGuard
  - PortFast
  - Port-security



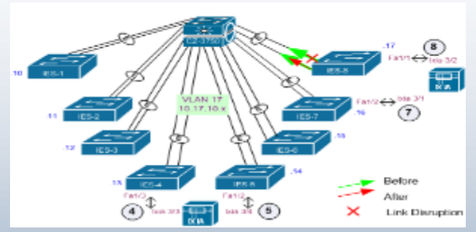
Testing Results:

FlexLinks and Etherchannel

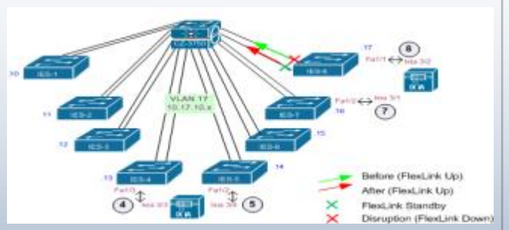
Redundant Star, Fibre Uplink Topologies With Etherchannel and Flexlinks support "Time-critical" Plant Applications

- Measured convergence consistently under 100 ms target
  - Multicast and unicast test streams measured
- Application timeouts occurred rarely
  - 1.5% of physical disconnects

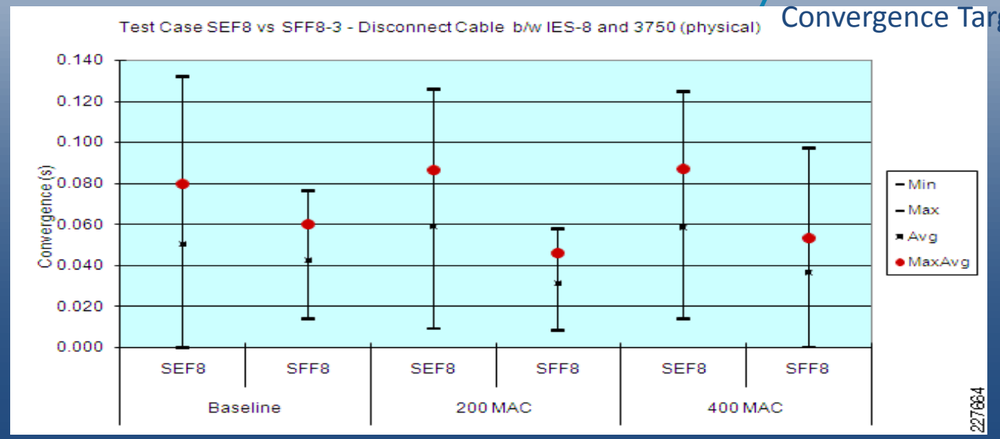
Etherchannel Topology



Flexlinks Topology



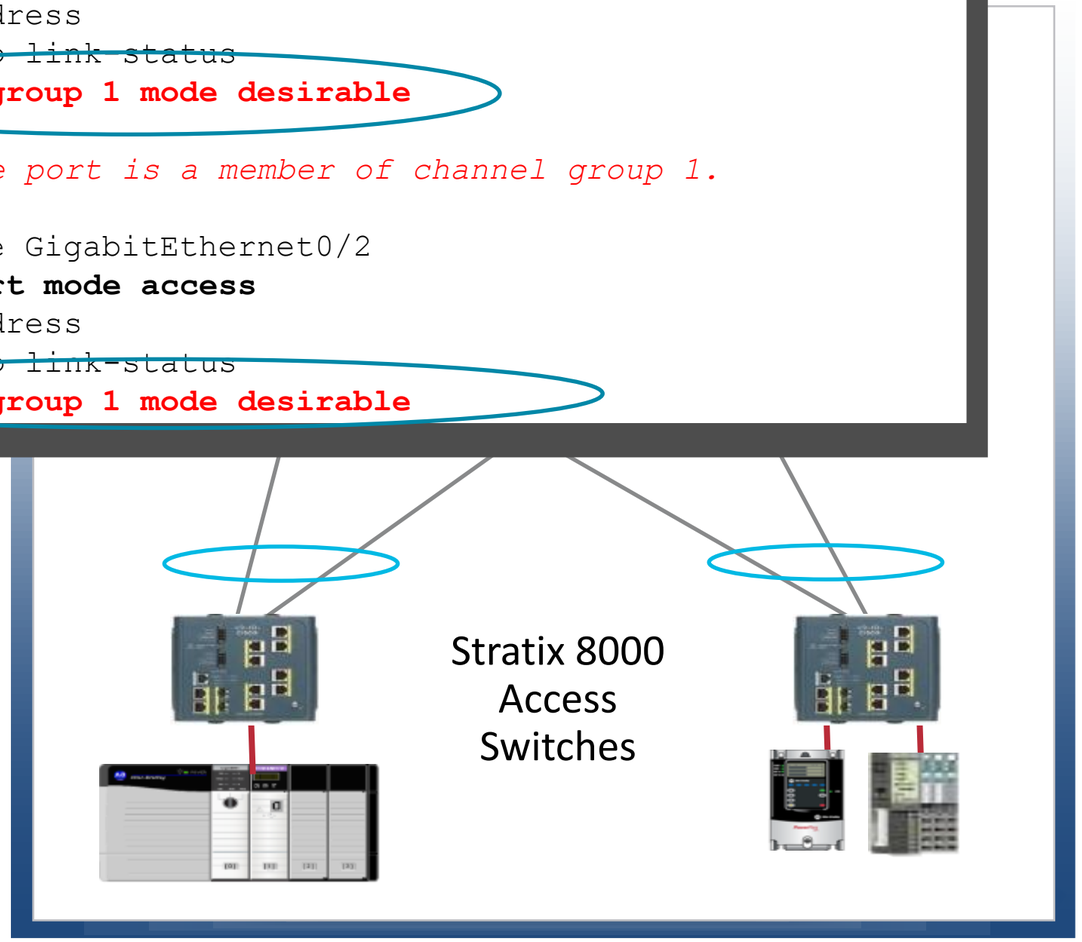
Time Critical Convergence Target



Configuring EtherChannels

- Link Aggregation Control Protocol (LACP) port aggregation—IEEE 802.3ad
- Redundant Star Topology
- A way of combining several physical links between switches into one logical connection to aggregate bandwidth (2 to 8 ports)
- Provides resiliency between connected switches if a connection is broken

```
!--- The port is a member of channel group 1.

interface GigabitEthernet0/1
switchport mode access
no ip address
snmp trap link-status
channel-group 1 mode desirable

 !--- The port is a member of channel group 1.

interface GigabitEthernet0/2
switchport mode access
no ip address
snmp trap link-status
channel-group 1 mode desirable
```



Configuring Flex Links

- Cisco te
- Redund
- Active/S
- Provide failures
- Unmana concept

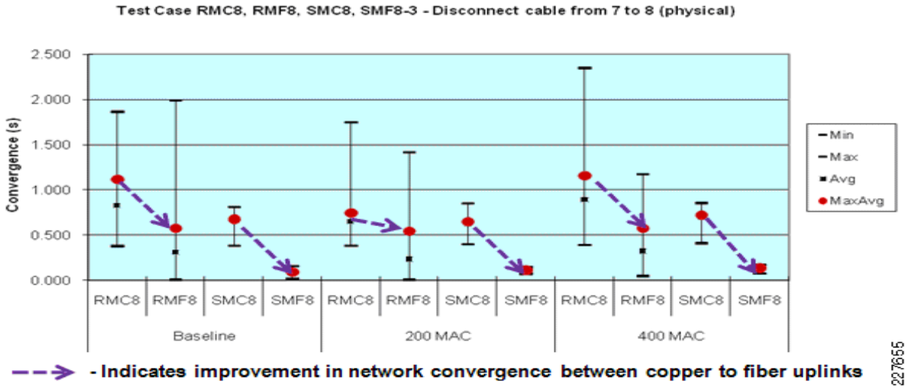
```
Switch# configure terminal
Switch(conf)# interface fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2
Switch(conf-if)# end
Switch# show interface switchport backup

Switch Backup Interface Pairs:


Active Interface Backup Interface State
------------------------------------------------------------------------------------------
FastEthernet1/0/1       FastEthernet1/0/2       Active Up/Backup Standby
FastEthernet1/0/3       FastEthernet2/0/4       Active Up/Backup Standby
Port-channel1 GigabitEthernet7/0/1    Active Up/Backup Standby
```

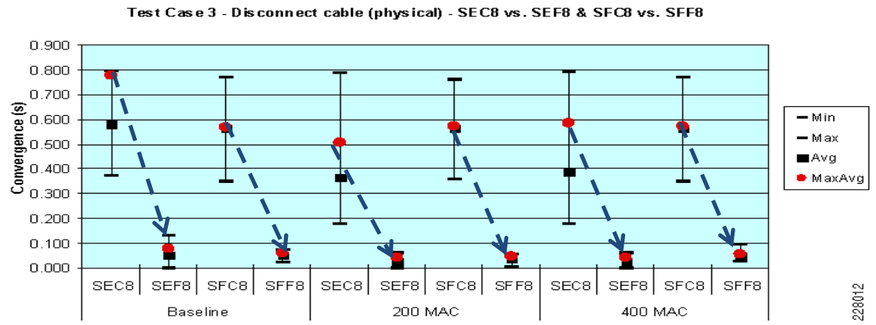
Testing Results:

Copper vs Fibre

Fibre Media for Uplinks Significantly Improves Network Convergence

- Compare test with same topologies with fibre vs. copper uplinks
  - Multimode LC fibre cables
  - Cat 5e and Cat 6 copper cables
- All fibre topologies converged faster than copper topologies, approx. 500ms faster
- Ethernet standards allow for higher range of link-down notification for copper-based links

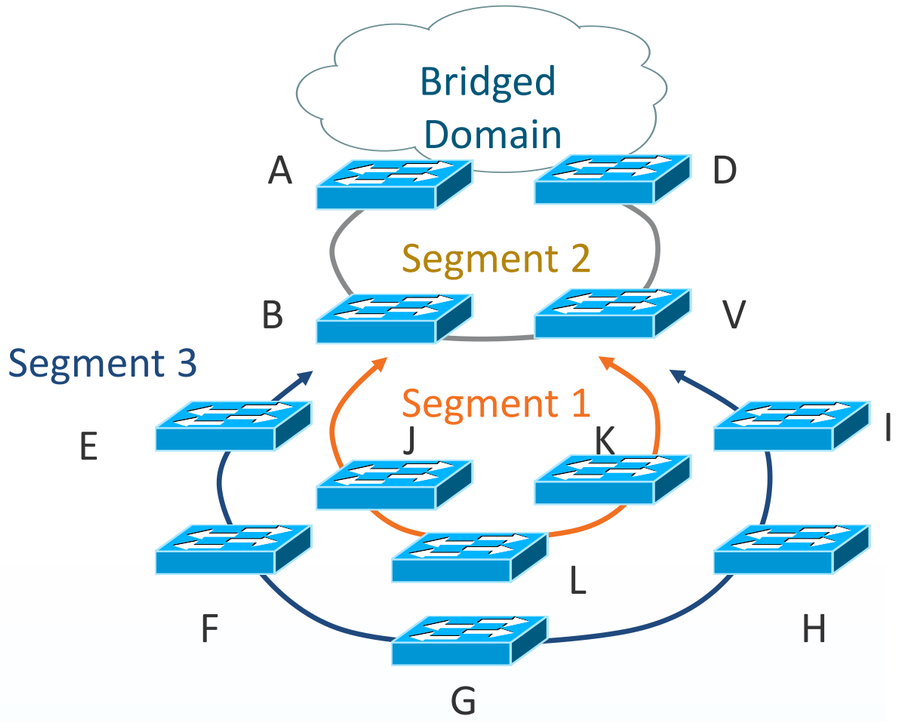


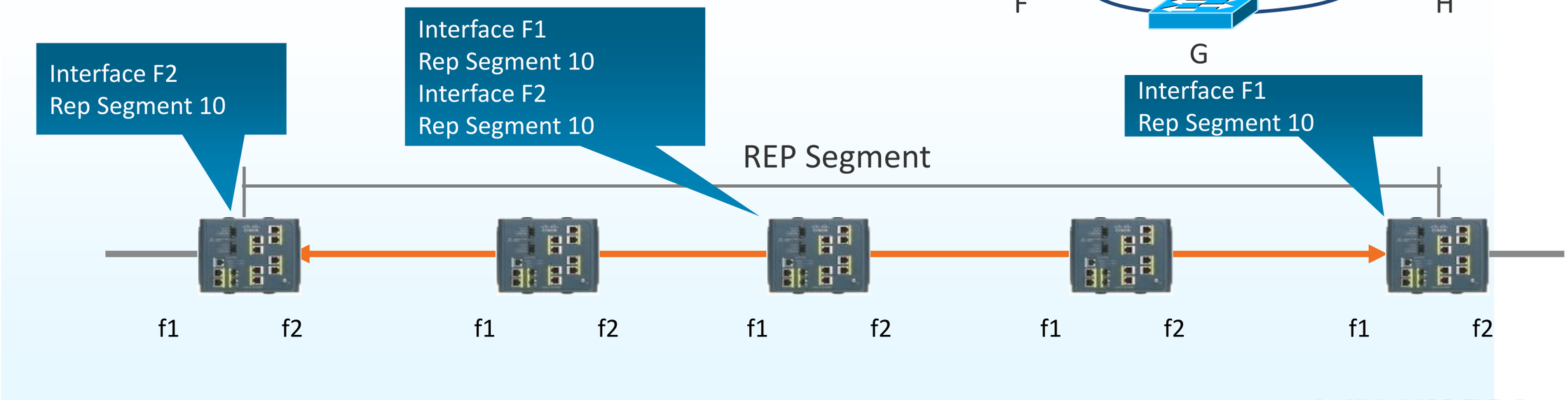


Resilient Ethernet Protocol

Segment Protocol

- REP operates on chain of bridges called segments
- A port is assigned to a unique segment
- A segment can have up to two ports on a given bridge

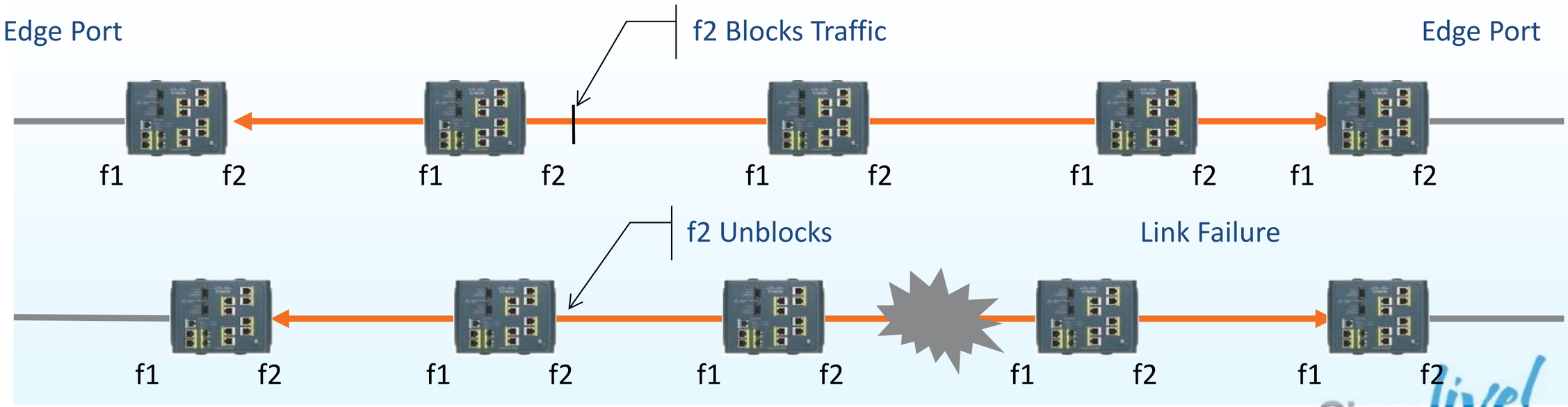




Resilient Ethernet Protocol

Blocked Port

- When all links are operational, a unique port blocks the traffic on the segment. Called the Alternate Port
- If any failure occurs within the segment, the blocked port goes forwarding

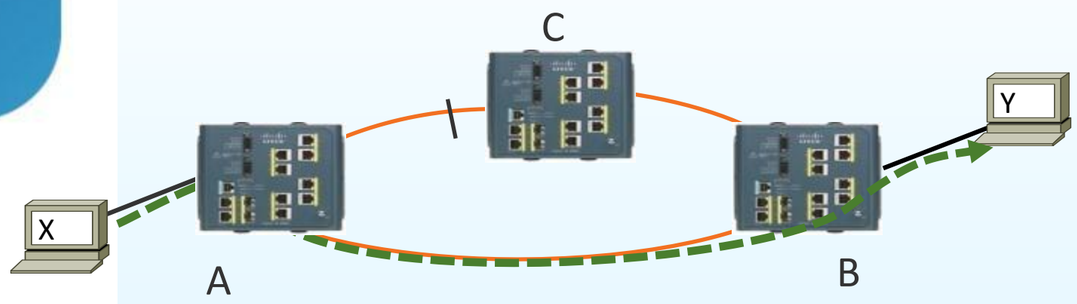


Configuring Resilient Ethernet Protocol

- Se… …nte…
- C… …t li…

```
!
rep admin vlan 4
!
vlan 101
 name wtg001
!
vlan 102
 name wtg002
```

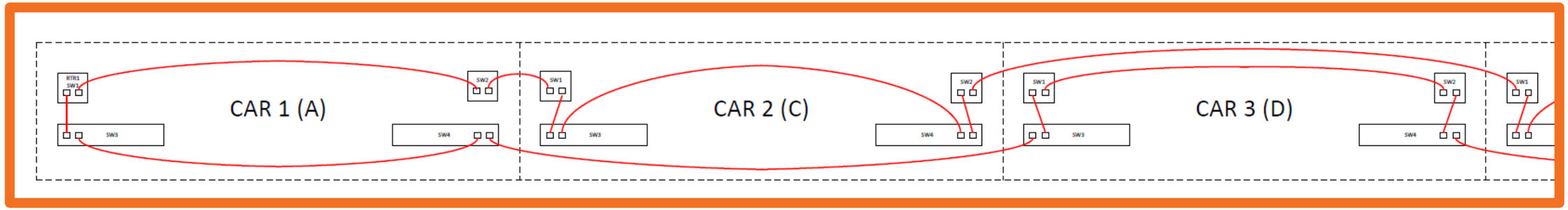
```
interface FastEthernet0/1
 description REP fiberloop1
 switchport trunk allowed vlan 4,101-120
 switchport mode trunk
 switchport nonegotiate
 duplex full
 priority-queue out
 rep segment 10 edge primary
 rep preempt delay 15
 rep block port 22 vlan 1-4094
 mls qos trust dscp
!
interface GigabitEthernet0/1
 description REP substation
 switchport mode trunk
 switchport nonegotiate
 priority-queue out
 rep segment 1 edge primary
 rep preempt delay 15
 rep block port 3 vlan 1-4094
 mls qos trust dscp
```



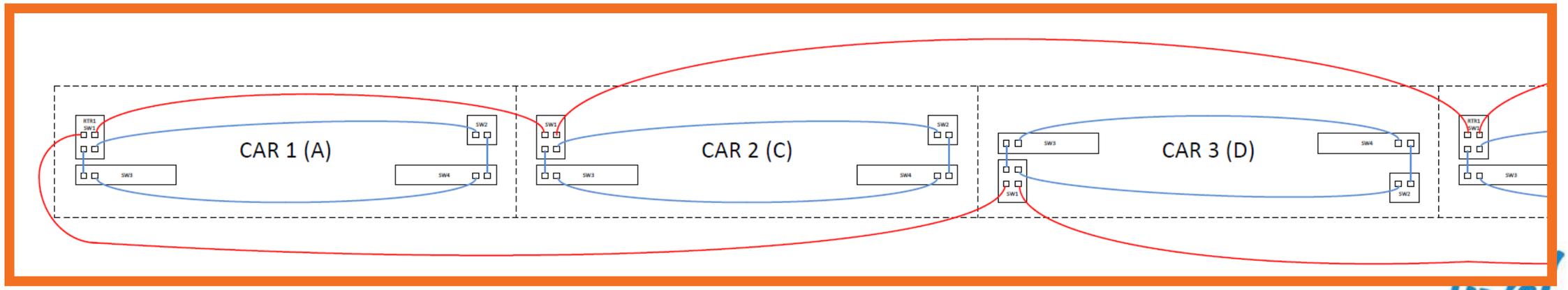
Example Topology Layouts – On-board Rail

Requirements: No car isolation if power fails.

Ring Layout 1

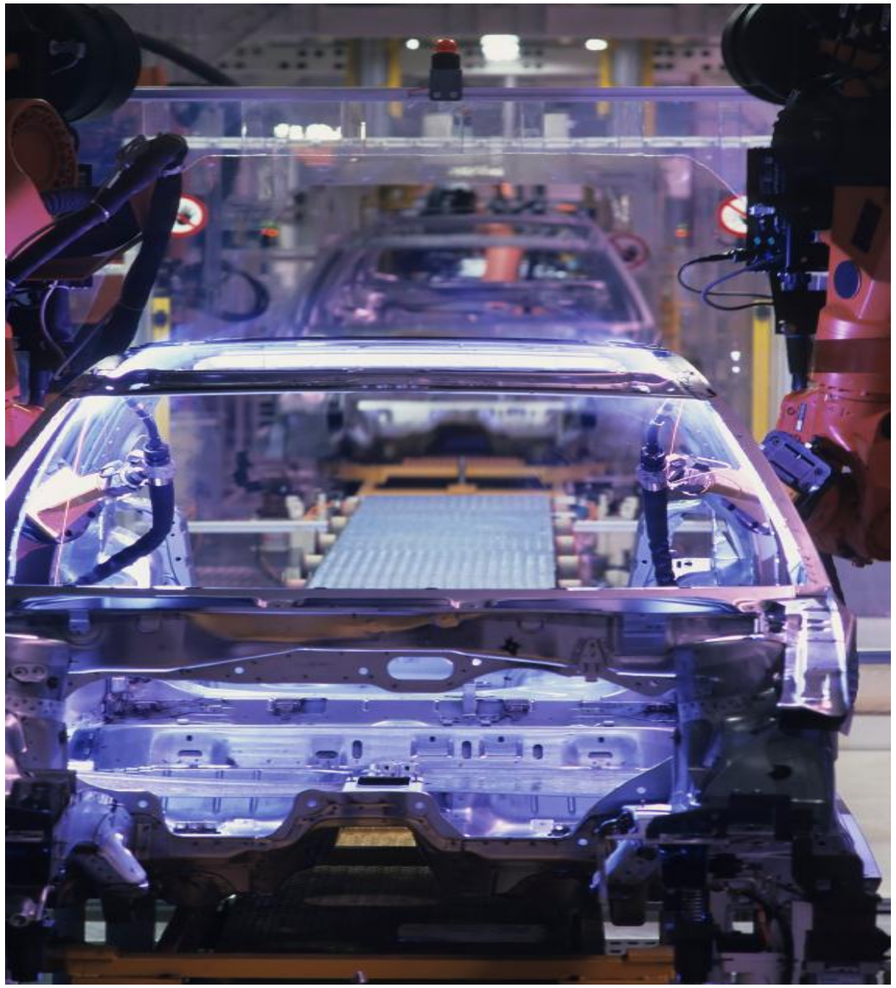


Ring Layout 2



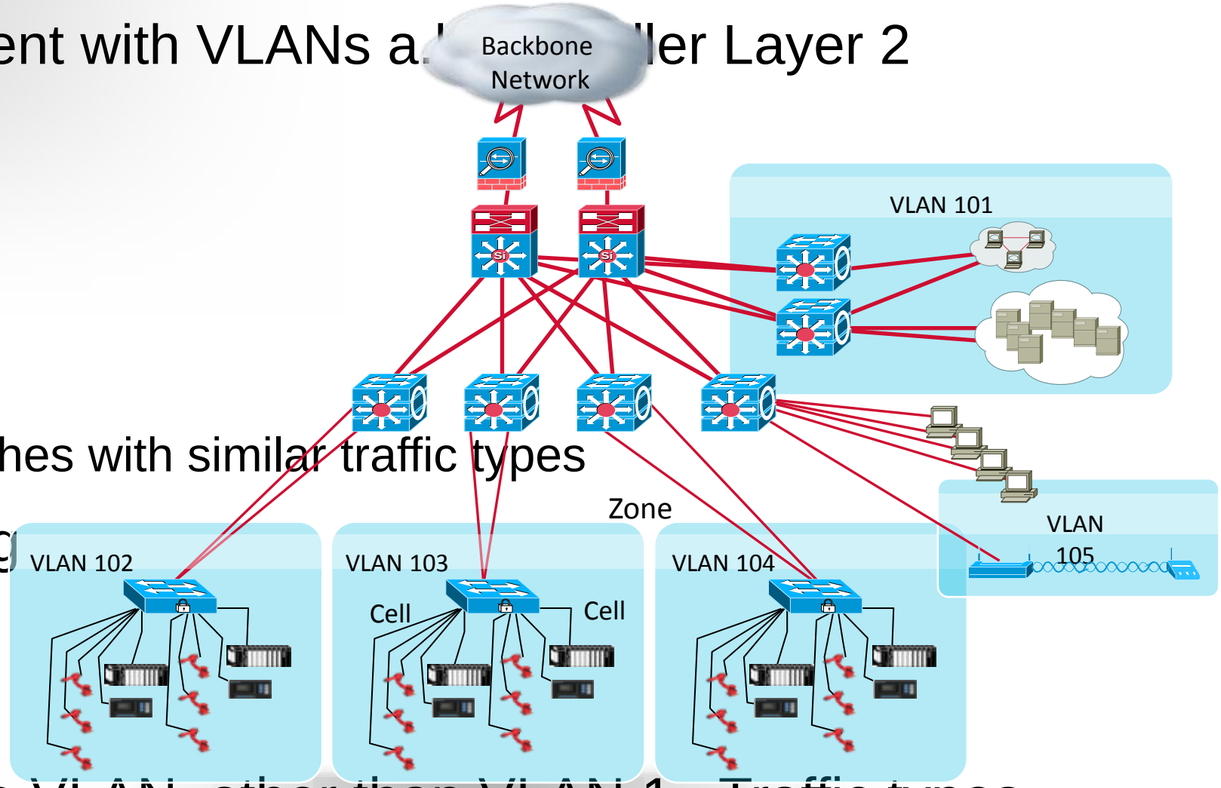
Agenda

- Industry Trends
- Connected Industry Architectures
- Design Considerations
  - Traffic Flows and Topologies
  - Availability and Resilience
  - Segregation and VLANs
  - QoS
  - Security
- Q&A
- Recommended Resources



VLANs in an Industrial Ethernet System

- Design Small Cell/Area zones – Segment with VLANs a… …ller Layer 2 Networks
  - Segment traffic types into VLANs
  - Small IP Subnets per VLAN
- Within the Cell/Area zone
  - Use Layer 2 VLAN trunking between switches with similar traffic types
- Use Layer 3 Inter-VLAN route/switching
  - Between VLANs within the same zone
  - Between zones
- Assign different traffic types to a unique VLAN, other than VLAN 1. Traffic types such as control, information, management, native.

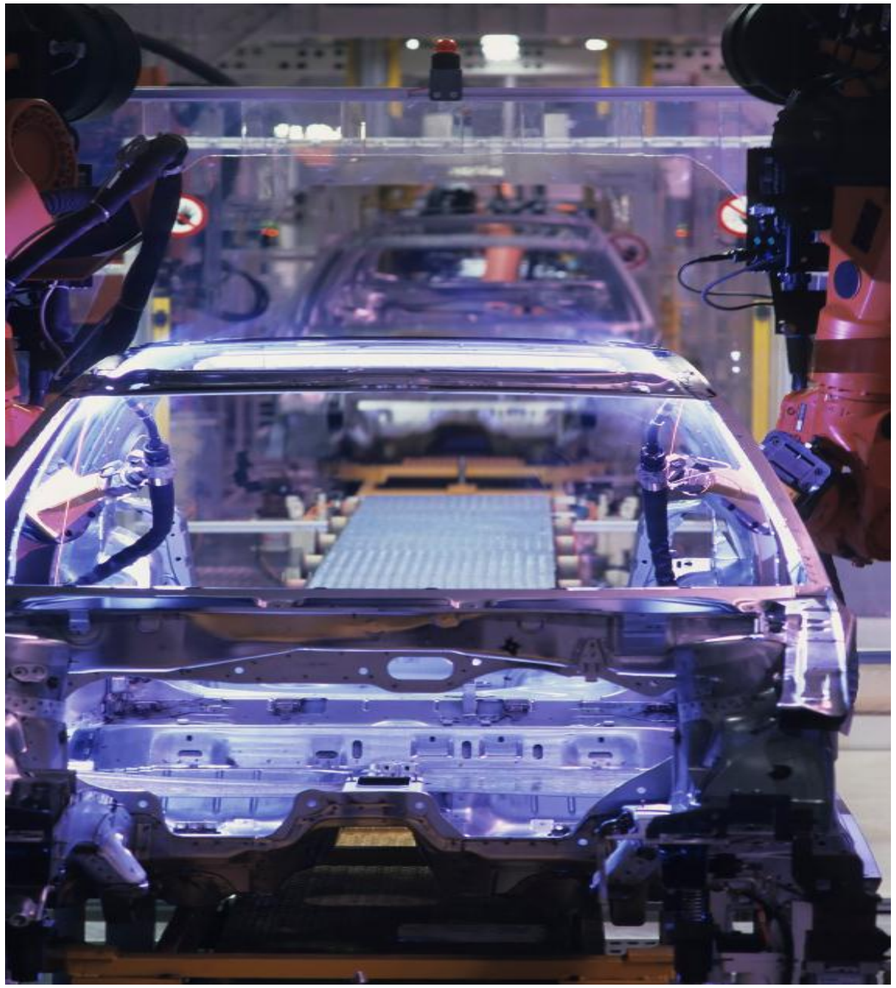


VLAN Considerations for Cell/Area Zone

- Design small Cell/Area zones, segment traffic types into VLANs and IP Subnets to better manage the traffic
- Requires Layer-3 switch or router to communicate between VLANs
- Use Layer 2 VLAN trunking between switches
  - When trunking, use 802.1Q, VTP in transparent mode
  - Set native VLAN to something other than 1
- Use switchport mode host command to assign VLAN to end device
  - Do not use VLAN 1 for EtherNet/IP Control & Information Traffic
- Enable IP directed Broadcast on Cell/Area VLANs with EtherNet/IP traffic for easy c… maintenance from IACS applications
- Prune unused VLANs for security
  - Use VLAN 1 for data is viewed as a security risk
- Create a Network Management VLAN, don't use VLAN 1

Agenda

- Industry Trends
- Connected Industry Architectures
- Design Considerations
  - Traffic Flows and Topologies
  - Availability and Resilience
  - Segregation and VLANs
  - QoS
  - Security
- Q&A
- Recommended Resources



Not All Traffic Is Created Equal

Prioritisation Is Required

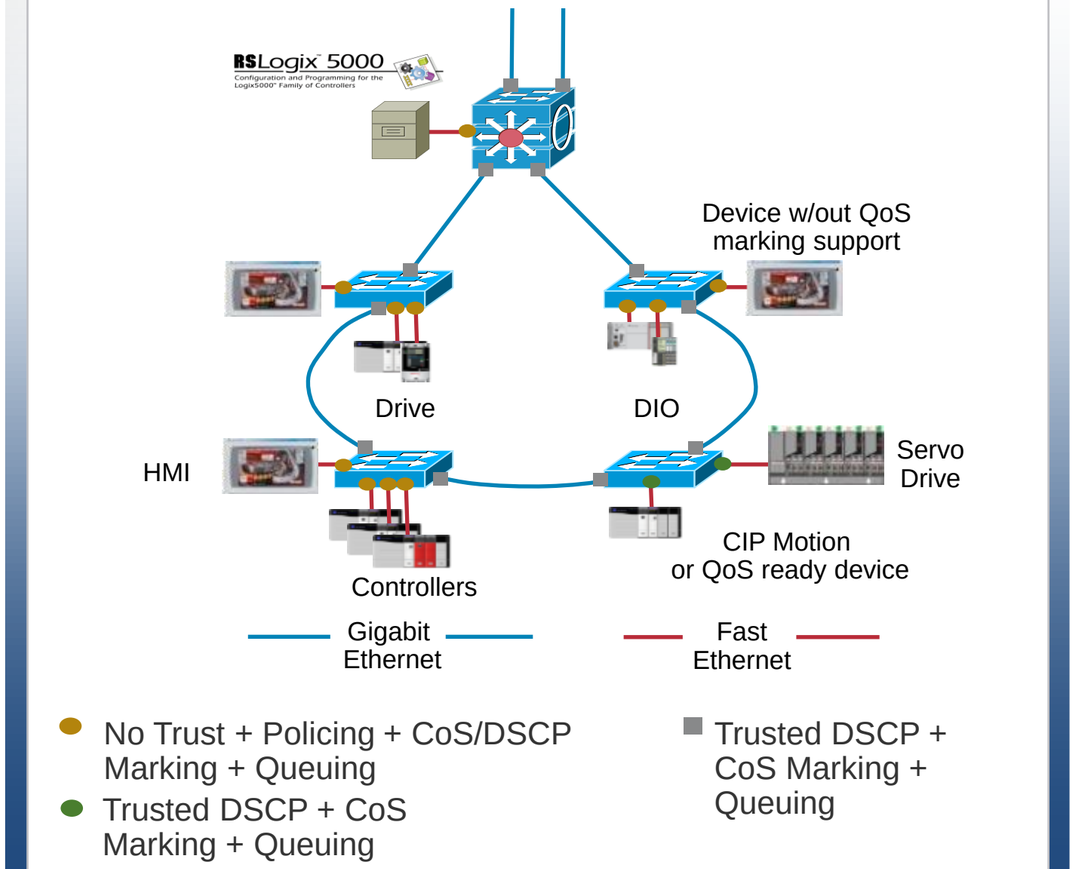
	Control (e.g., CIP)	Video	Data (Best Effort)	Voice
Bandwidth	Low to Moderate	Moderate to High	Moderate to High	Low to Moderate
Random Drop Sensitivity	High	Low	High	Low
Latency Sensitivity	High	High	Low	High
Jitter Sensitivity	High	High	Low	High

Control Networks Must Prioritise Control Traffic over Other Traffic Types to Ensure Deterministic Data Flows with Low Latency and Low Jitter

QoS Design Considerations

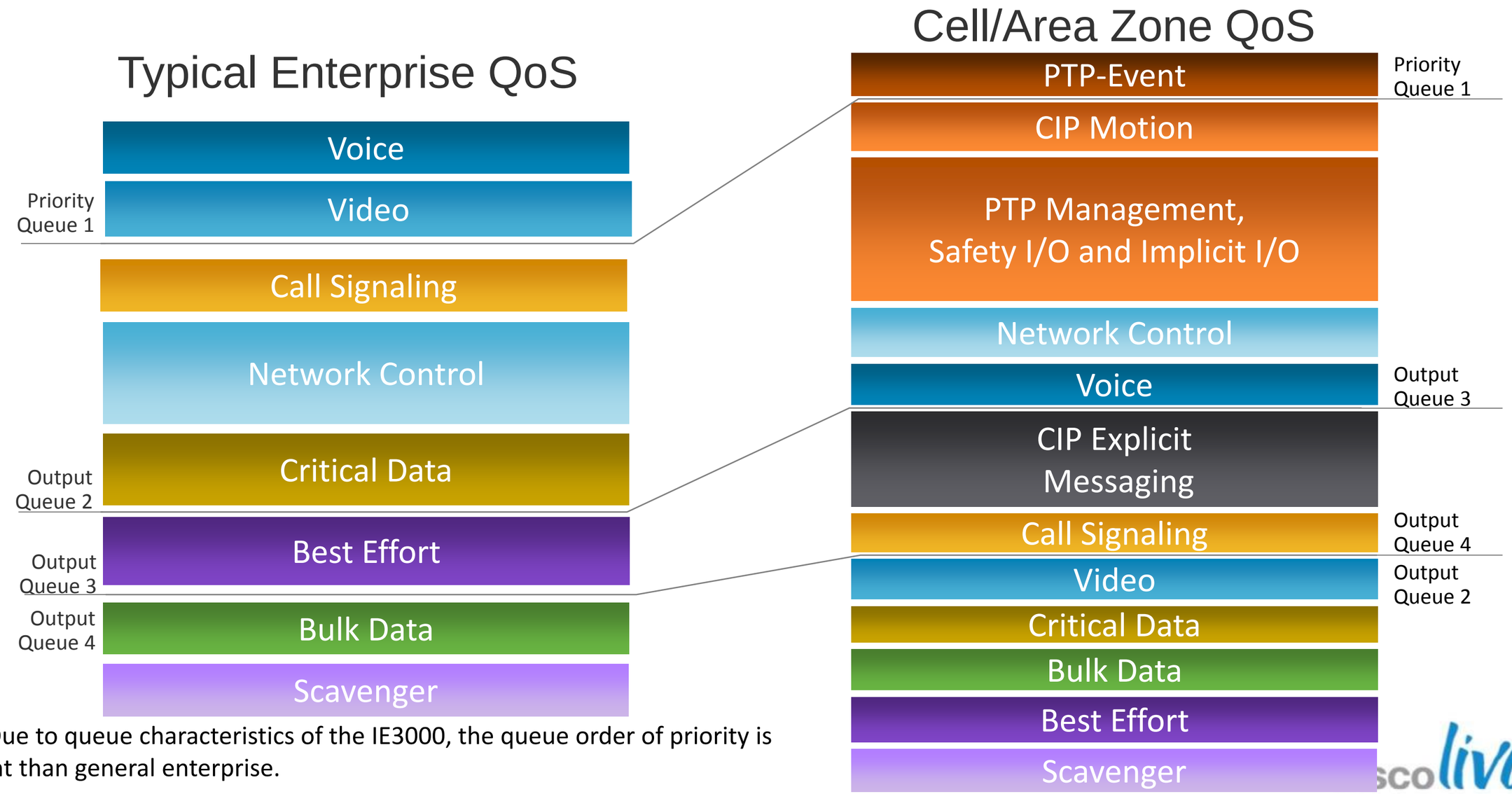
- Priority for latency and jitter sensitive I/O traffic
  - Guaranteed delivery for time sync, motion
  - Minimise impacts by DDoS attacks
- QoS deployed throughout industrial network
- QoS trust boundary moves from switch access ports to QoS-capable industrial devices

- For existing industrial devices, marking at the access port is based on port number e.g.
  - CIP I/O UDP 2222
  - CIP Explicit TCP 44818



Cell/Area Zone QoS Priorities

Example Output Queue Traffic Prioritisation



Note: Due to queue characteristics of the IE3000, the queue order of priority is different than general enterprise.

QoS

Design and Implementation Conside

- QoS is integrated into the standard swit configurations
- Express Setup macros create the QoS policy.
- Smartport macros enables QoS on port
  - QoS-enabled EtherNet/IP device macro for that can mark traffic
  - Regular EtherNet/IP device macro for other automation devices
  - IE-Switch macro applies QoS for trunks and
- Deploy QoS consistently throughout th industrial network.

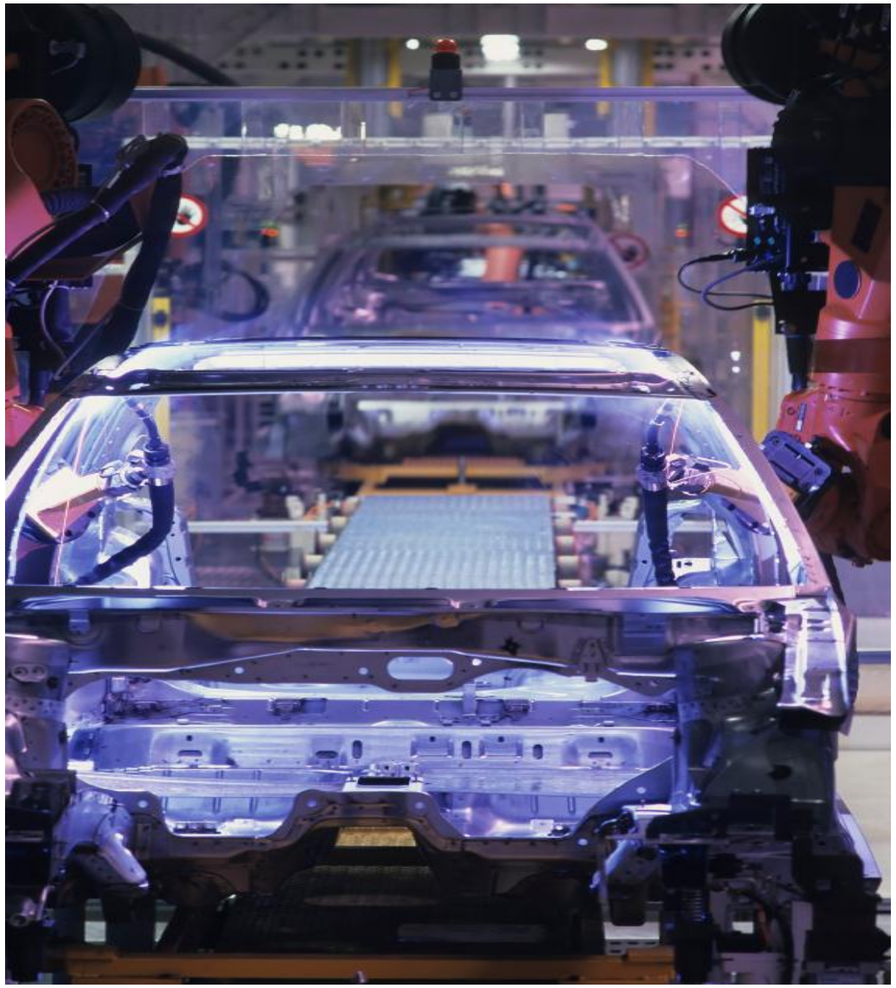
```
rep admin vlan 4
!
!
interface FastEthernet0/1
 description REP fiberloop1
 switchport trunk allowed vlan 4,101-120
 switchport mode trunk
 switchport nonegotiate
 duplex full
 priority-queue out
 rep segment 10 edge primary
 rep preempt delay 15
 rep block port 22 vlan 1-4094
 mls qos trust dscp
!
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 priority-queue out
 spanning-tree portfast
 service-policy input mark_roadrunner_server_in
```

```
class-map match-all mark_roadrunner_server_in
 match access-group name mark_roadrunner_server_in
!
!
policy-map mark_roadrunner_server_in
 class mark_roadrunner_server_in
  set dscp ef
 class class-default
  set dscp default
!
ip access-list extended mark_roadrunner_server_in
 permit udp any any eq 9500
```

Quality of Service Does Not Incr
Treatment to Automation and Contr

Agenda

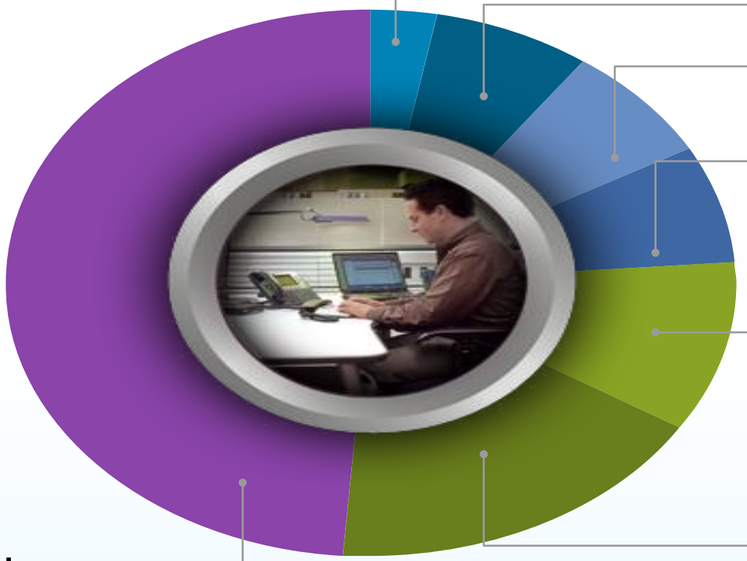
- Industry Trends
- Connected Industry Architectures
- Design Considerations
  - Traffic Flows and Topologies
  - Availability and Resilience
  - Segregation and VLANs
  - QoS
  - Security
- Q&A
- Recommended Resources



Industrial Security

Source of Industrial Security Incidents

Source: BCIT (2009)



3% Wireless System

7% VPN Connection

7% Dial-up Modem

7% Telco Network

10% Trusted Third-Party Connection (Includes Infected Laptops)

17% Internet Directly

49% Via Corporate WAN and Business Network

Average Cost of Manufacturing Downtime = $210,000 per Hour

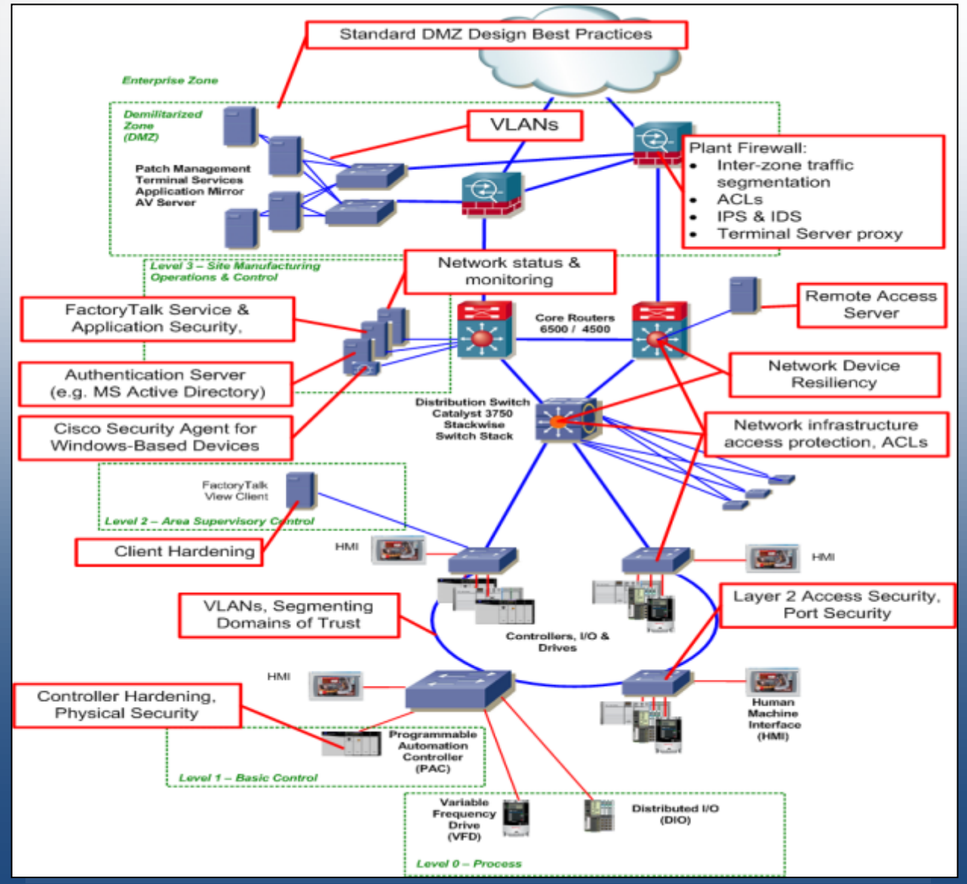
Source: Infonetics (2005)

Common Areas of Vulnerability

- Fragile TCP/IP Stacks – NMAP, Ping Sweep lockup
- Little or no device level authentication
- Poor network design – daisy chains, hubs
- Windows based IA servers – patching, legacy OS
- Unnecessary services running – FTP, HTTP
- Open environment, no port security, no physical security of switch, Ethernet ports
- Limited auditing and monitoring of access to IA devices
- Unauthorised use of HMI, IA systems for browsing, music/movie downloads
- Lack of IT expertise in IA networks, many blind spots

Security Guidelines

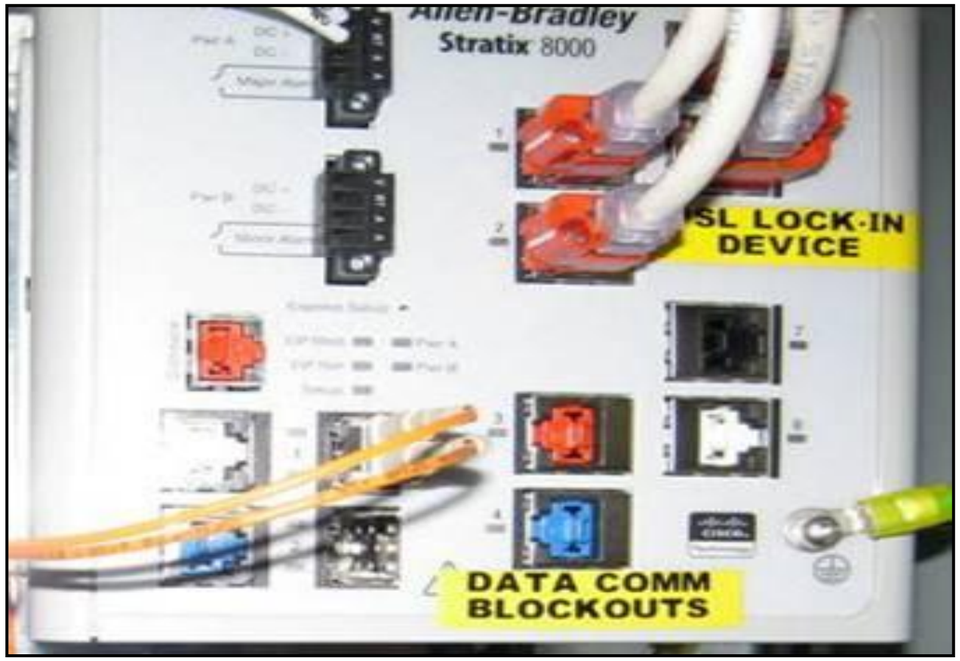
- Controls Security Policy
- Demilitarised Zone (DMZ)
- Defending the Control edge (IPS/IDS, ISE)
- Protect the Interior (ACL/Port Security)
- Remote Access Policy
- Small Domains of Trust
- Physical Security
- Endpoint Hardening



Defence-in-Depth

Physical Security - Examples

- Keyed solutions for copper and fibre
- Lock-in, Blockout products secure connections



PANDUIT®

Cisco live!

DMZ and Secure Remote Access

Guiding Principals

Use IT-Approved Access and Authentication

- VPN for secure remote access
- Enterprise Access and Authentication servers (e.g Active Directory, Radius, etc.)

IAC Protocols Stay home

Control the Application

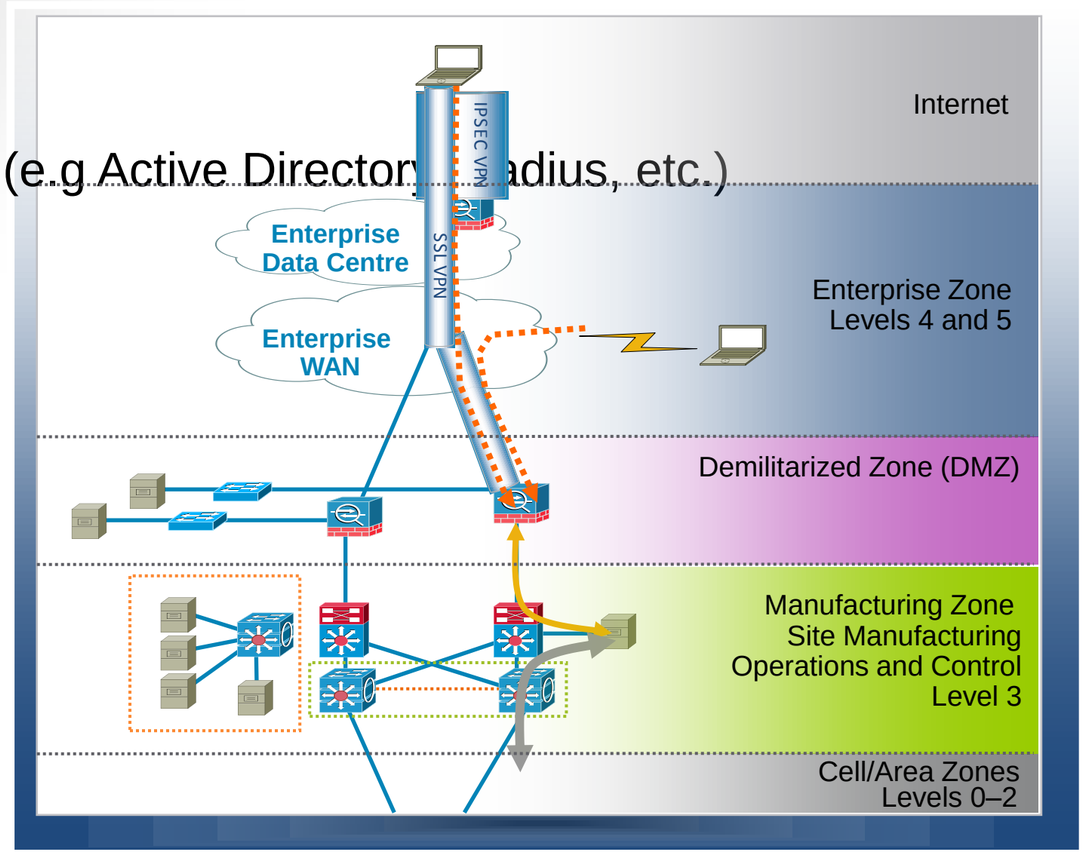
Remote Access (Terminal) Server

Application level security

No direct traffic through the firewall

Only one path in and out of manufacturing zone

—the firewalls

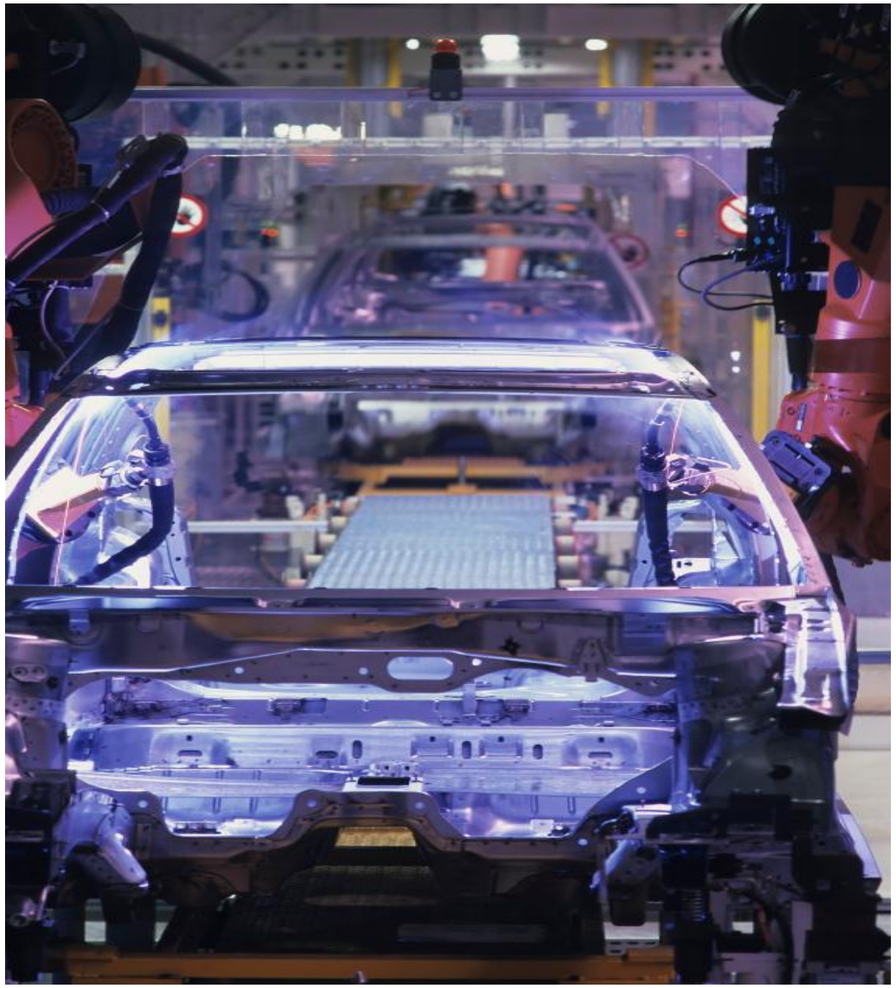


Additional Best Practices

Feature	Description	Mechanism
Network Foundation Protection	Protecting the core network infrastructure and services from unauthorized access, changes or attacks	Port security, Layer 2 and 3 protection, configuration templates
Trust and Identity	Confirmation that a user or device that is requesting service is a valid device. Authentication, Authorization and Accounting	ACLs, MAC-filtering, VLANs, FactoryTalk Security, application authorization
Threat Detection & Mitigation	Continuously and proactively monitor network activity for anomalous behavior	Firewall, Intrusion Protection, Analysis and Response, Syslog
Layer 2	Employ L2 features to minimize possible network outages	VTP transparency, Loop/Root/BPDU guard, DHCP snooping, VLAN pruning, disable ports
Secure Connectivity	Secure the communication over un-trusted transport environments	VPN, Encryption, IPsec
Security Management	Configuration, monitoring, analysis and respond to network activity.	Policy enforcement, monitoring, analysis and response, audit and reporting

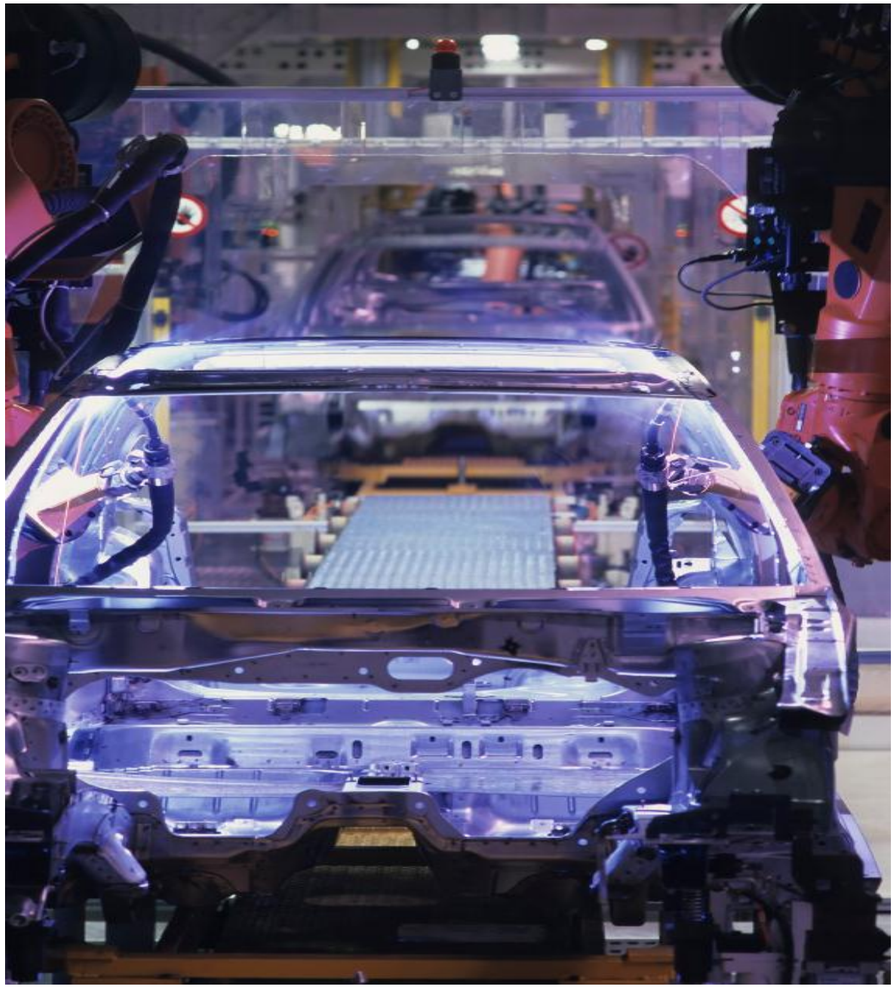
Agenda

- Industry Trends
- Connected Industry Architectures
- Design Considerations
- Q&A
- Recommended Resources



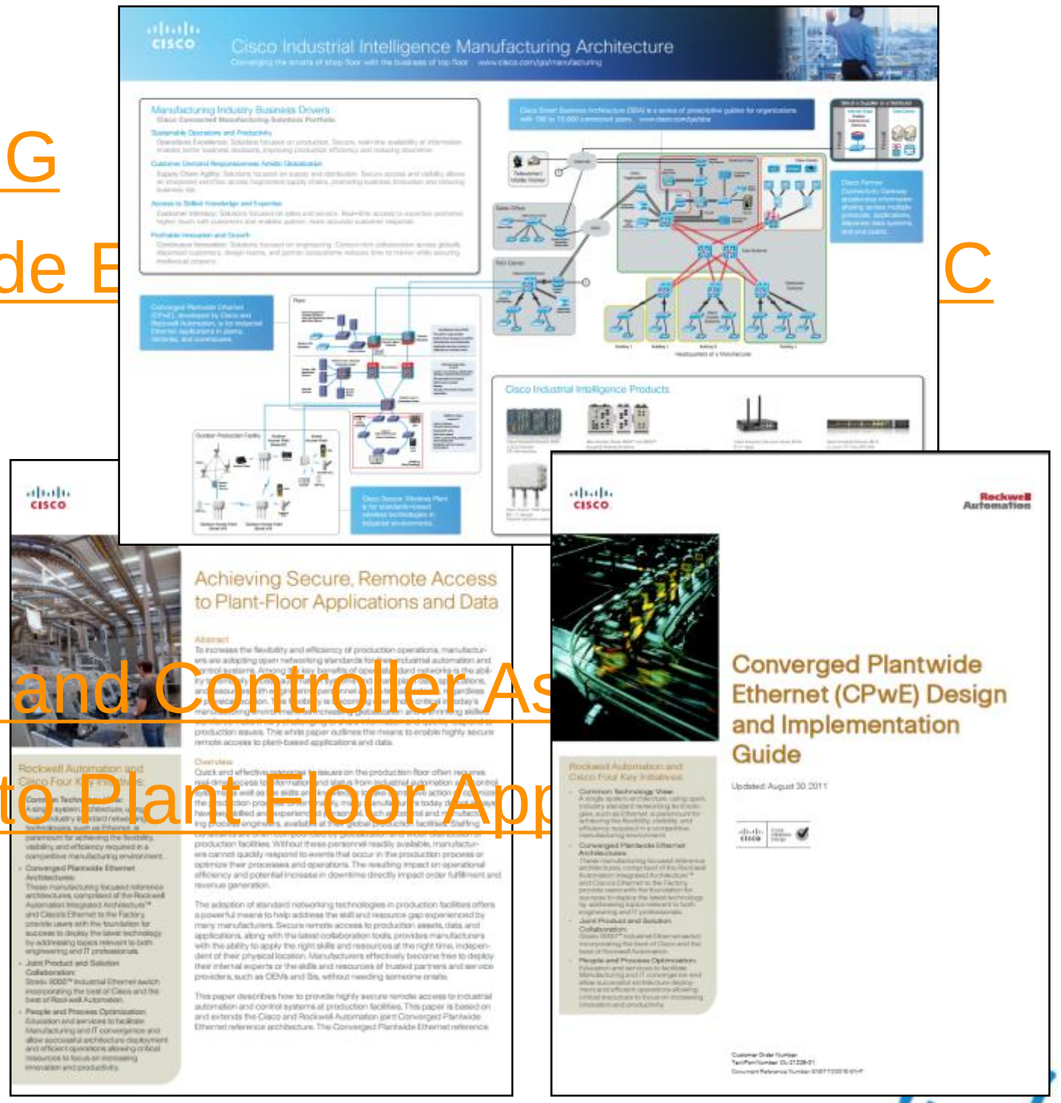
Agenda

- Industry Trends
- Connected Industry Architectures
- Design Considerations
- Q&A
- Recommended Resources



Recommended Resources

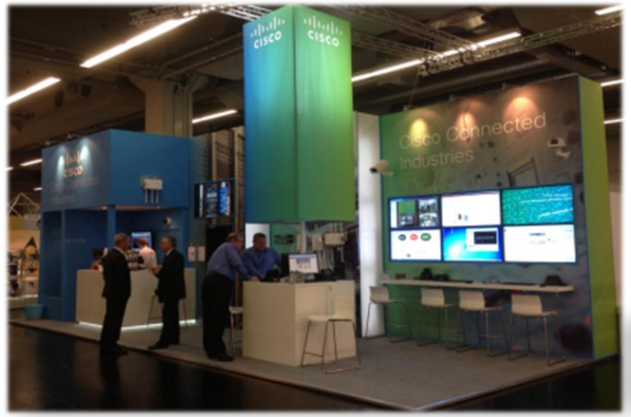
- Converged Plant-Wide Ethernet DIG
- Planning for a Converged Plant-wide E… C Group
- Secure Wireless Plant
- Industrial Intelligence Architecture
- Securing Manufacturing Computer and Controller As…
- Achieving Secure Remote Access to Plant Floor App…



Call to Action

- **Visit** the IoT exhibition in the World of Solutions
  to experience the following demos/solutions in action:
  Networked Automation, Secure Remote Access, Resilient Ethernet Protocol, Virtualised SCADA, Sensor Mesh Networking

- **Meet** the Engineer
  Available in the MTE village on Thurs 31st from 10:30am-12pm



Ciscolive!

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww

Cisco live!