
TOMORROW starts here.
cisco
Cisco live!

Industrial Networking Concepts, Design, Resilience and Security

BRKRST-2661

David Bell
Consulting Solution Architect
Industry Solutions Group – Ecosystems

Cisco live!

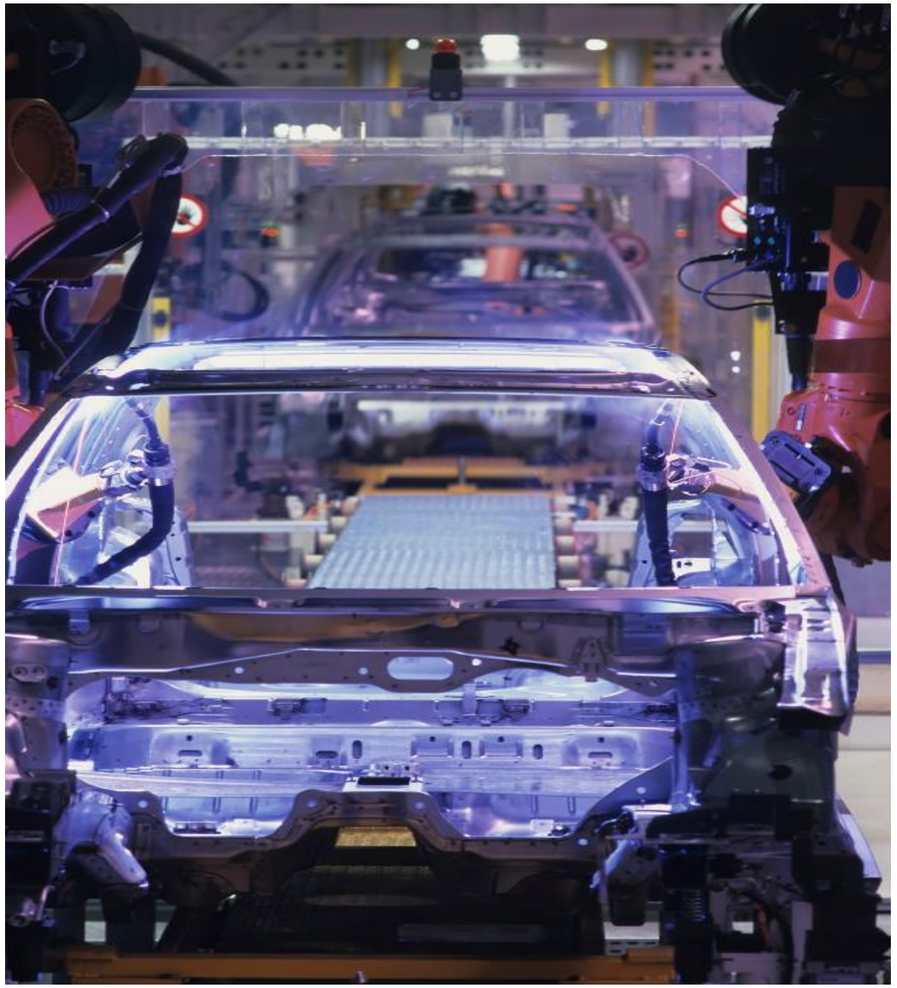
Session Abstract

Session Title: Industrial Networking Concepts, Design, Resilience and Security

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.

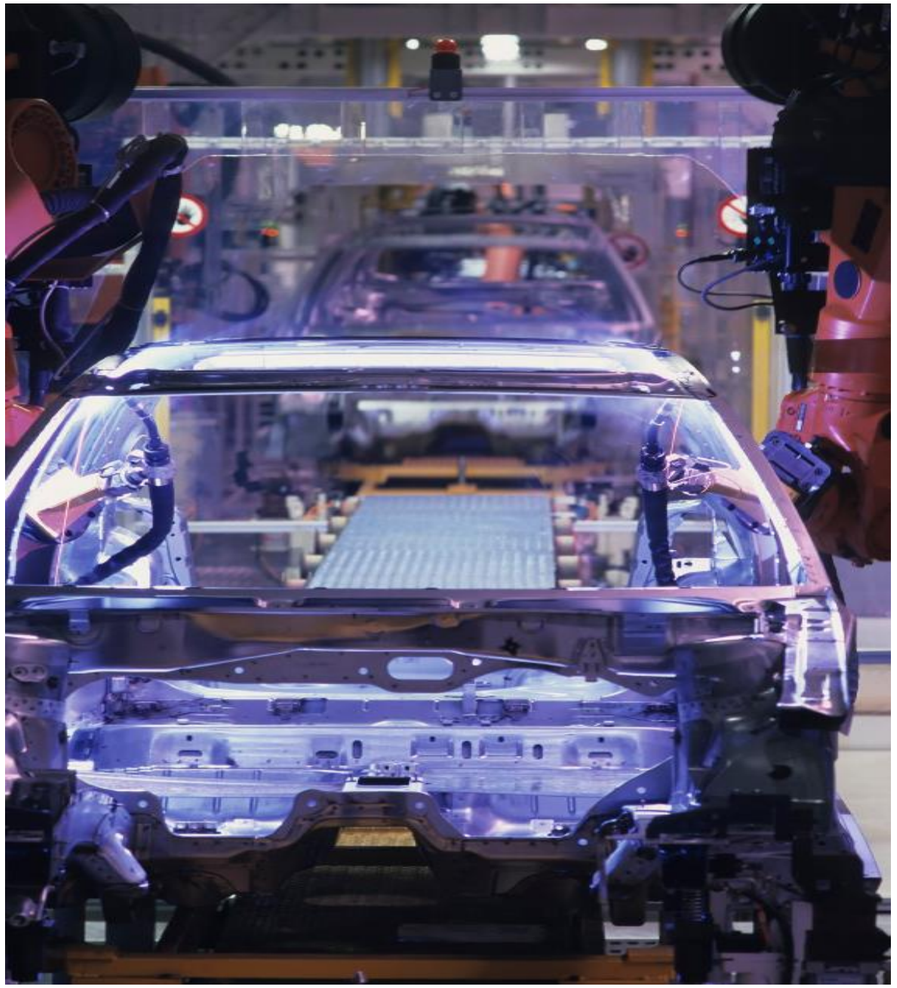
Agenda

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



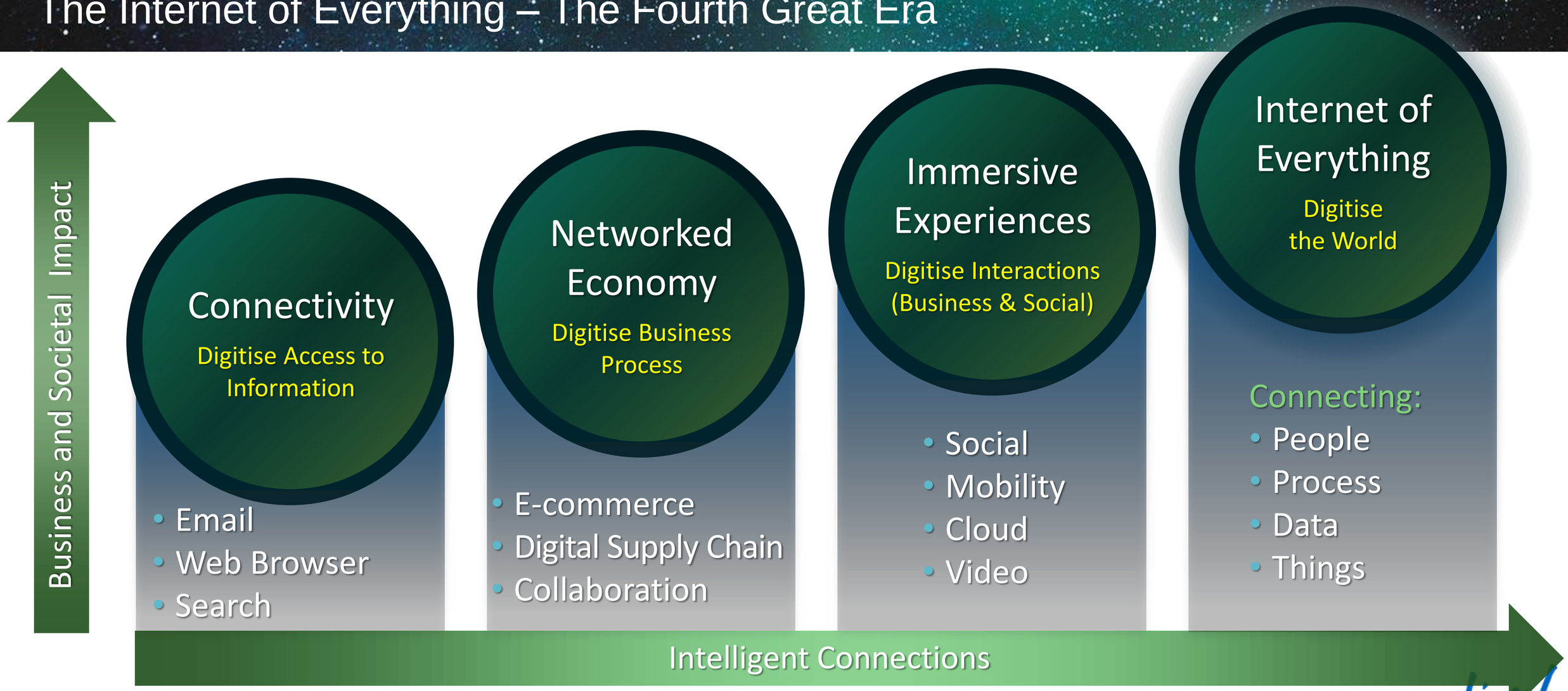
Agenda

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



Evolution to IoE

The Internet of Everything – The Fourth Great Era



IoT in the Real World

The future is already here

- ✓ 120 sensors…
- ✓ 1,000 readings / sensor / second / race
- ✓ Approx 750-850 **Million** data points / race
- ✓ Trying to save 2/10th second per lap

http://www.youtube.com/watch?v=SpJ-YYIDD9k

“ We grab information and turn it into stories and use them to make decisions on how we race.”

“The more we measure the more we understand.”

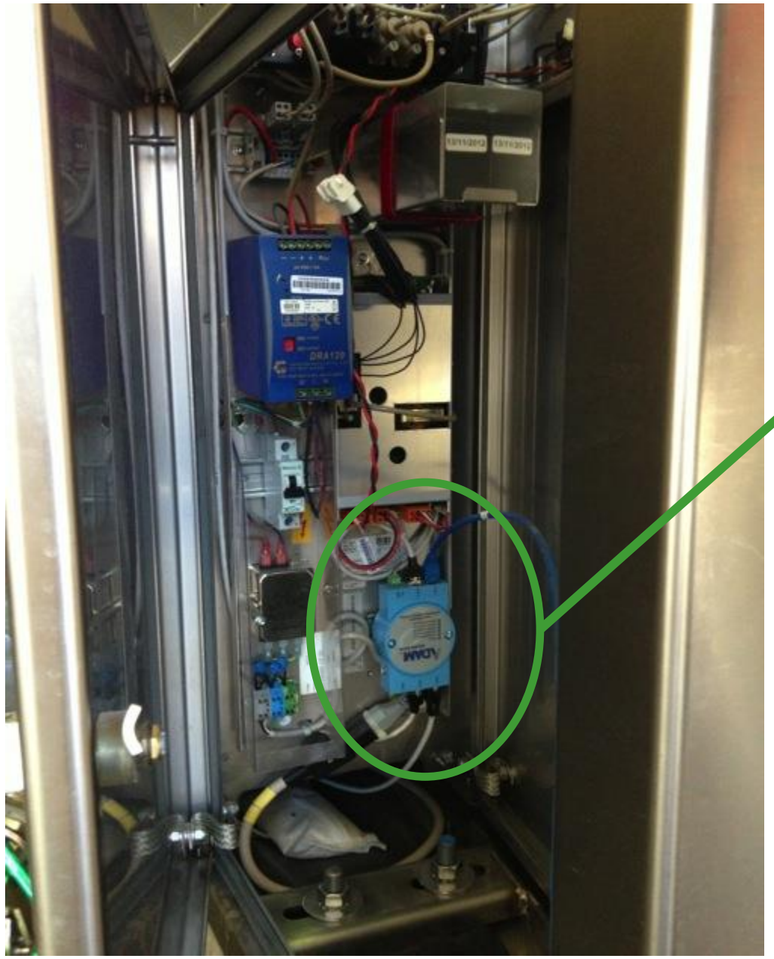
Peter van Manen, Managing Director, McLaren

Industrial Networking is Everywhere!

Walking past Flinders Street station, Melbourne (Cisco Live ANZ)

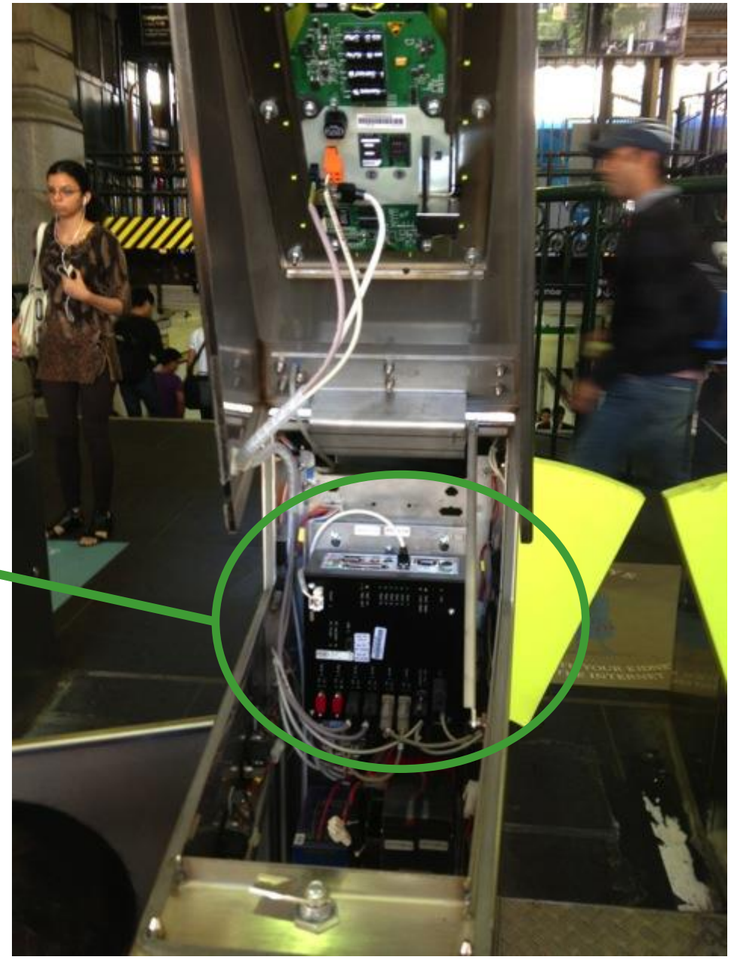
Industrial Networking is Everywhere!

Walking past Flinders Street station, Melbourne (Cisco Live ANZ)



Industrial Switch

Industrial PC



Industrial and Enterprise Networks Are Converging

Cisco Internet of Things Group - IOTG

Connected Industries

+

Connected Energy

+

Connected Safety & Security

=

Internet of Things Group

Cisco IoT – Industry, Energy and Security

New 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

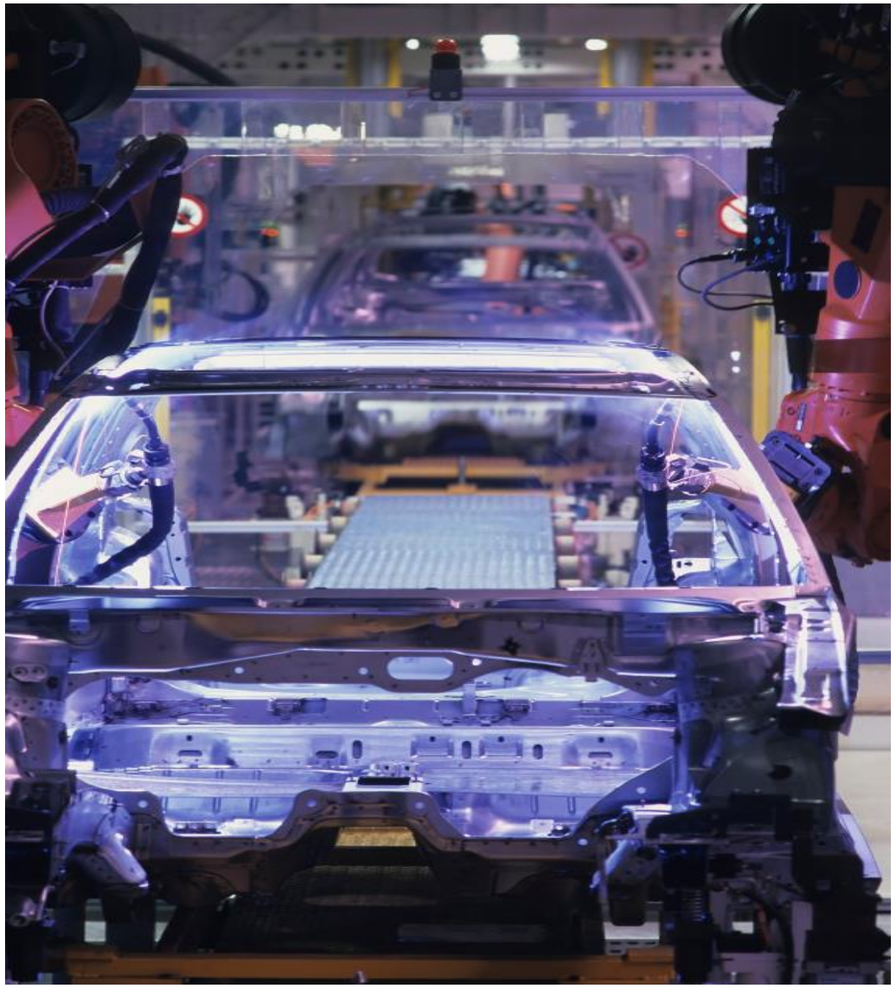
Unauthorised actions by employees

Unauthorised remote access

Unintended employee actions

Agenda

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



Industrial Networking 101..

..or, what's on the other side of the curtain?

Industrial Networks

- Industrial Networks are old style multi-protocol networks and the Internet of Things at once

- Don’t confuse IT ‘networking’ with OT ‘networking’ - they are very different animals

Industrial Sector ‘Definitions’

Discrete is about making ‘objects’ that **can** be returned to constituent parts

- The final product may be produced out of single or multiple inputs based on a Bill Of Materials.
- Examples: automotive, white goods, electrical devices




Process is associated with formulas and manufacturing recipes that **cannot** be returned to constituent parts

- Packaging ‘recipes’ can be considered alongside the process recipes as they define the final assembly

Examples: Petrol, food and beverages, paints and coatings, specialty chemicals,



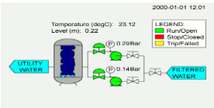
Some industries may be hybrid and contain both discrete and process. E.g. Pharmaceuticals ..

Industrial Networking Lexicon

Talk the OT Language

Applications

MES - Manufacturing Execution System. Collection of software..



SCADA - Supervisory Control and Data Acquisition. ICS/DCS*.

Historian – Data collection and analysis.

* ICS - Industrial Control System (Discrete)
DCS - Distributed Control System (Process)

Cell/Area Zone – Smallest area where something is made.

Devices

HMI - Human Machine Interface. Control and monitoring point.

PLC/PAC - Programmable Logic (Automation) Controller.

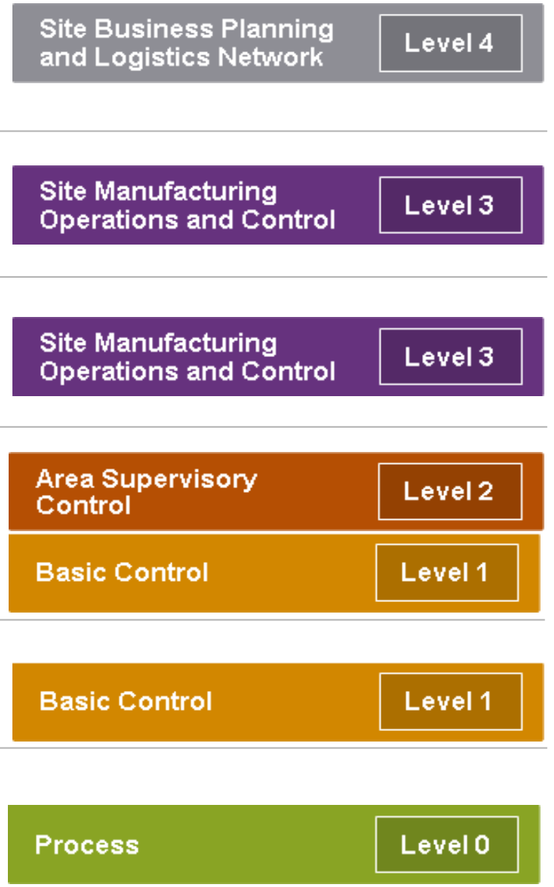
I/O - Input / Output.

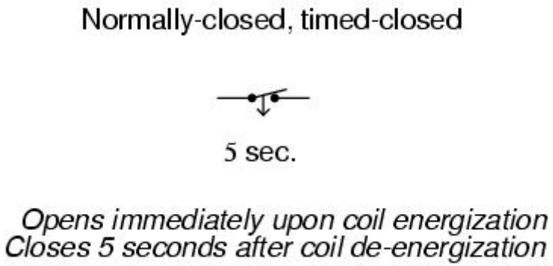
Actuator/Drive – Makes something happen.

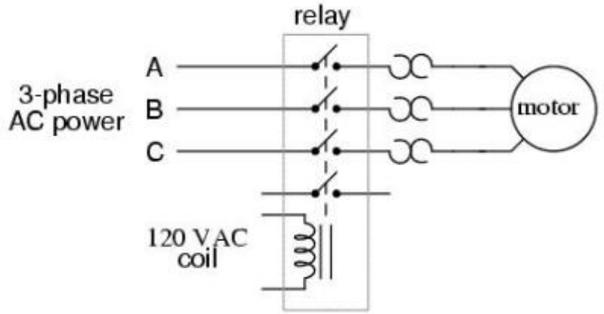
Industrial Lexicon 101

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

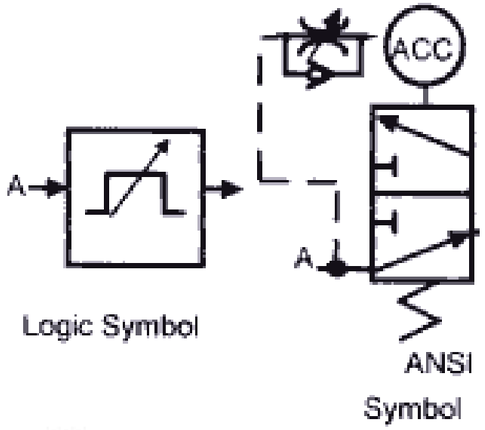


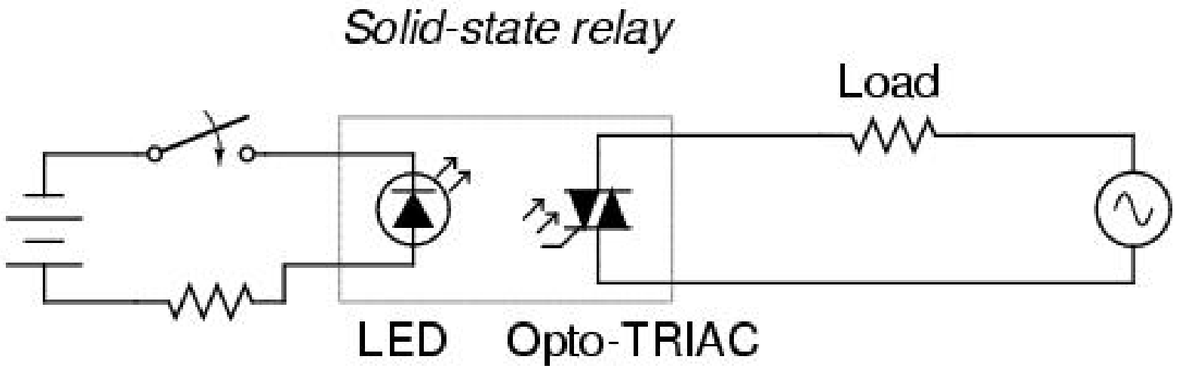


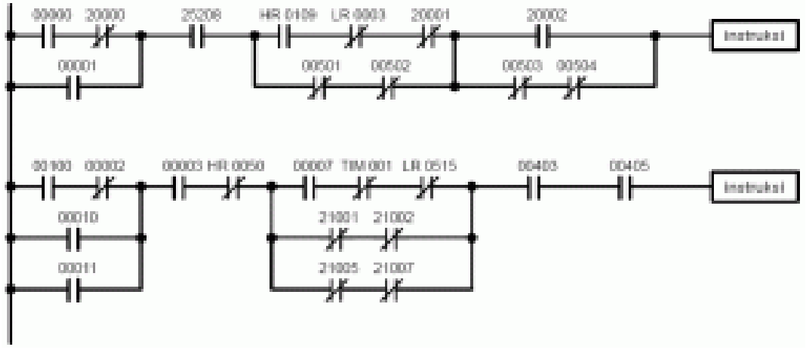


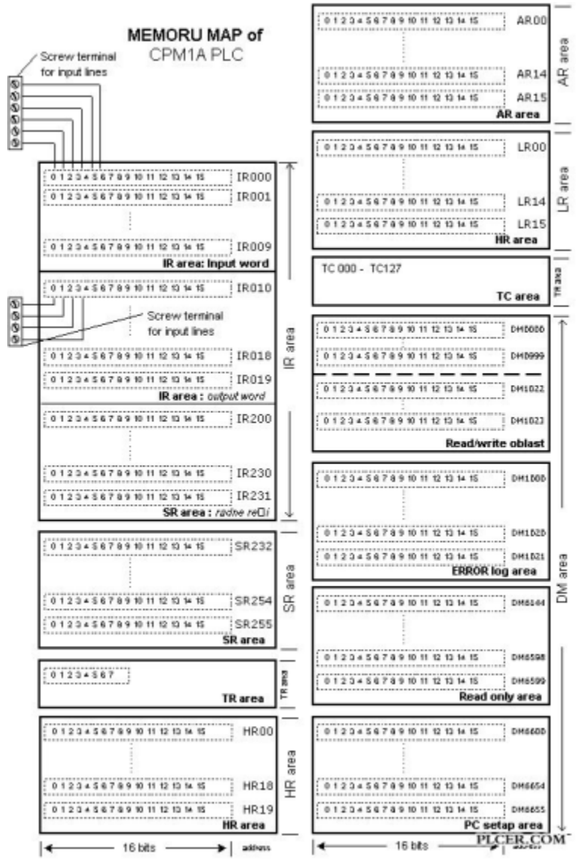
In the beginning…

Motion in the industrial space was accomplished with human, wind, water and great beasts









…then along came the PLC…

The Programmable Logic Controller

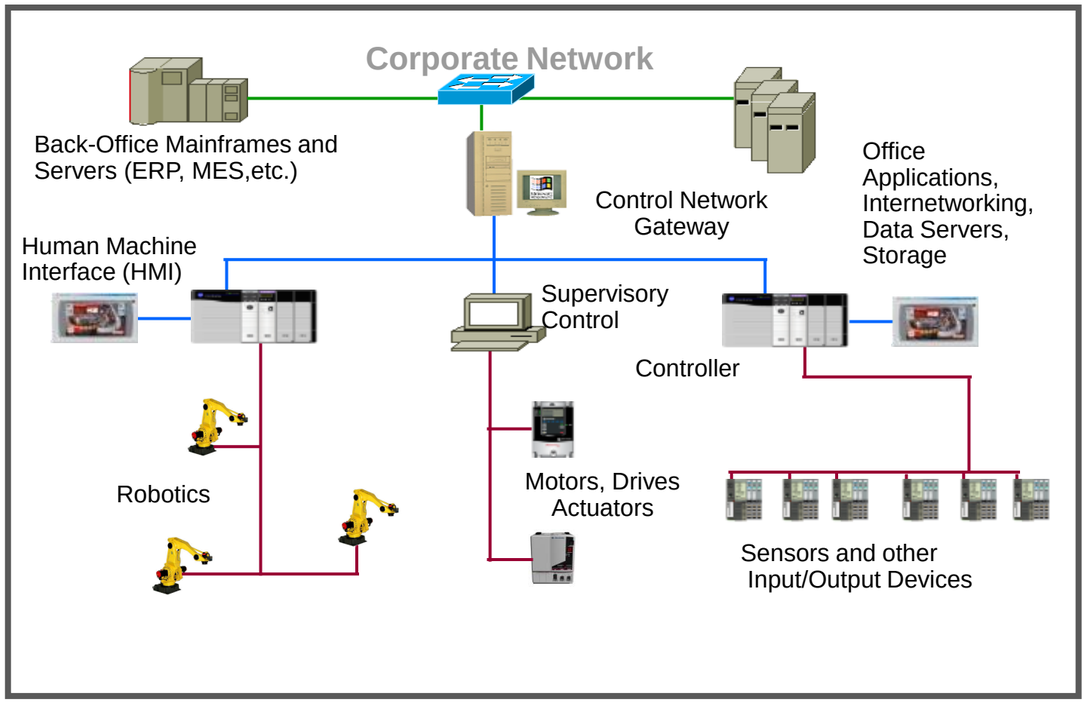
A small ‘hardened’ computer (temp/environmentals)

Use ‘I/O’ devices to communicate with external switches and feedback sensors

Support both digital and ‘analog’ signals via this I/O

Programmed with **ladder logic** ‘simulates’ basic binary switch concepts

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



Control Loops Could Not Tolerate This

Legacy 10BASE2/10BASE5 Ethernet: Lots of CSMA/CD Collisions
The reason Ethernet got a bad rep with determinism…

Evolution of Ethernet

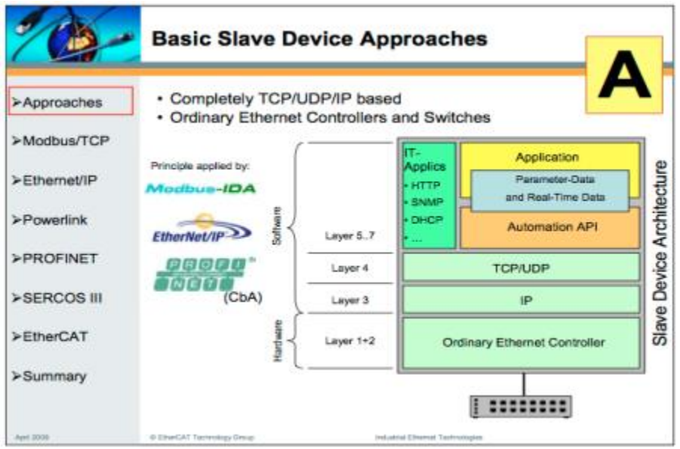
10BASE-T, Fibre and Beyond: Full Duplex Switched

Major Improvements. Add QoS but still not often converged or (necessarily) deterministic…

A Plethora of Standards and Protocols

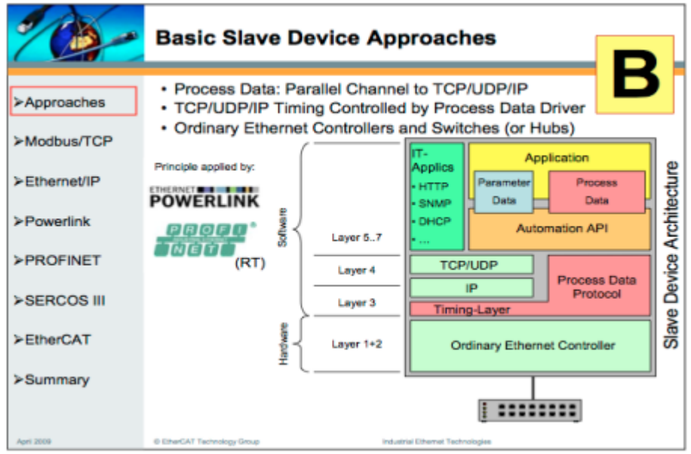
Familiar story – drive to consolidate standards and protocols

Standard Network Stack



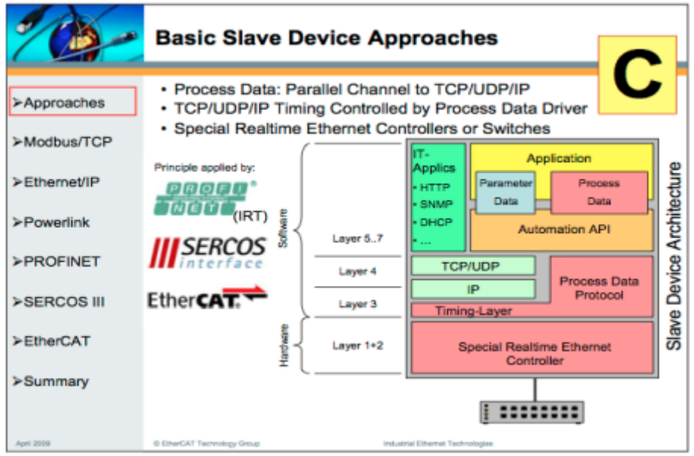
- Based on Open Standards at layers 1-4
- Use of IEEE 1588 Precision Time Protocol (PTP) for further determinism
- Viewed as slow or non-deterministic

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

Common Industrial Automation Protocols

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

- CIP - Common Industrial Protocol. 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 (Common Industrial Protocol.)
- Ethernet Powerlink – a deterministic open protocol managed by the Ethernet POWERLINK Standardisation 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.

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.

Common Protocol Characteristics

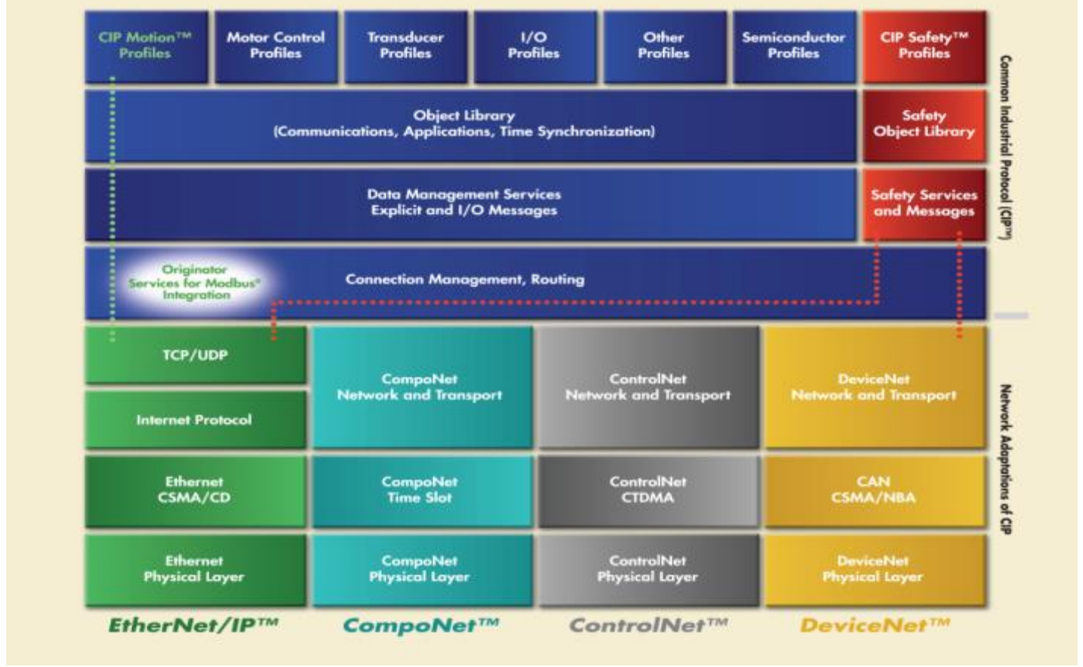
- The important stuff happens in the data part
- Notion of time
  - Cyclic
  - Isochronous
  - Deterministic
- Derived from the original controller
  - Example HART is really about device description. In the same way Profinet sends GDSML data (XML format) to describe a device.
  - The registers and the values defined to that area of memory are manufacturer specific
- Most supported by an “independent standards group”
- Some standards are open and some are “pay to play”
- Most attempt to provide many if not all of the following services
  - Control
  - Safety
  - Synchronisation
  - Motion
  - Configuration
  - Information
- More proprietary is more deterministic and less latent.

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
- EtherNet/IP is based on Ethernet, IP and TCP/UDP
- Supported by the Open Device Vendor Association
- Key communication includes:
- CIP Control traffic: I/O control, drive control
  - Uses UDP protocol (multi-cast and uni-cast)
- CIP: Information traffic: HMI, MSG's, Program upload/download
  - Uses TCP protocol
- Other common traffic
  - HTTP, Email, SNMP, etc.

- Uses EDS files (Electronic Data Sheet) on devices to describe properties and functions of field devices
- Pre-installed and configured on Cisco IE switches

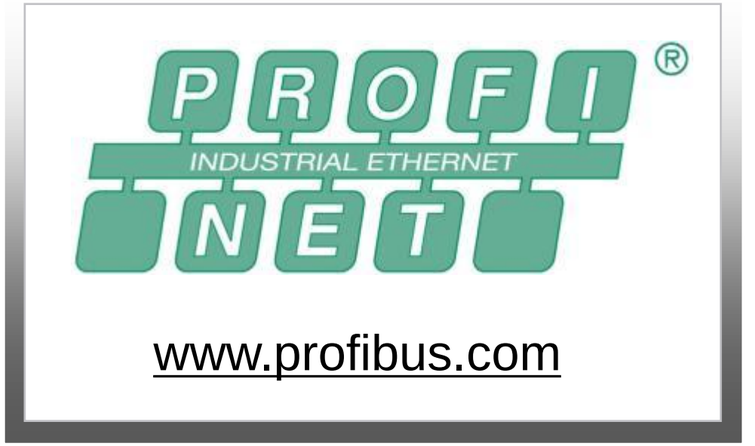


ODVA: www.odva.org

What are Profinet CBA, Profinet RT and Profinet IRT

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

- PROFINET CBA/IP - Typically messaging, program download, diagnostics etc. Layer 3 UDP/IP.
- PROFINET RT – Communication class of PROFINET IO. Layer 2.
  - Transmission of data, alarms and control
  - Cycle times of 5-30ms
  - Uses standard Ethernet
- PROFINET IRT – Communication class of PROFINET IO. Layer 2 non-standard.
  - 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

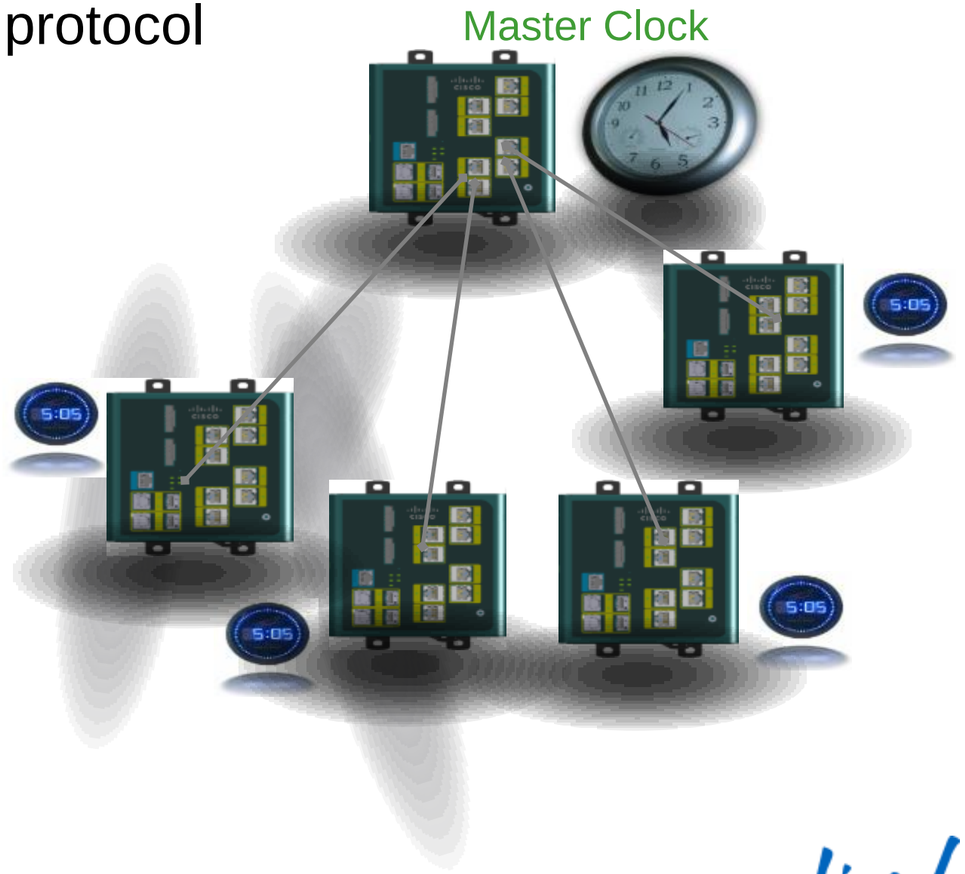


- PROFINET uses GSD file (General Station Description) to describe properties and functions of field devices.
- GSD files are pre-installed and configured on Cisco IE switches

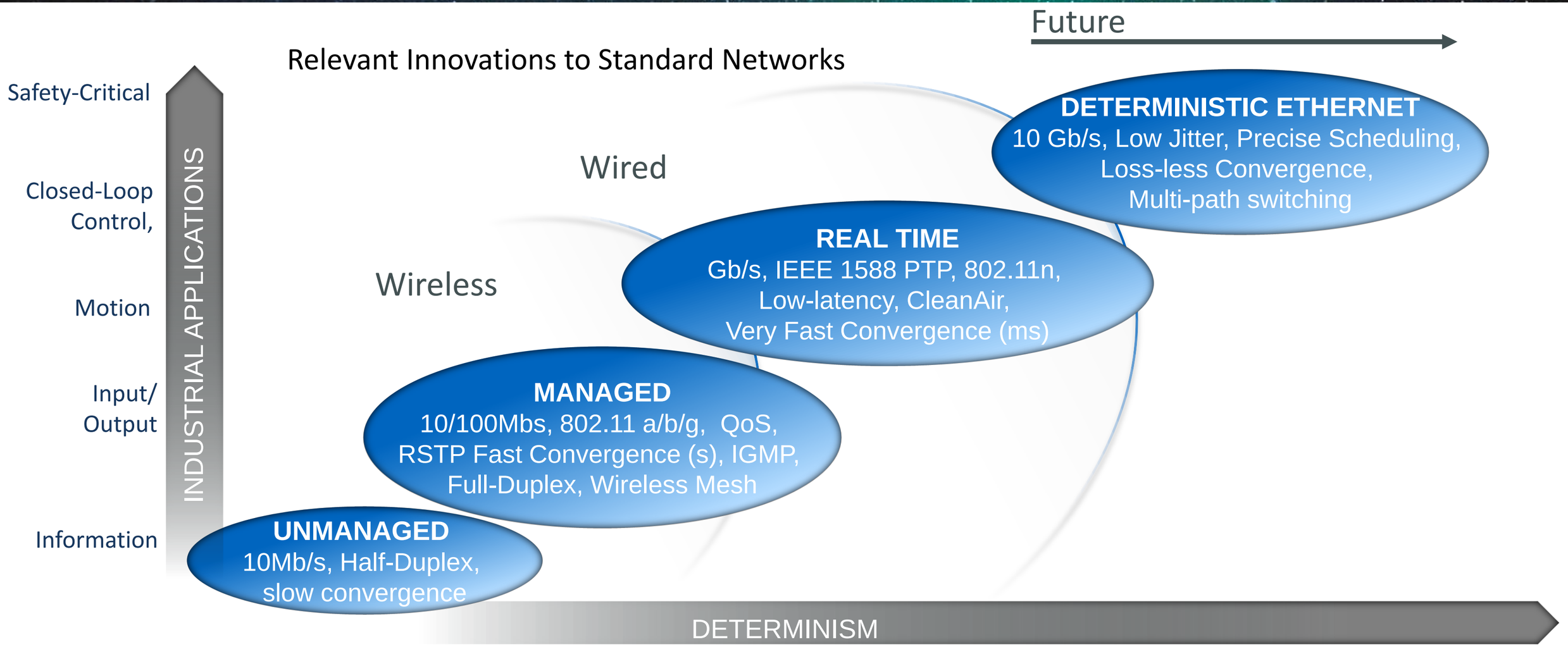
Industrial Time Synchronisation

IEEE1588 – PTP – Precision Time Protocol

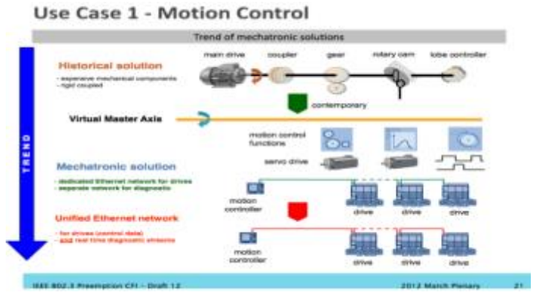
- Distributed control components to share a common notion of time
- Implements IEEE-1588 precision clock synchronisation protocol
  - Provides +/- 100 ns synchronisation (hardware-assisted clock)
  - Provides +/- 100 µs synchronisation (software clock)
  - NTP is approx 2ms-1000ms depending on LAN/WAN conditions
- 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.

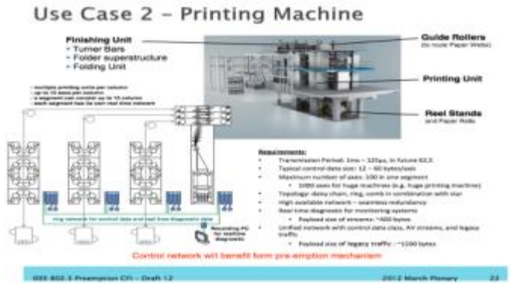


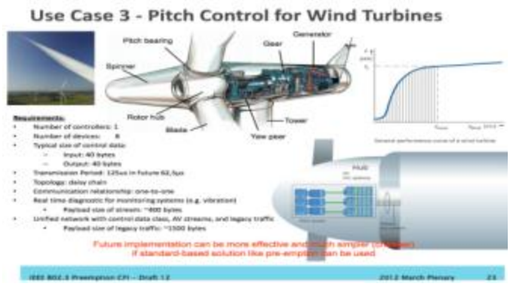
Industrial Communications Evolution

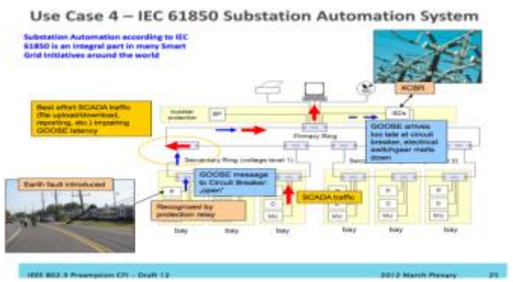


Deterministic Ethernet Standards





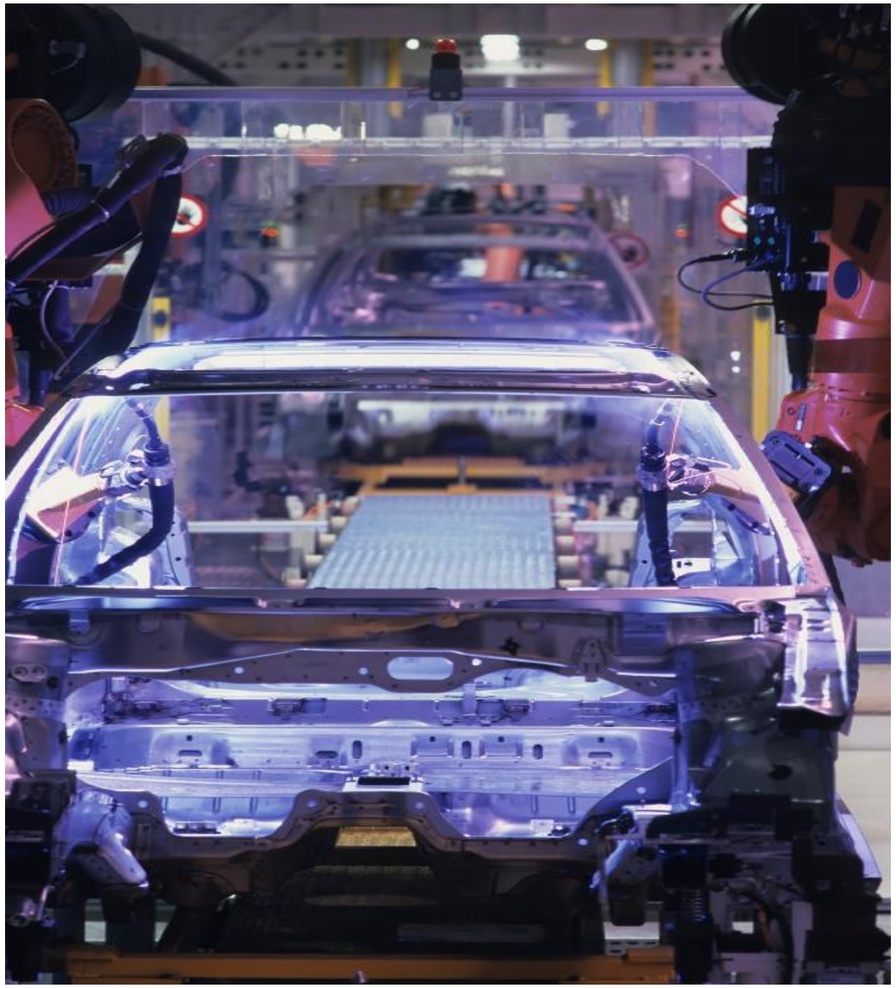




- Cisco and IEEE 802.1 & 802.3 are undertaking to make Ethernet deterministic including:
  - Guaranteed Delivery over a variety of multi-path topologies
  - Scheduled Delivery; Low-latency (< x µs), low-jitter
  - Time synchronisation across end-devices and the network (<100ns drift)
  - Converge critical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

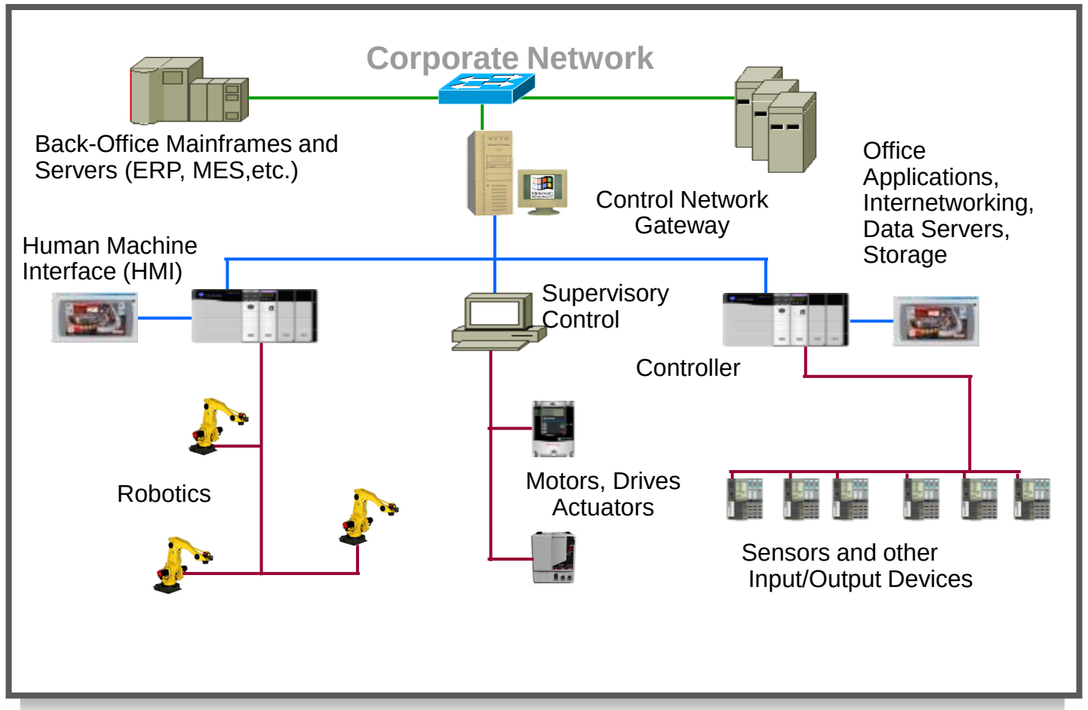
Agenda

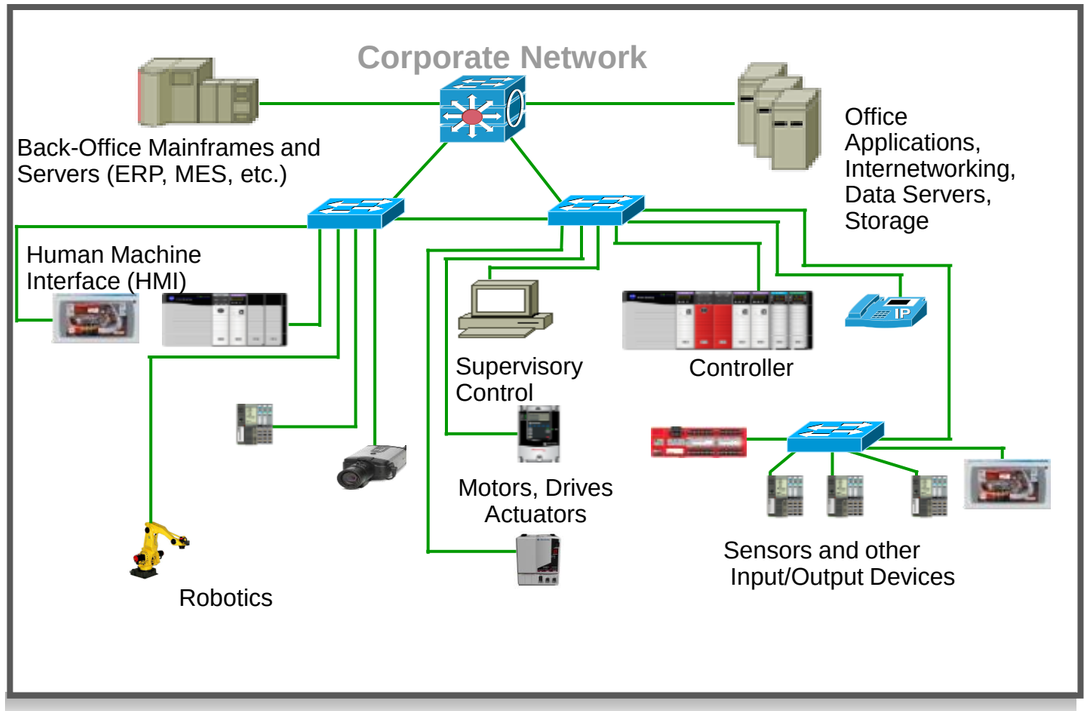
- Industry Trends
- Connected Industry Architectures
  - Applications and Protocols
  - Architectures
  - Solutions and Technologies
- Design Considerations
- Recommended Resources
- Q&A



Industrial Network Convergence

The Journey Towards IP Everywhere

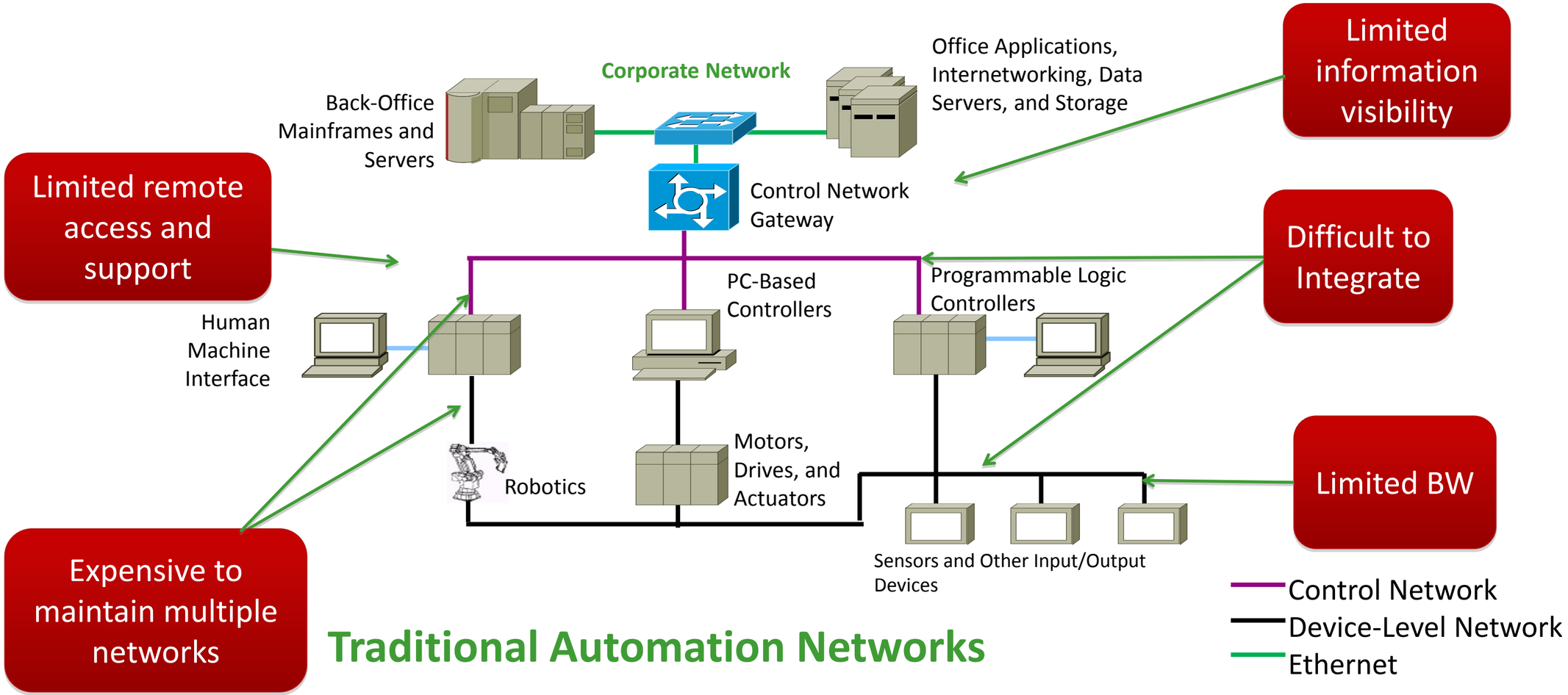




Traditional

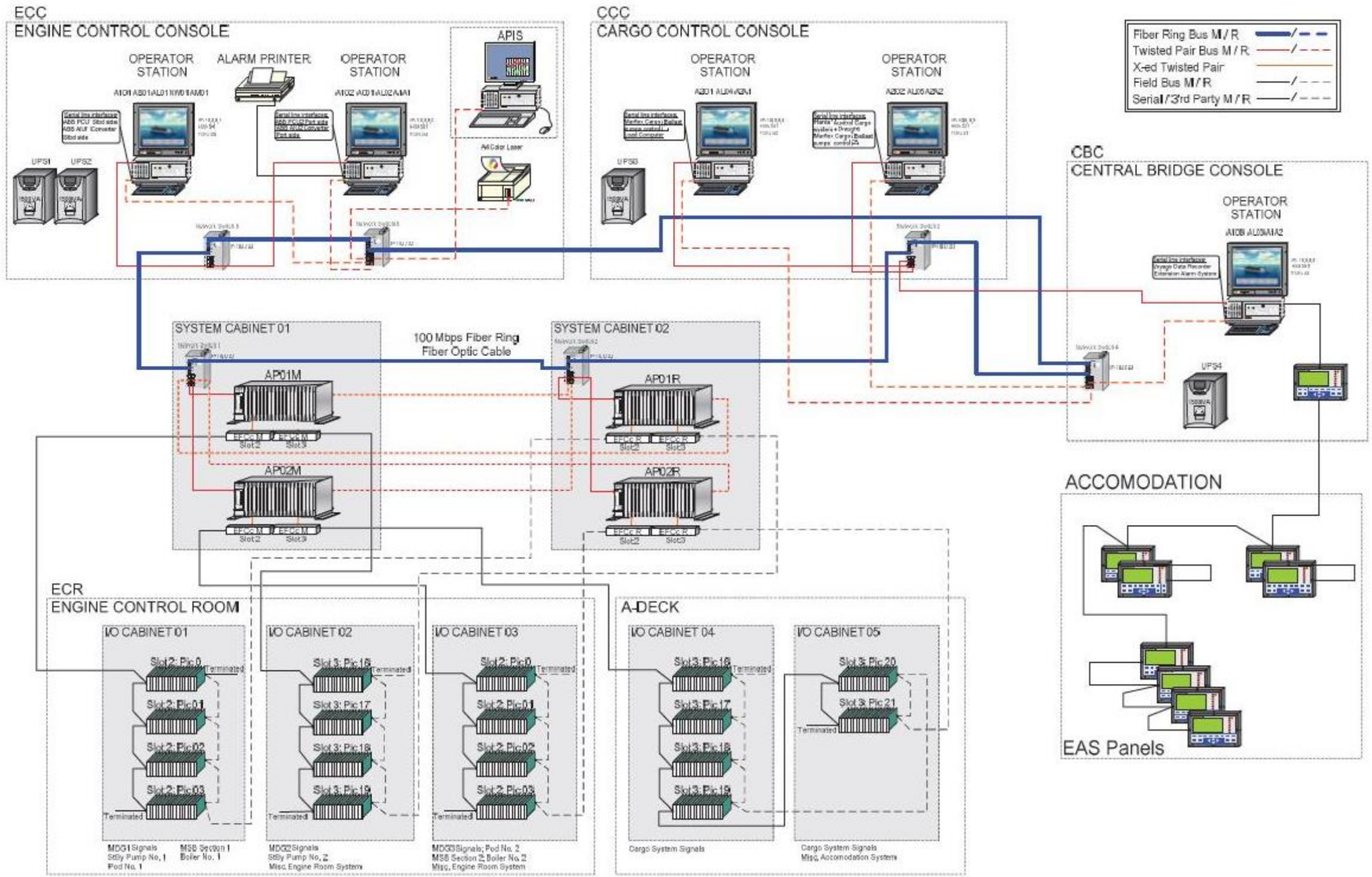
Converged Ethernet

Traditional Industrial Automation Networks



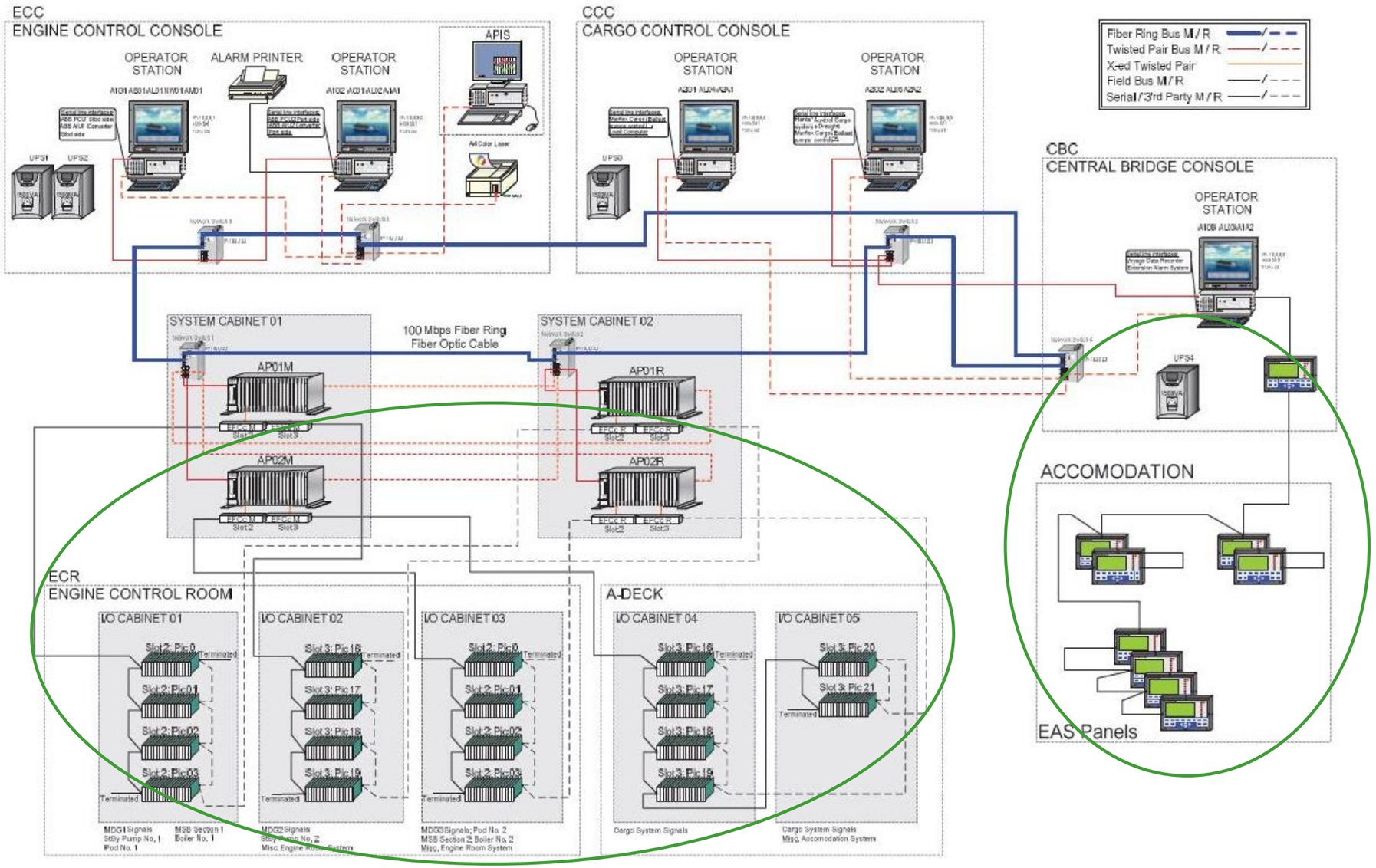
Traditional Automation Network Example

Cargo Ship Control System

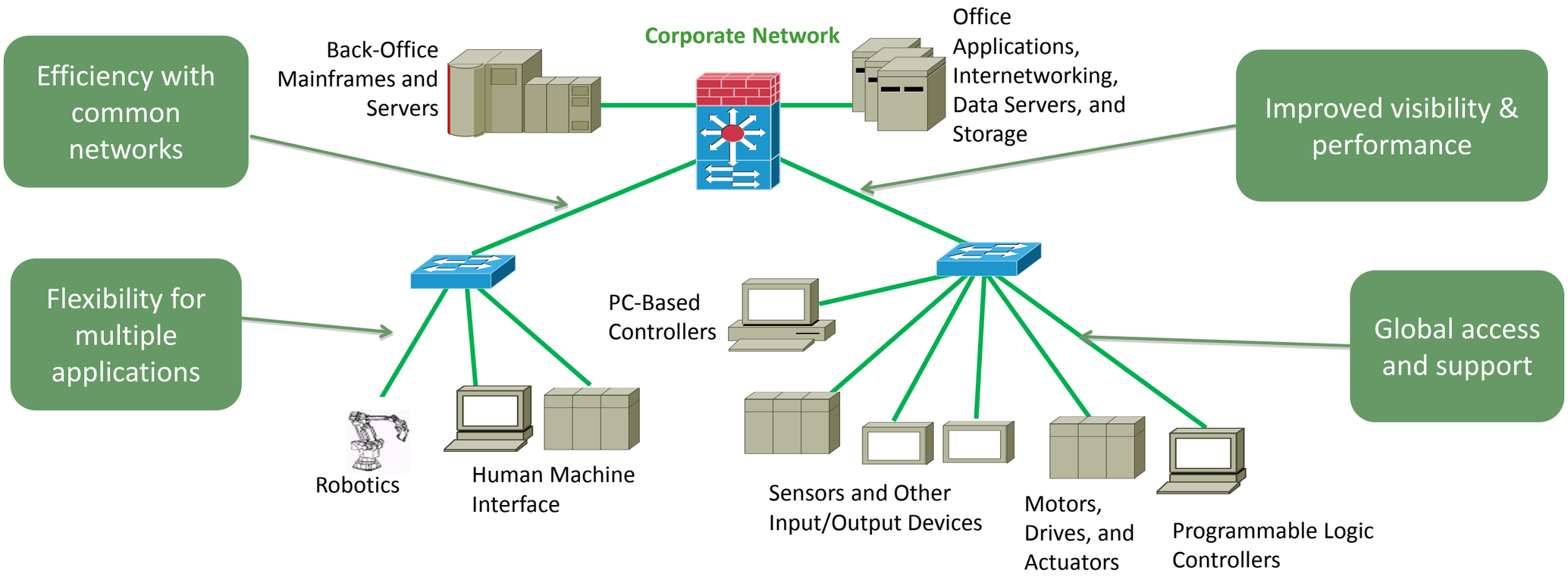


Traditional Automation Network Example

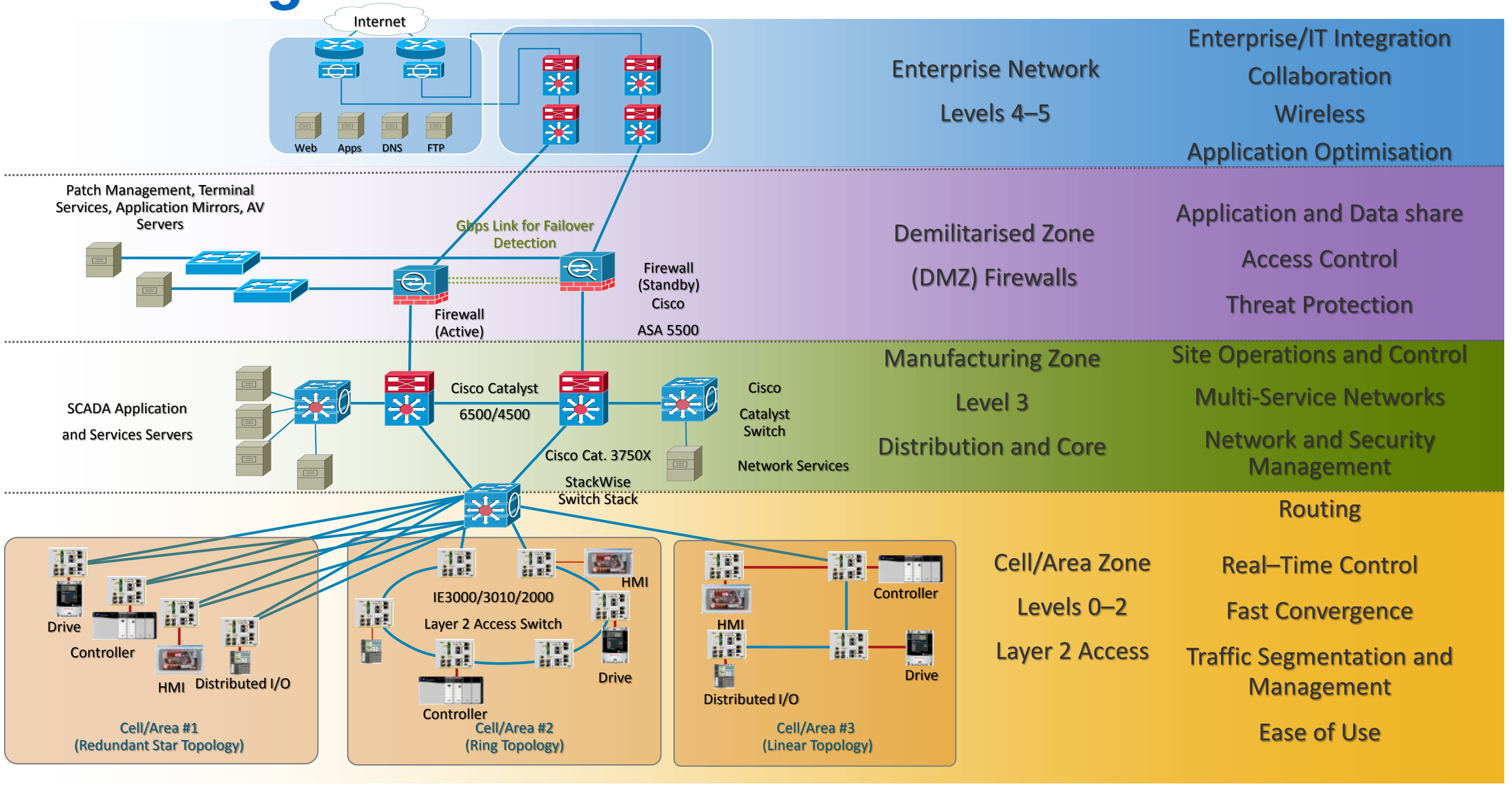
Cargo Ship Control System



Modern Ethernet & IP Based Industrial Automation Networks

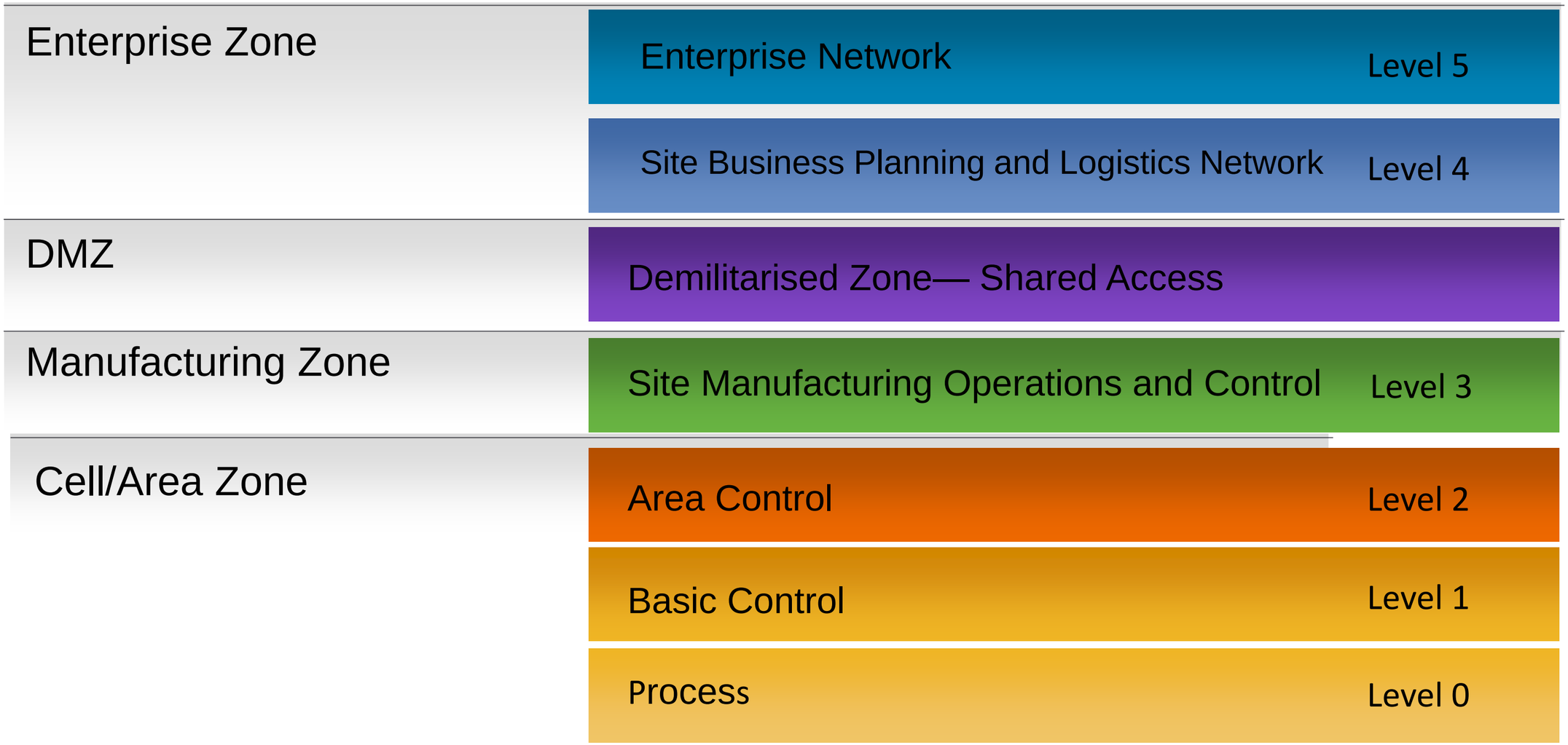


Converged Plant-wide Ethernet Architecture



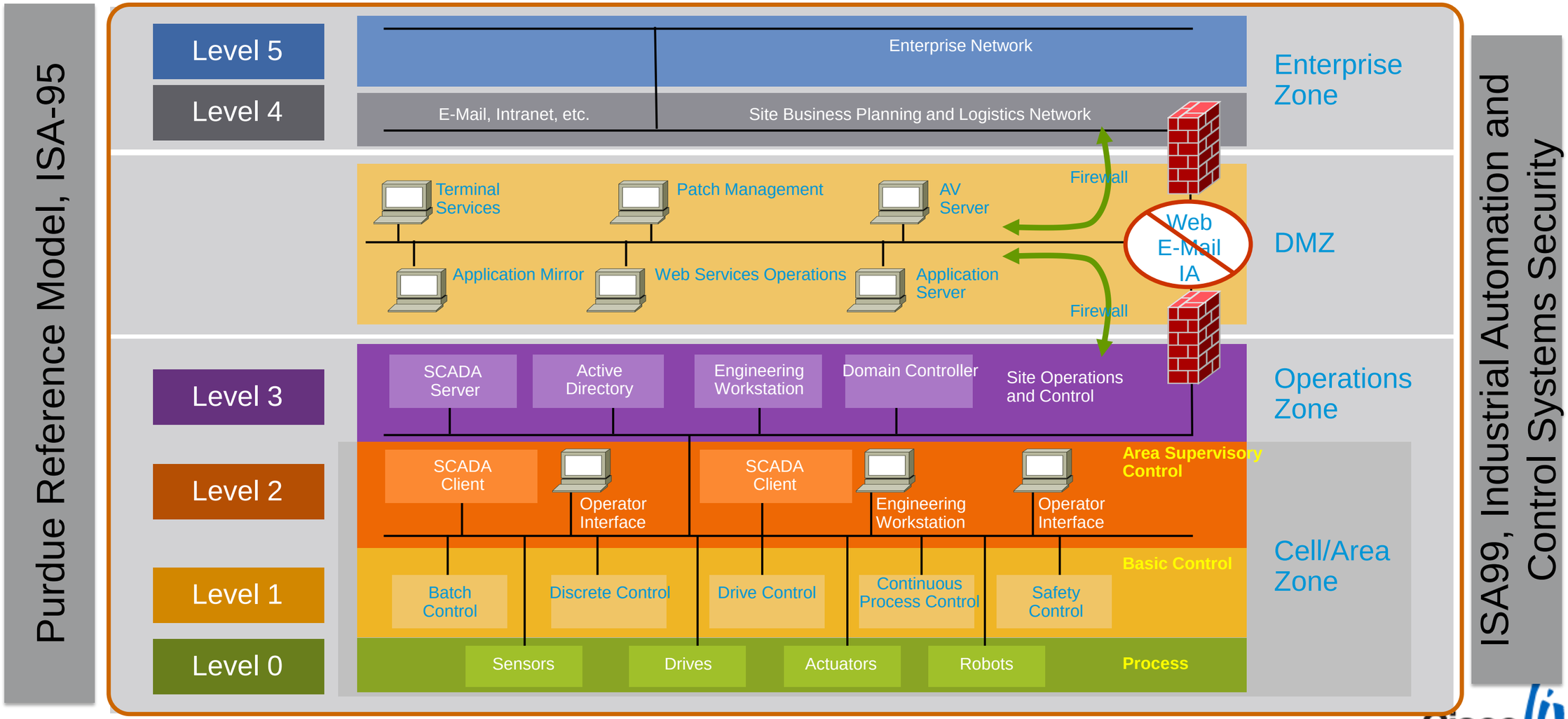
Built on Industry Standards

Purdue Reference Model, ISA95



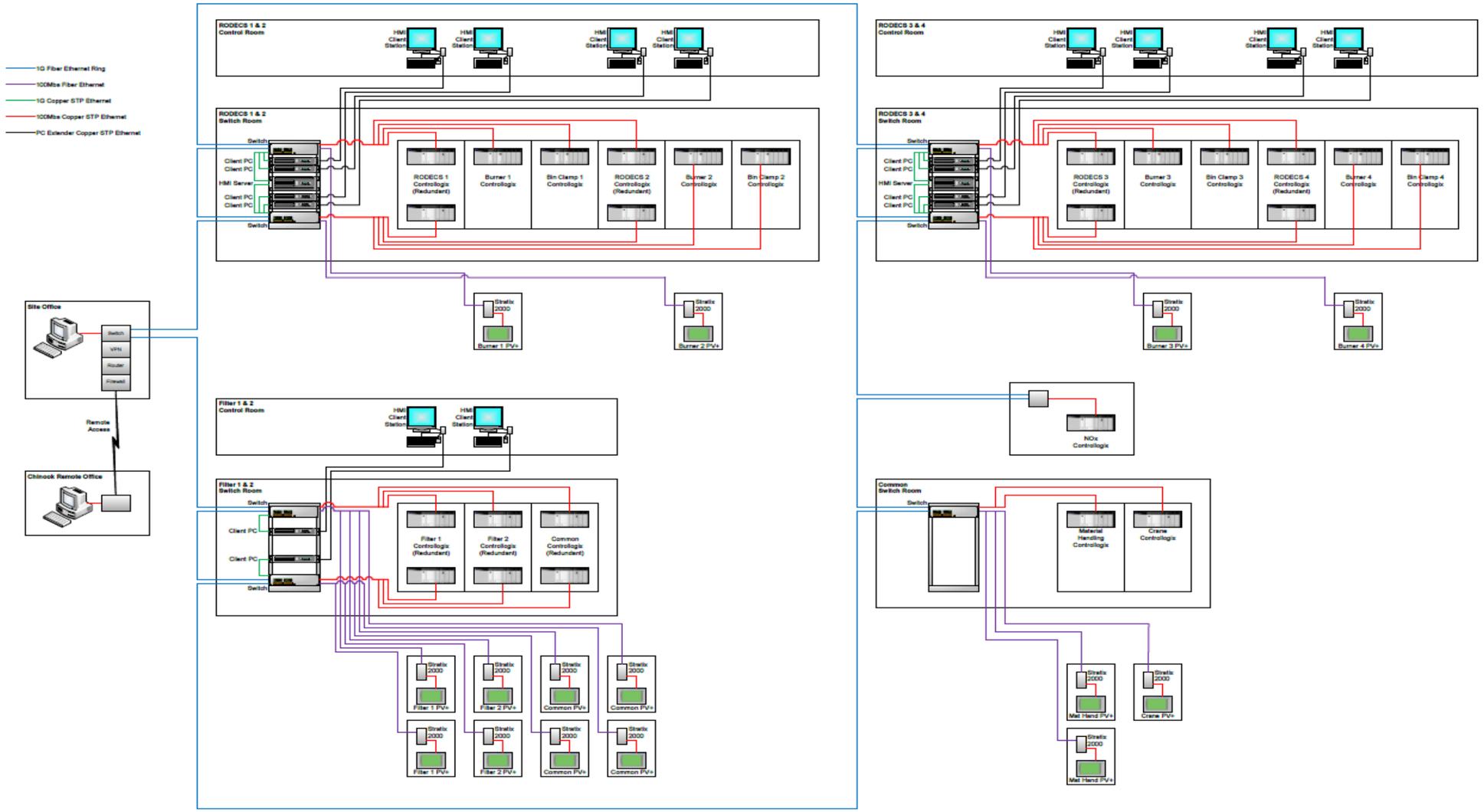
Security Framework, ISA99 aka IEC 62443

Strong Segmentation



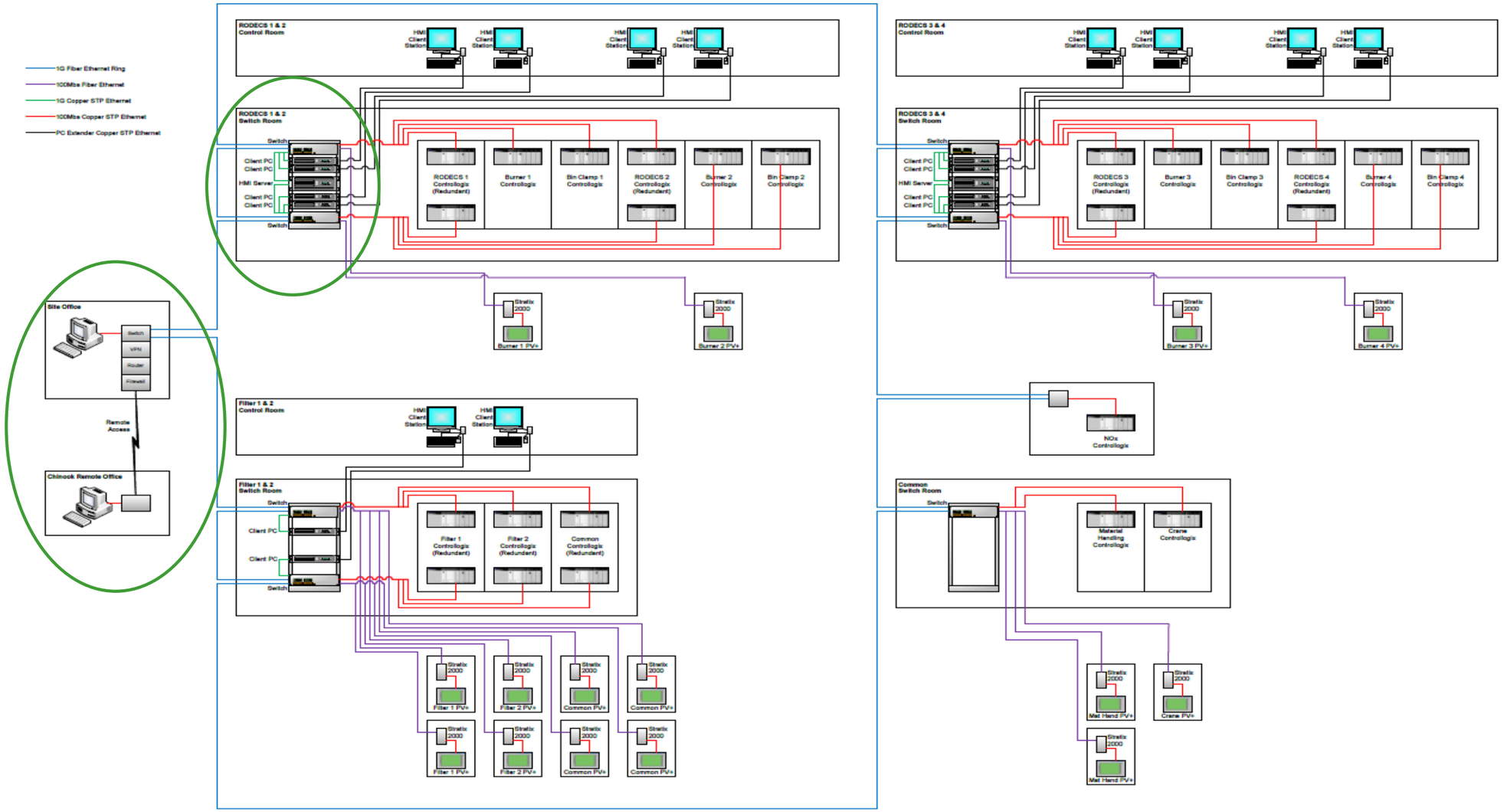
Ethernet and IP Automation Network Example

Material Recycling Plant Control System



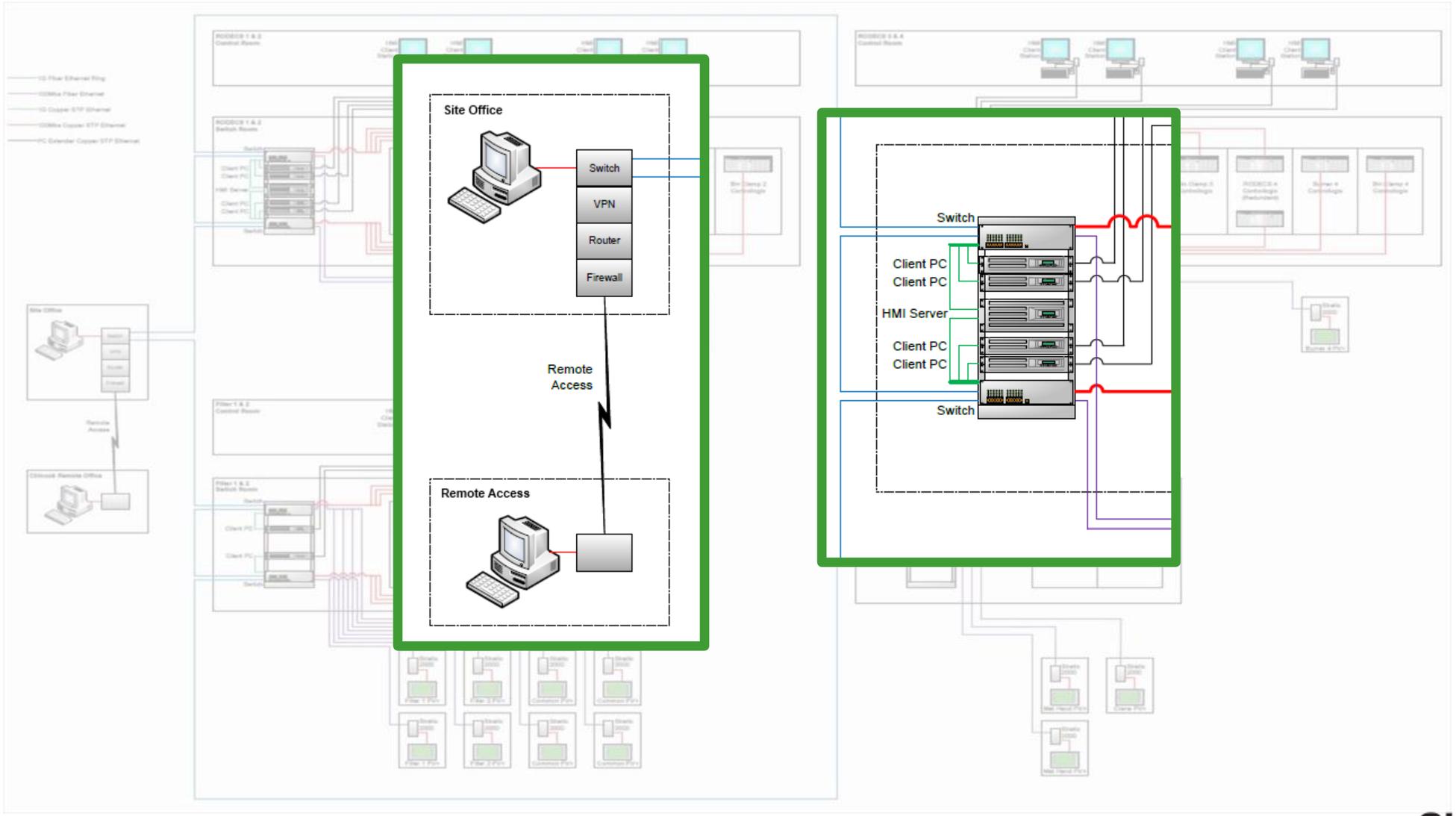
Ethernet and IP Automation Network Example

Material Recycling Plant Control System



Ethernet and IP Automation Network Example

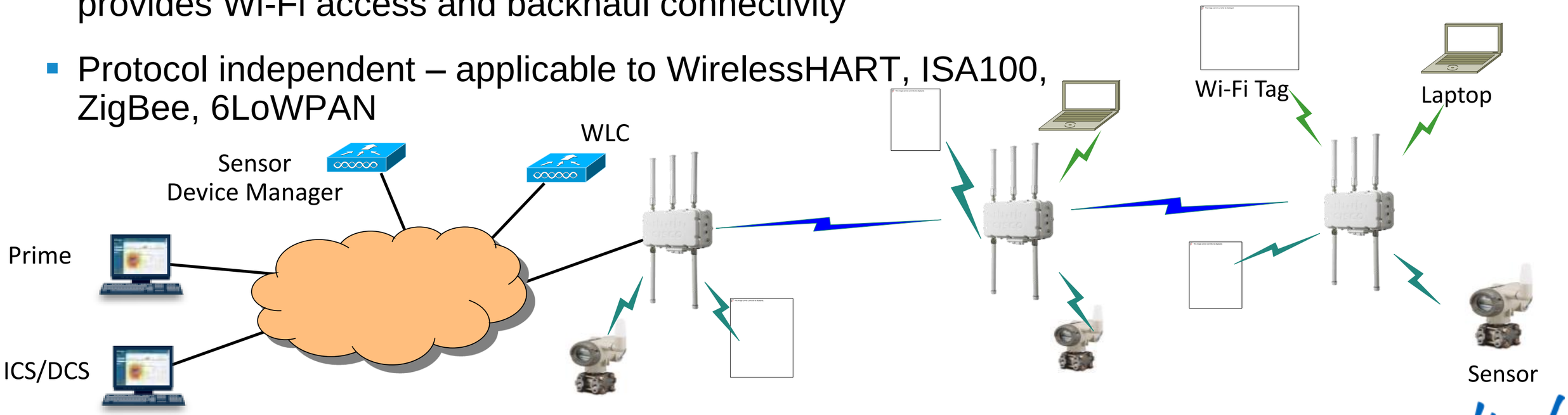
Material Recycling Plant Control System



Industrial Wireless Sensor Networks

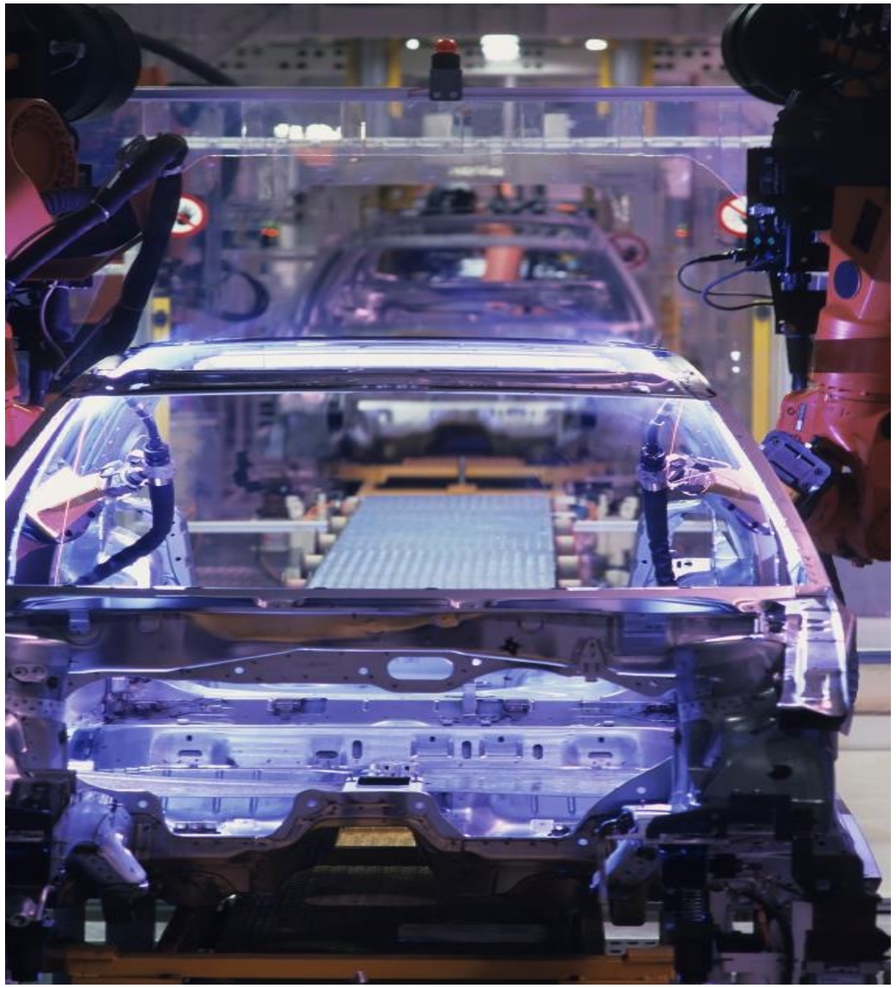
Non-WIFI technologies integrated into 802.11 wireless

- 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



Agenda

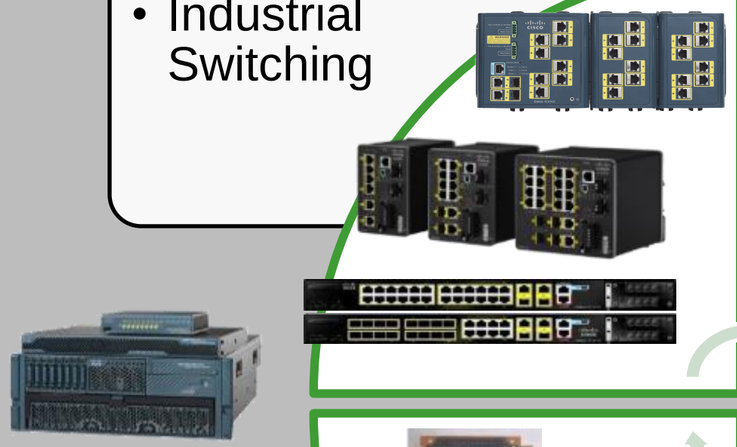
- Industry Trends
- Connected Industry Architectures
  - Applications and Protocols
  - Architectures
  - Solutions and Technologies
- Design Considerations
- Recommended Resources
- Q&A



Cisco Connected Industries Product Portfolio

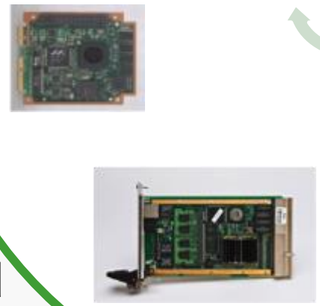
Security

- Industrial Switching



- Industrial Wireless

- 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

Rockwell Automation

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

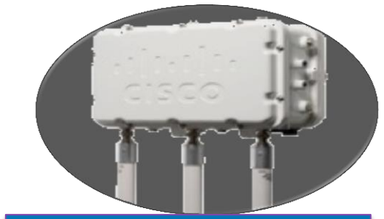
Feature rich
- GPS
- Mobile IP
- IPV6-Ready
- WAAS Express Option
- ScanSafe
- Dual SIM

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

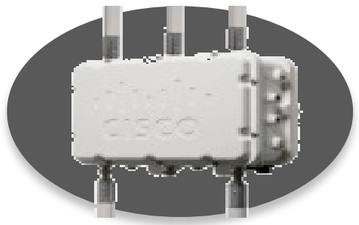
- Extension of 1550 Outdoor AP product line
- Converges industrial wireless access and sensor networks
- 802.11 a/b/g/n Mesh AP's
- Hazardous location qualified (Class 1, Div/Zone 2)
- Ideal for mining, oil and gas, manufacturing, and process control applications



1552H

3 Antennae (2.4/5 GHz)
AC Power

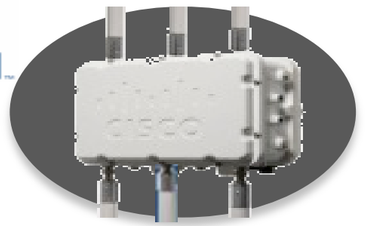
Honeywell



1552S

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

EMERSON

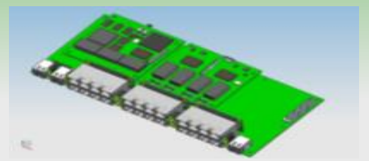


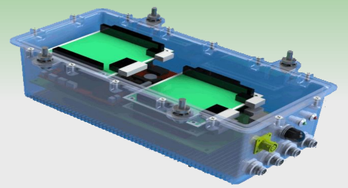
1552WU

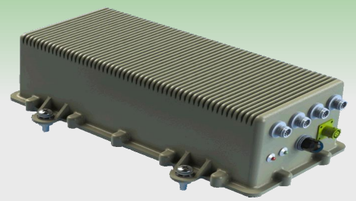
6 Antennae (3x2.4, 3x2.5)
DC Power
WiHART Sensor Gateway

Embedded Industrial Networking Portfolio

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





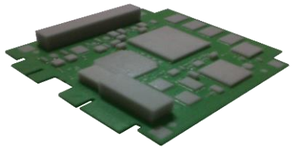


Military

Government Services

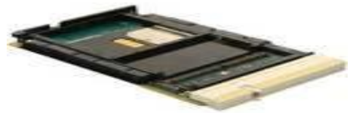
Transportation

Oil and Gas



C5915 ESR

Mid Range Router
PC104 Form Factor



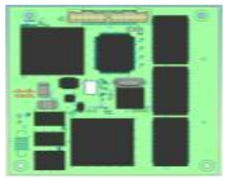
C5940 ESR

High End Router
cPCI Form Factor

IOS

C5921 ESR

IOS Only
Run on your own hardware
Atom/Intel

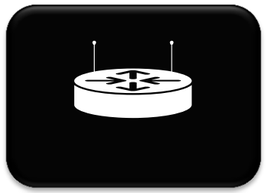


ESS 2020

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



Secure Router

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

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

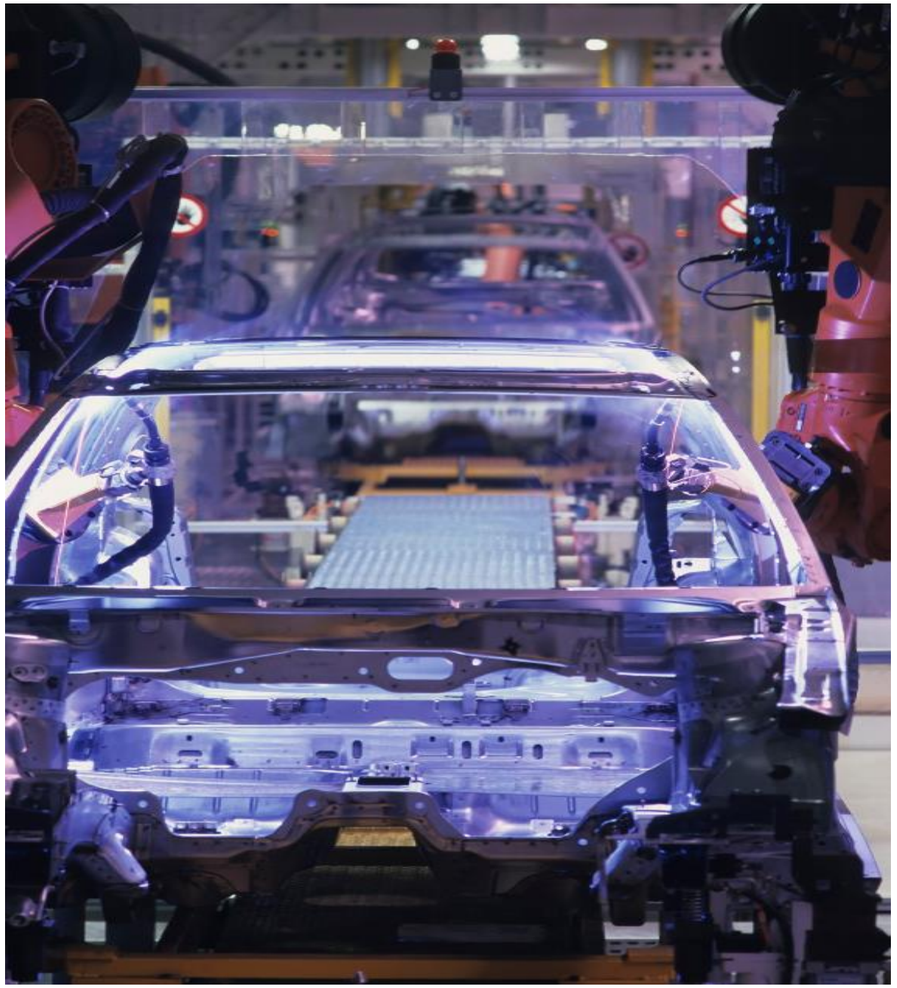
Network Portfolio for an End-to-End Industrial Architecture

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
- Recommended Resources
- Q&A

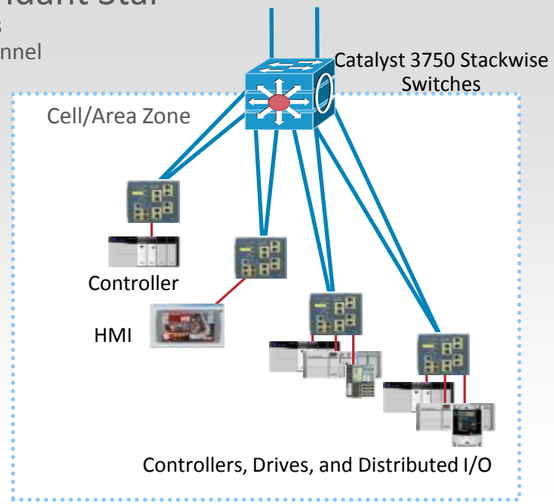


Industrial Network Topologies

Cell/Area Zone Topology Options

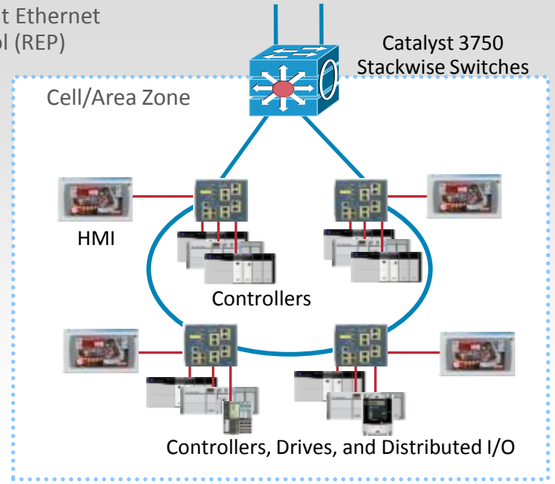
Redundant Star

Flex Links
EtherChannel

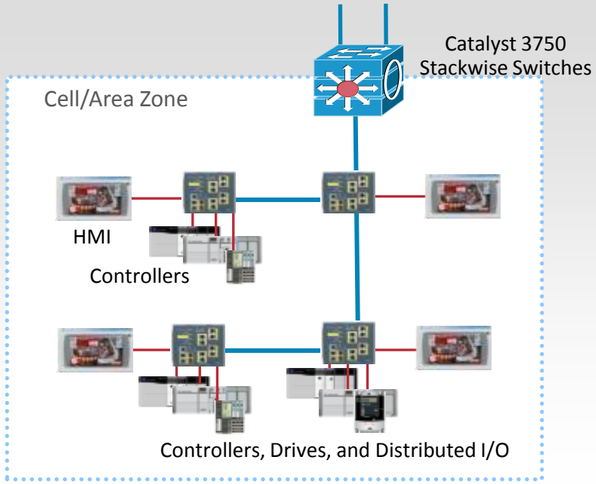


Ring

Resilient Ethernet Protocol (REP)



Star/Bus Linear

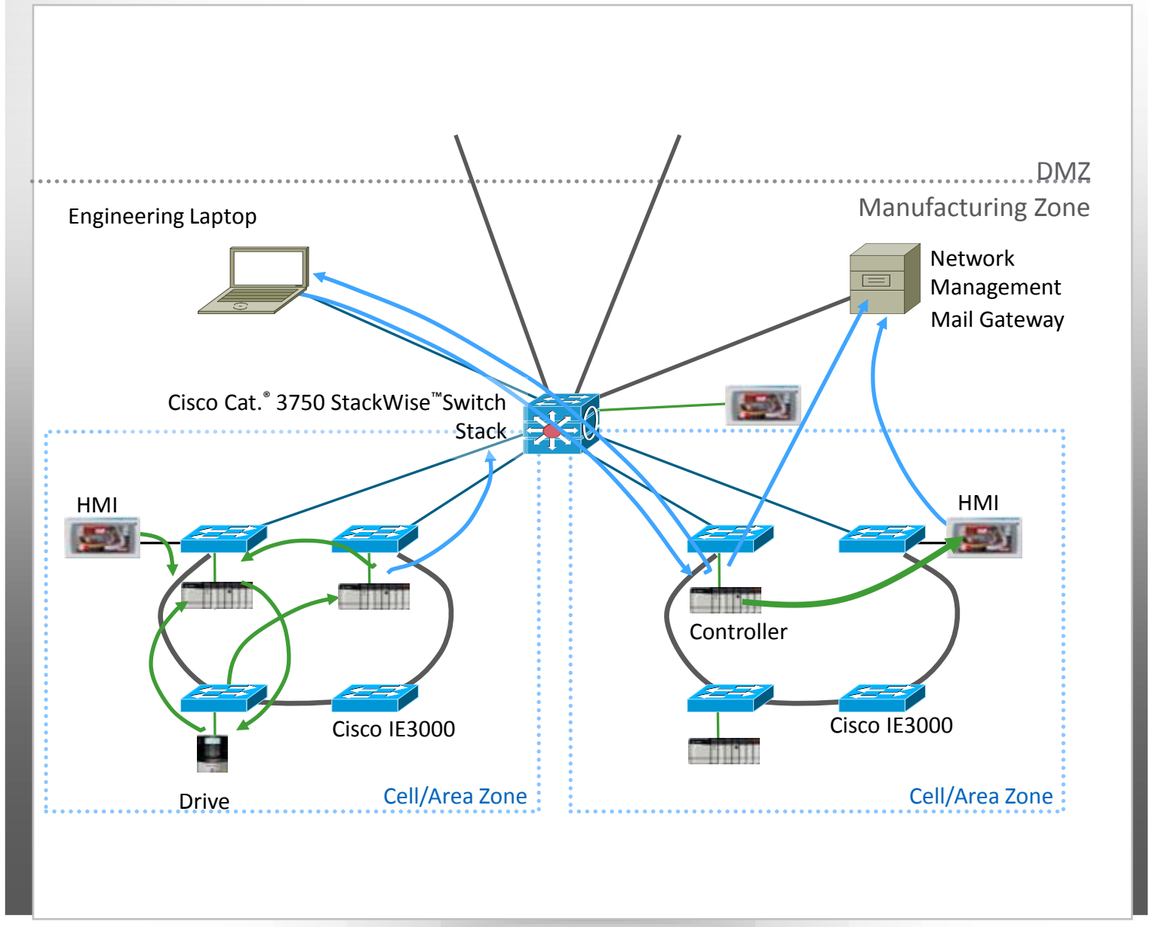


	Redundant Star	Ring	Linear
Cabling Requirements			
East of Configuration			
Implementation Costs			
Bandwidth			
Redundancy and Convergence			
Disruption During Network Upgrade			
Readiness for Network Convergence			
Overall in Network TCO and Performance	Best	OK	Worst

Typical Cell/Zone 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)

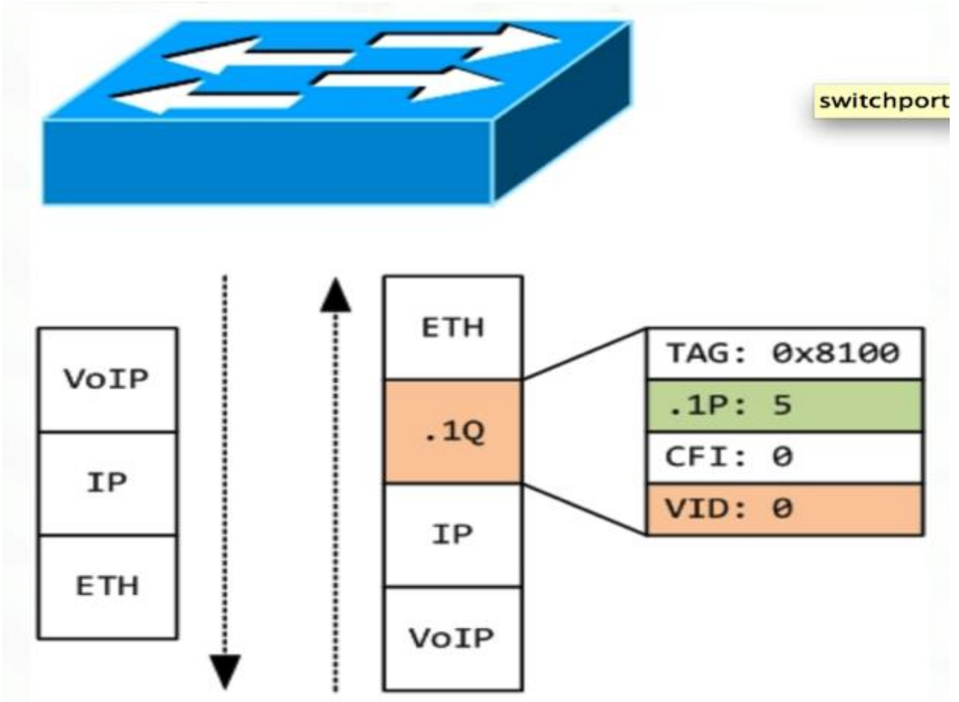
- The rest is informational control and administration (or Explicit) traffic flows intra- and inter-cell/area
  - Non-critical administrative or data traffic
  - Diagnostic information via HTTP/S
  - Status and fault warnings via SNMP or SMTP
  - Packets are larger, ~500 bytes but infrequent (100s of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



Profinet Considerations

Default behaviour on Cisco Switches

- Profinet is L2 and un-routable. Requires large flat L2 networks ☹
- Profinet uses 802.1p to prioritise frames
- Inserts an 802.1Q tag with:
  - VLAN ID = 0
  - PCP (COS) = 5
- Depending on switch ASIC, VLAN0 handled differently:
  - Legacy 2950/3550 – Accepted on access port
  - 2960/3560/3750 – Dropped on access port
  - On IE2000/IE3000/IE3010 – Dropped – UNLESS!
    - Enable “profinet vlan <xxx>” command



Profinet Considerations

Example configuration

- On 2960/3560/3750 Switches

If the PLC or IO Device Is An Access Device

```
interface GigabitEthernet1/0/1
 switchport mode access
 switchport access vlan yyy
 switchport voice vlan xxx
 spanning-tree portfast
```

- On IE2000/IE3000/IE3010 Switch

Profinet Considerations

Example configuration

- On 2960/3560/3750 Switches

If the PLC or IO Device Is An Access Device

```
interface GigabitEthernet1/0/1
 switchport mode access
 switchport access vlan yyy
 switchport voice vlan xxx
 spanning-tree portfast
```

- On IE2000/IE3000/IE3010 Switch

If the PLC or IO Device Is An Access Device

```
profinet vlan xxx

interface GigabitEthernet1/0/1
 switchport access vlan xxx
 switchport mode access
 spanning-tree portfast
```

Profinet Considerations

Example configuration

- On 2960/3560/3750 Switches

If the PLC or IO Device Is An Access Device

```
interface GigabitEthernet1/0/1
 switchport mode access
 switchport access vlan yyy
 switchport voice vlan xxx
 spanning-tree portfast
```

If the PLC or IO Device Is Configured as A Trunk

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan xxx
 switchport mode trunk
 spanning-tree portfast trunk
```

- On IE2000/IE3000/IE3010 Switch

If the PLC or IO Device Is An Access Device

```
profinet vlan xxx

interface GigabitEthernet1/0/1
 switchport access vlan xxx
 switchport mode access
 spanning-tree portfast
```

Profinet Considerations

Example configuration

- On 2960/3560/3750 Switches

If the PLC or IO Device Is An Access Device

```
interface GigabitEthernet1/0/1
 switchport mode access
 switchport access vlan yyy
 switchport voice vlan xxx
 spanning-tree portfast
```

If the PLC or IO Device Is Configured as A Trunk

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan xxx
 switchport mode trunk
 spanning-tree portfast trunk
```

- On IE2000/IE3000/IE3010 Switch

If the PLC or IO Device Is An Access Device

```
profinet vlan xxx

interface GigabitEthernet1/0/1
 switchport access vlan xxx
 switchport mode access
 spanning-tree portfast
```

If the PLC or IO Device Is Configured as A Trunk

```
profinet vlan xxx

interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan xxx
 switchport mode trunk
 spanning-tree portfast trunk
```

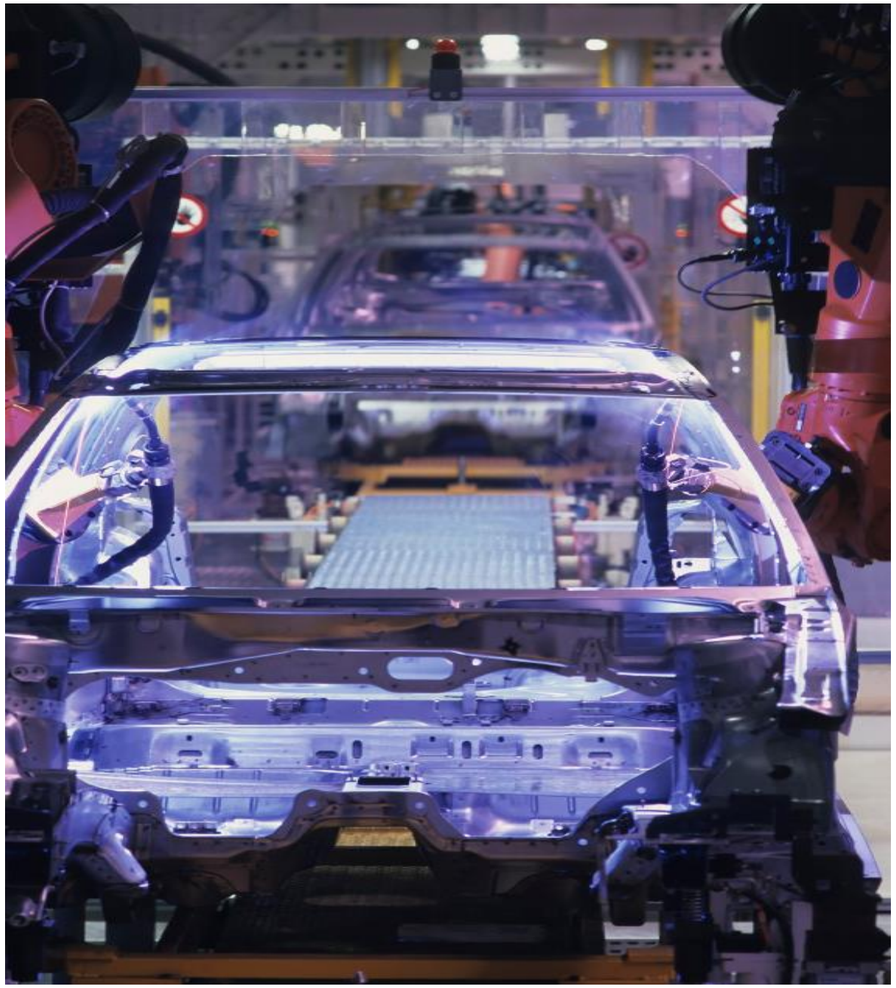
Profinet Considerations

Check Status on IE Switches

```
Switch(config)#profinet vlan 101

Switch# sh profinet status
State       : Enabled
Vlan        : 101
Id          : IE2000-4T-G
Connected   : Yes
ReductRatio : 128
GSD version : Match
```

Agenda

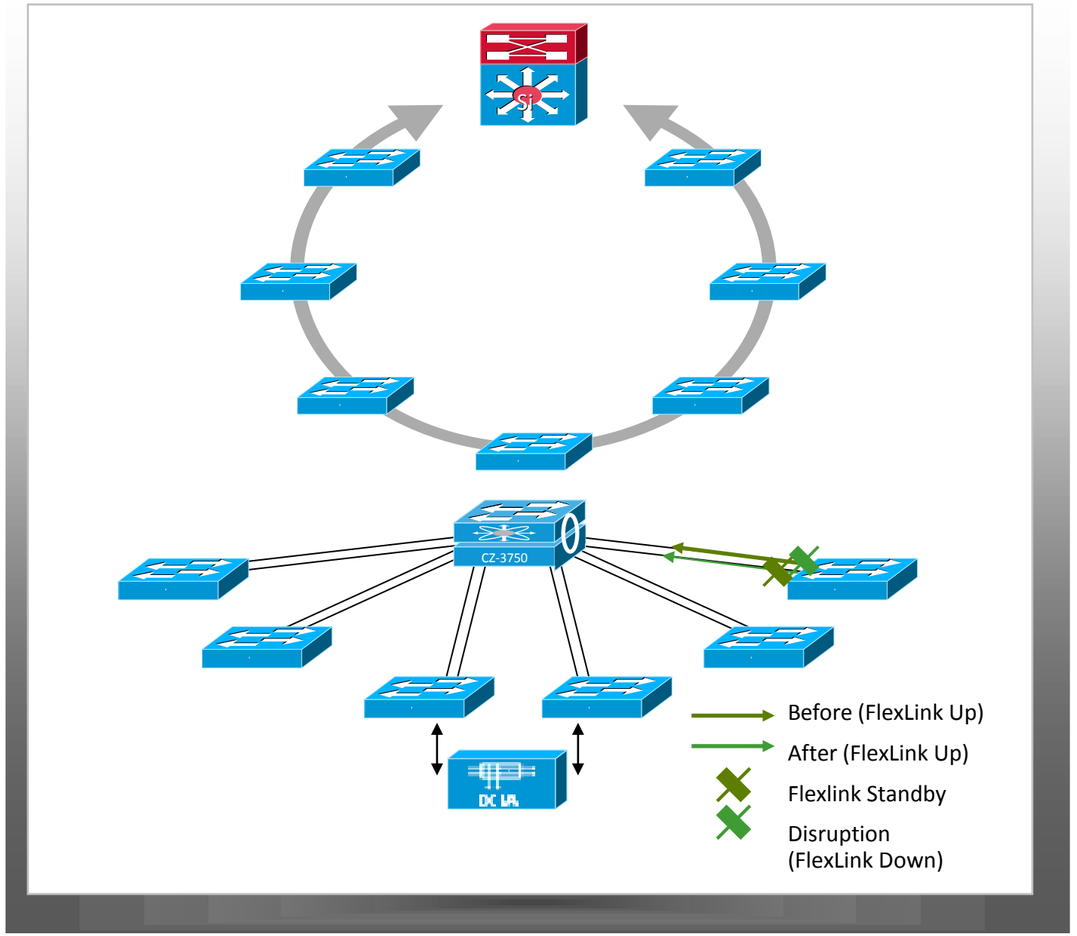
- Industry Trends
- Connected Industry Architectures
- Design Considerations
  - Traffic Flows and Topologies
  - Availability and Resilience
  - Segregation and VLANs
  - QoS
  - Security
- Recommended Resources
- Q&A



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 common ICS/DCS applications and multicast traffic
- Fast convergence avoids application reset and improves uptime
- Critical for industrial applications



Performance Requirements

Industrial Automation & Control Applications

	Process Automation	Discrete Automation	Motion Control
			
Function	Information Integration, Slower Process Automation	Time-critical Factory Automation	Multi-axis Motion Control
Comm. Technology	.Net, DCOM, TCP/IP	Industrial Protocols, CIP, Profinet	Hardware and Software solutions, e.g. CIP Motion, IRT
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 Discrete automation
Applications	Pumps, compressors, mixers; monitoring of temperature, pressure, flow	Material handling, filling, labeling, palletising, packaging; welding, stamping, cutting, metal forming, soldering, sorting	Synchronisation of multiple axes: printing presses, wire drawing, web making, picking and placing

Source: ARC Advisory Group

Network Resiliency Protocols

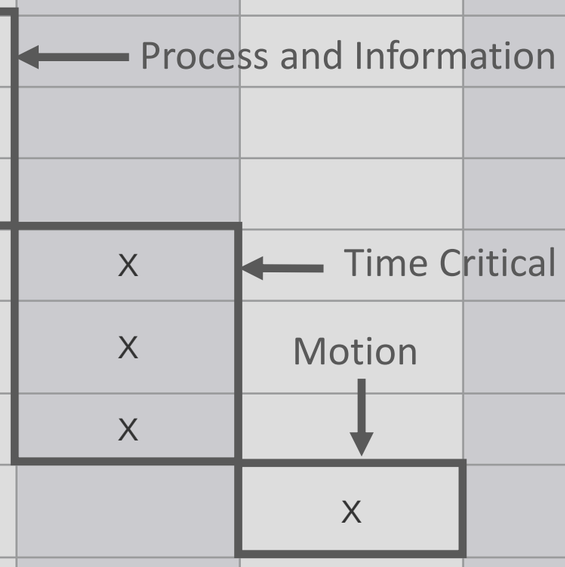
Selection Is Application Driven

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	

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	



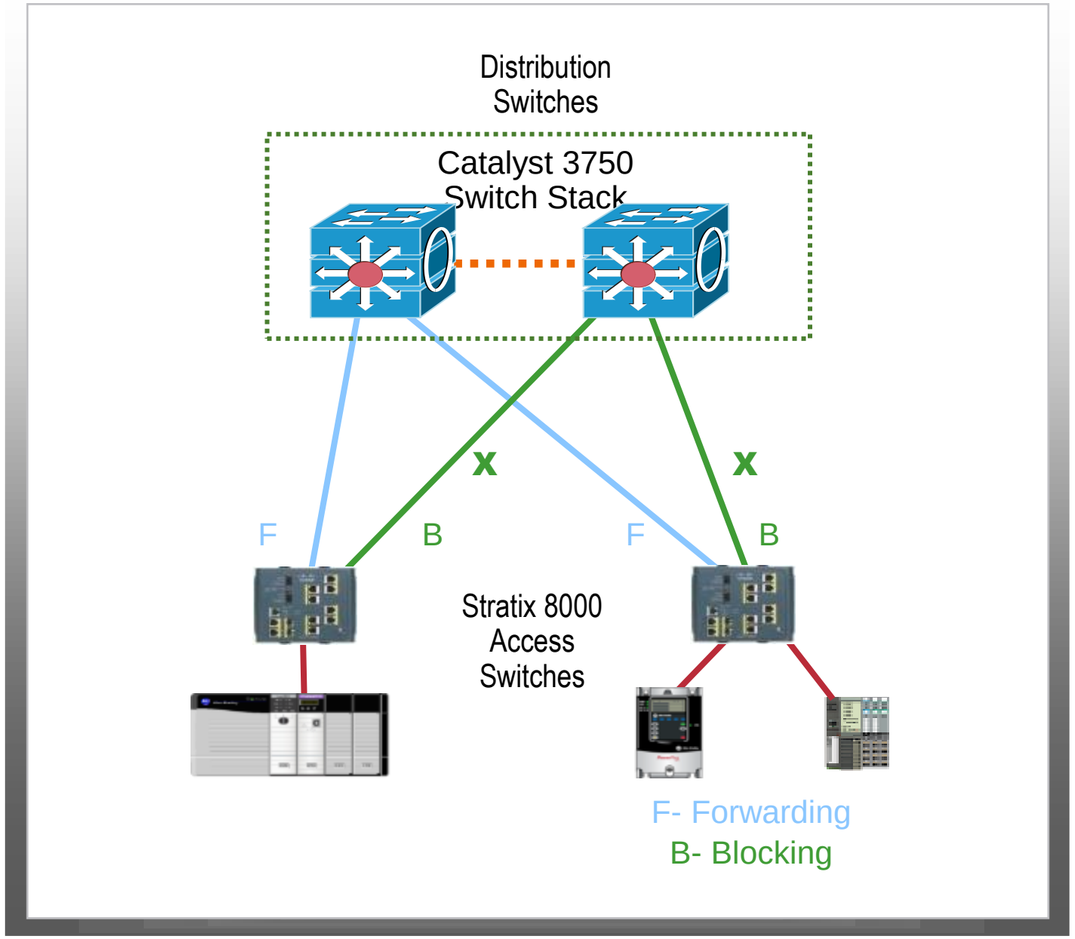
L2 Industrial Network Redundancy Protocols

Resiliency Protocol	Ring Topology (Switch or Device Level)	Redundant Star or Mesh Topology	Typical Network Convergence Time	Max Number of Switch Nodes	Remark
Standardised					
STP (802.1D)	S	X	30s	7	Limited network diameter
RSTP (802.1w)	S	X	2s	7	Superseded by 802.1D-2004
MRP (IEC 62439-2)	D		10-500ms	50	Recovery increases with number of nodes
MSTP (802.1s)	S	X	250ms	255	Number of VLANs and node increases convergence time significantly
RSTP (802.1D-2004)	S	X	50-200ms	255	Recommend limit of 40 nodes. Needs optimising for rapid convergence
EtherChannel (LACP 802.3ad)		X	100ms	2	Switch to switch redundancy only
G.8032v2 (ITU-T)	S	X	50ms	255	Recommend limit of 16 nodes
DLR (IEC & ODVA)	D		3ms	50	Worst case 3ms for 50 nodes
HSR (IEC 62439-3.5 2012)	D	X	10ms per hop		HSR is a device ring, requires FPGA
PRP-1 (IEC 62439-3.4 2012)	D	N/A	0ms	N/A	PRP requires duplicate L2 networks, no special hardware
Proprietary					
S-Ring (GarettCom)	S		200ms-700ms	Unlimited	No upper limit to number of nodes but recommend 50
HiperRing (Hirschmann)	S		200-500ms	Unlimited	Recovery depends on number of nodes
TurboRing (Moxa)	S		200-300ms	Unlimited	Recover depends on number of nodes
FlexLinks (Cisco)		X	100ms	2	Switch to switch redundancy only
REP (Cisco)	S		50ms	Unlimited	Recovery tested up to 130 nodes
eRSTP (RuggedCom)	S	X	5ms per hop	80	Recover depends on number of nodes
StackWise (Cisco)	S	X	5ms	9	Offers L2 and L3 redundancy

Spanning Tree Protocol (STP)

Often required for interoperability

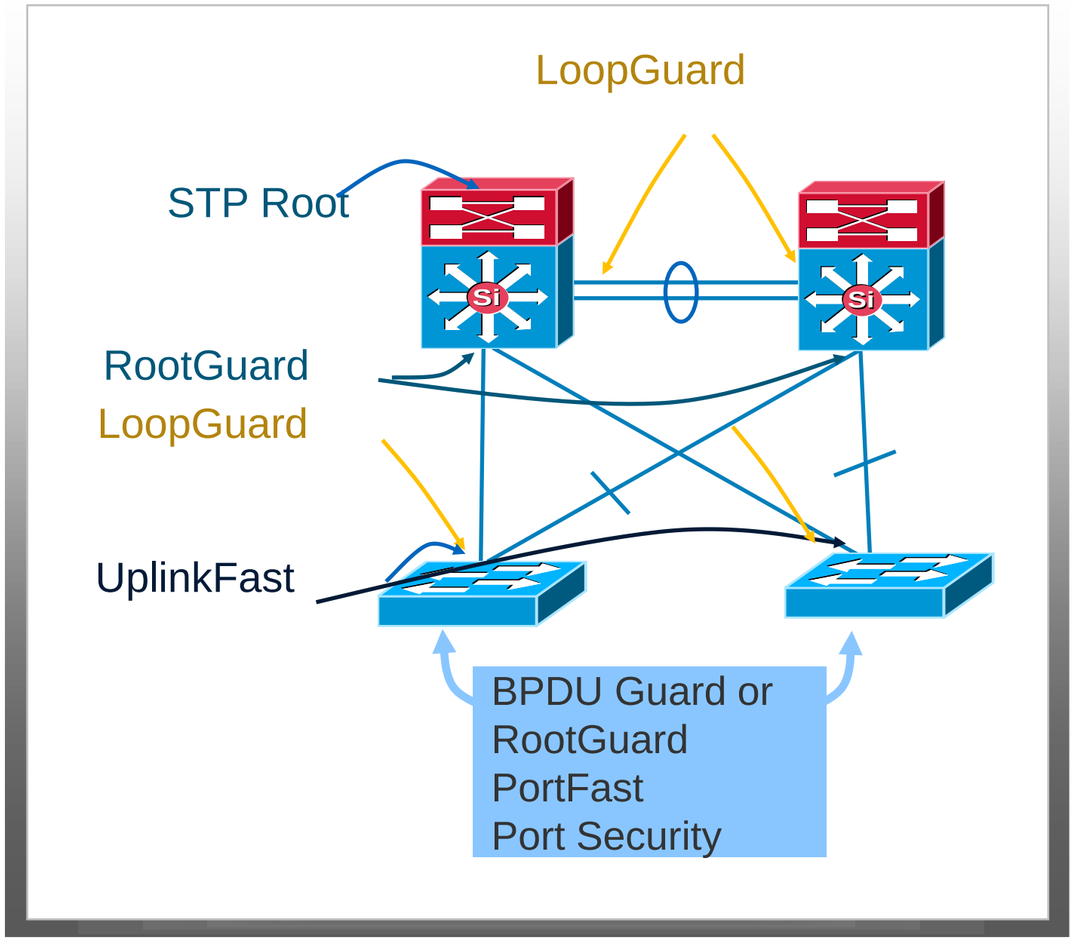
- Most common standard protocol for network resiliency—IEEE 802.1D
- Supports Redundant Star and Ring Topology
- Provides alternate path in case of failures, avoiding loops
- Unmanaged switches don’t support STP
- Versions: STP, RSTP, MSTP and RPVST+ :there are differences
- Coordinate with IT before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



Layer 2 Hardening

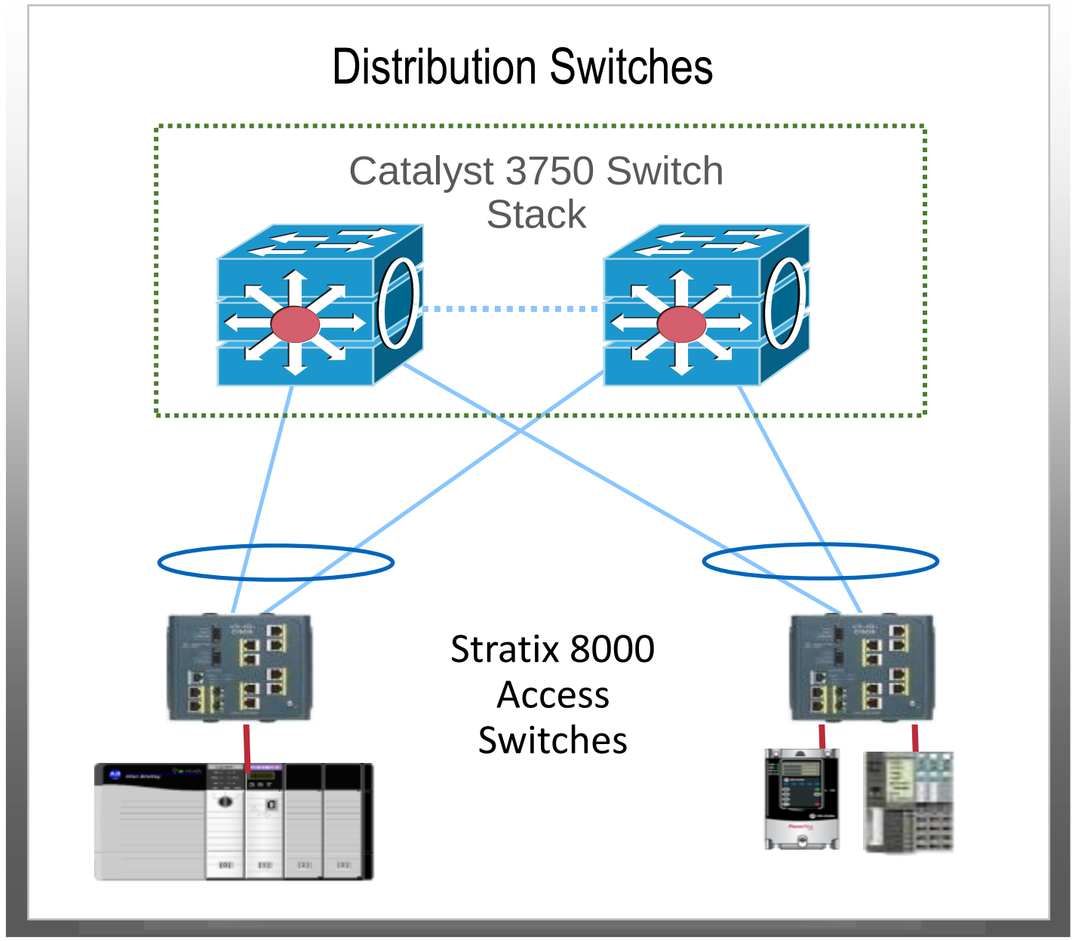
Spanning Tree Should Behave the Way You Expect

- 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



Configuring EtherChannels

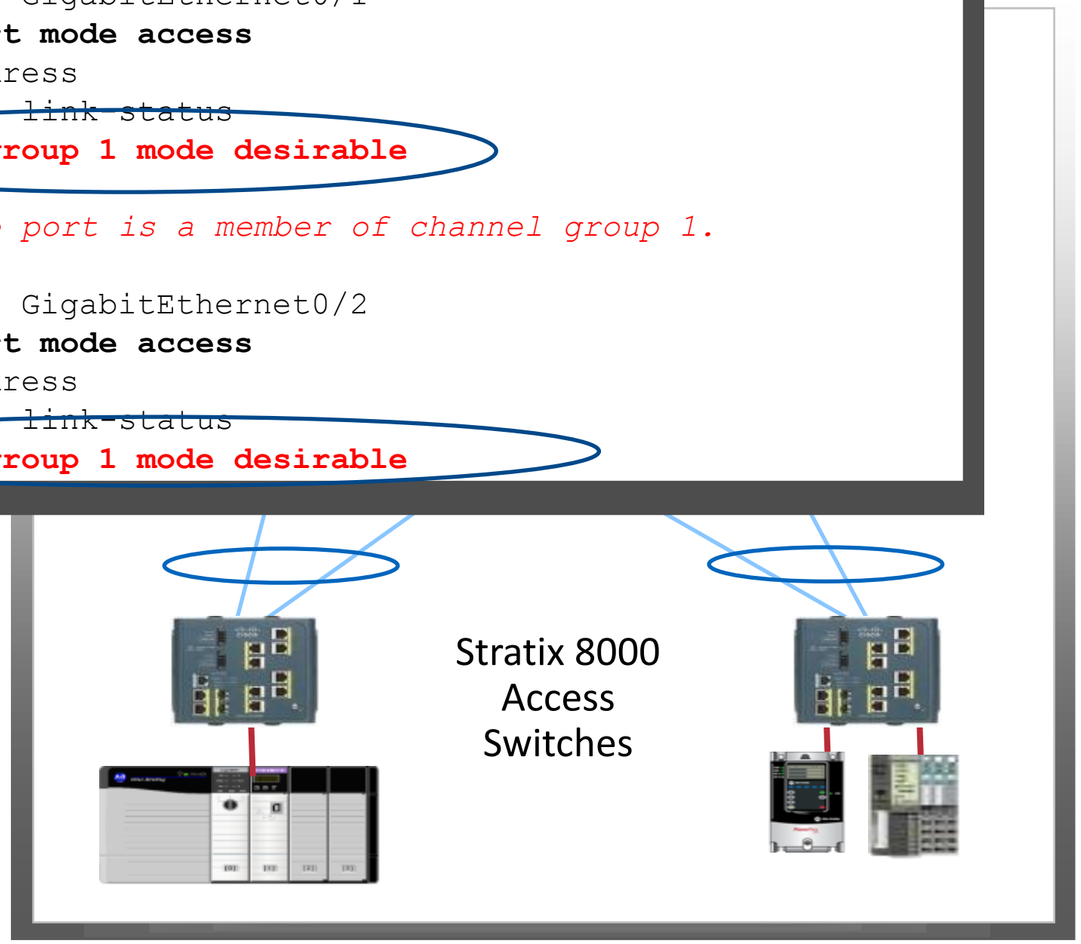
- Link Aggregation Control Protocol (LACP) port aggregation—IEEE 802.3ad
- Redundant Star Topology
- A way of combining several physical links between switches into one logical connection to aggregate bandwidth (2 to 8 ports)
- Provides resiliency between connected switches if a connection is broken



Configuring EtherChannels

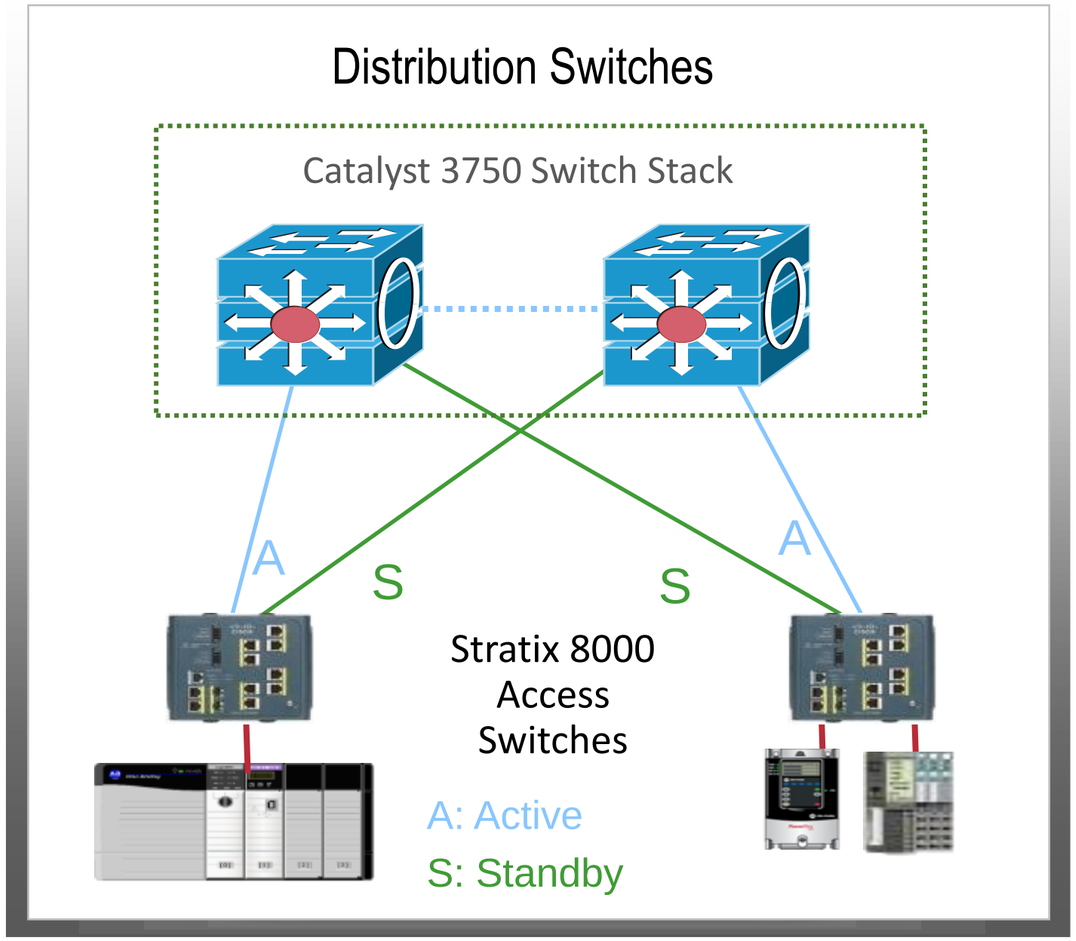
- Link Aggregation Control Protocol (LACP) aggregation—IEEE 802.3ad
- Redundant Star Topology
- A way of combining several physical links switches into one logical connection to ag bandwidth (2 to 8 ports)
- Provides resiliency between connected switches if a connection is broken

```
!--- 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 technology
- Redundant Star topology
- Active/Standby port scheme
- Sub 100ms recovery times
- Provides alternate path in case of failures, avoiding loops
- Unmanaged switches don’t support this concept



Configuring Flex Links

- Cisco technolo
- Redundant Sta
- Active/Standby
- Sub 100ms rec
- Provides alterr
  avoiding loops
- Unmanaged sv
  concept

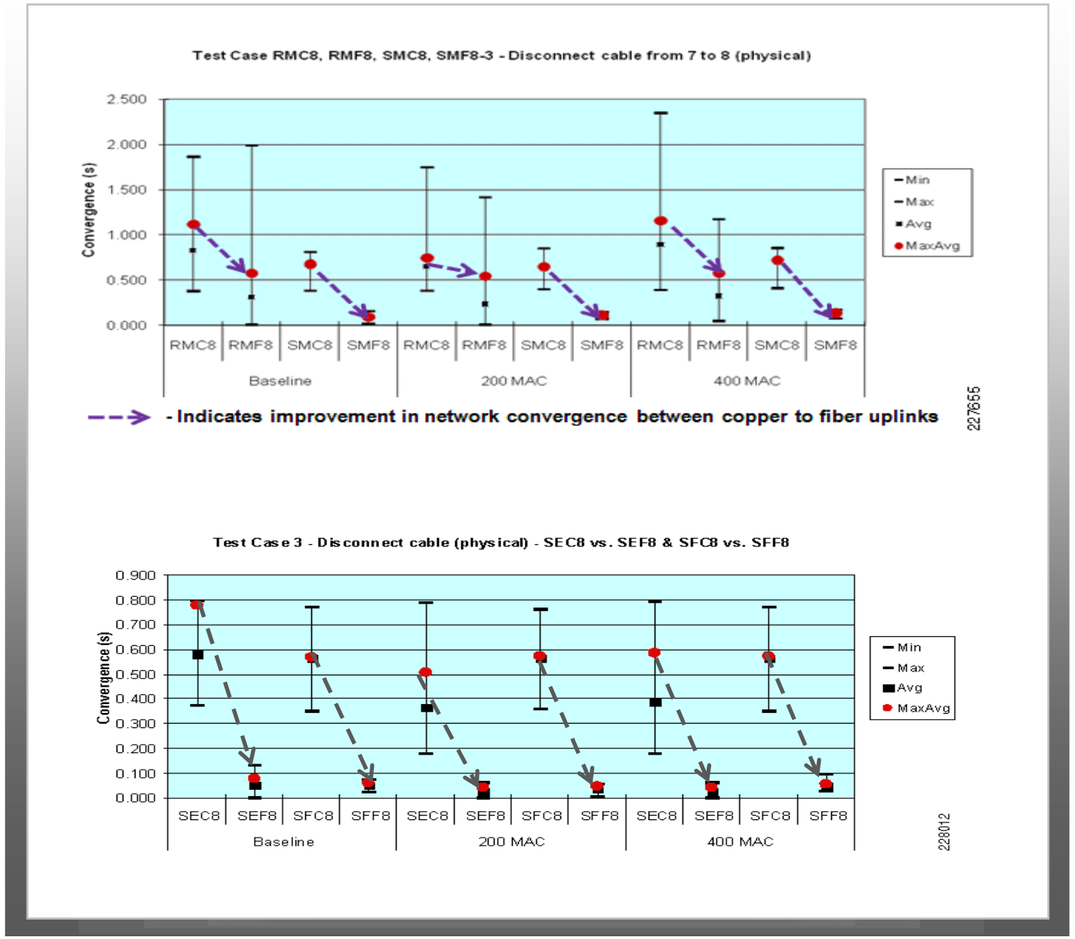
```
Switch# configure terminal
Switch(conf)# interface fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2
Switch(conf-if)# end
Switch# show interface switchport backup

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

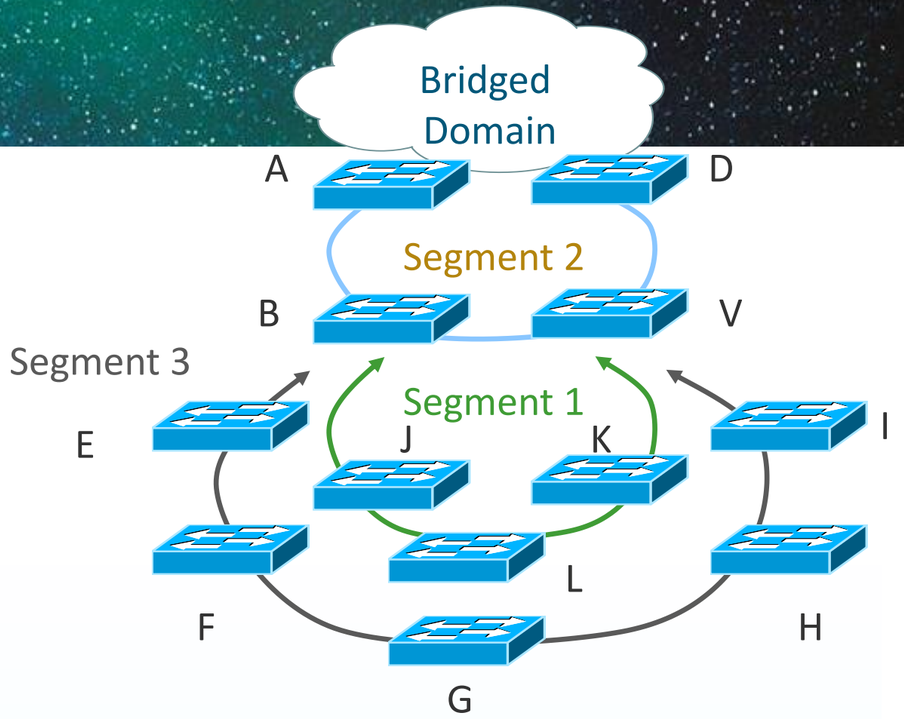
- Compare test with same topologies with fibre vs. copper uplinks
  - Multimode LC fibre cables
  - Cat 5e and Cat 6 copper cables
- All fibre topologies converged faster than copper topologies, approx. 500ms faster
- Ethernet standards allow for higher range of link-down notification for copper-based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

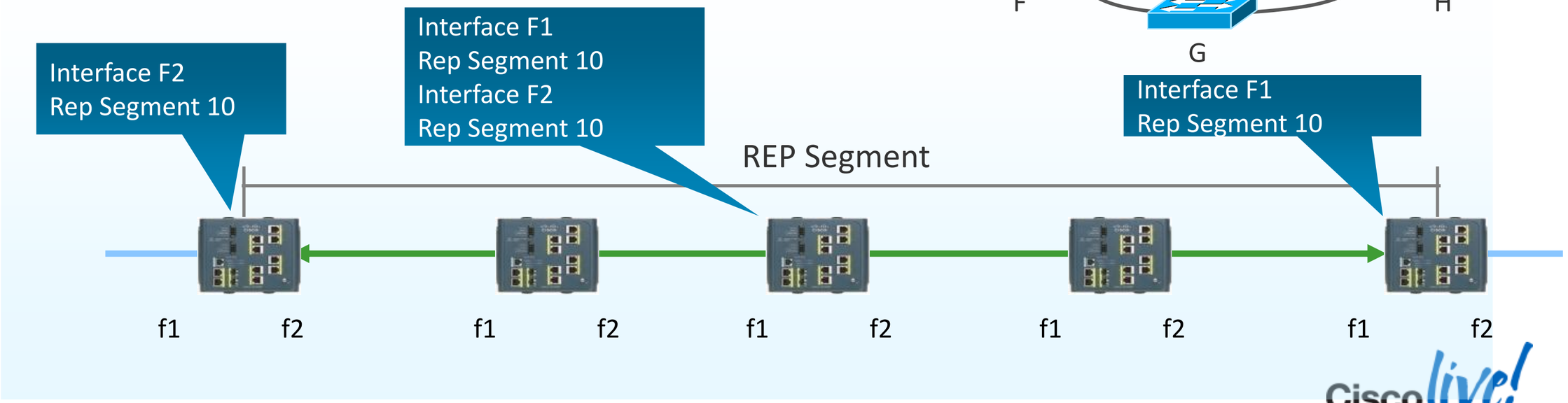


Resilient Ethernet Protocol

Segment Protocol

- REP operates on chain of bridges called segments
- Typically 20-50ms convergence
- A port is assigned to a unique segment

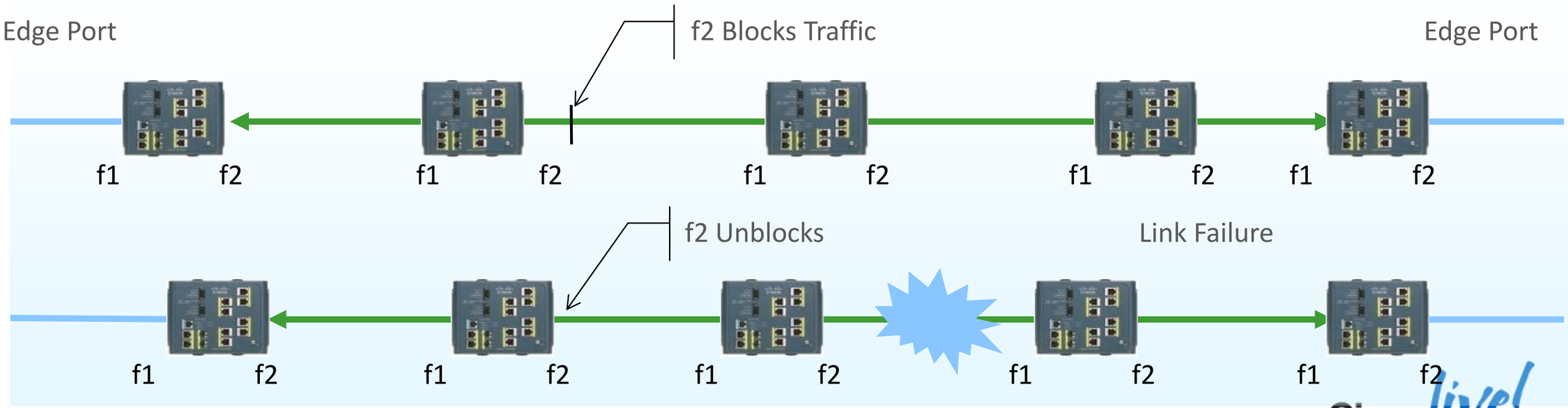




Resilient Ethernet Protocol

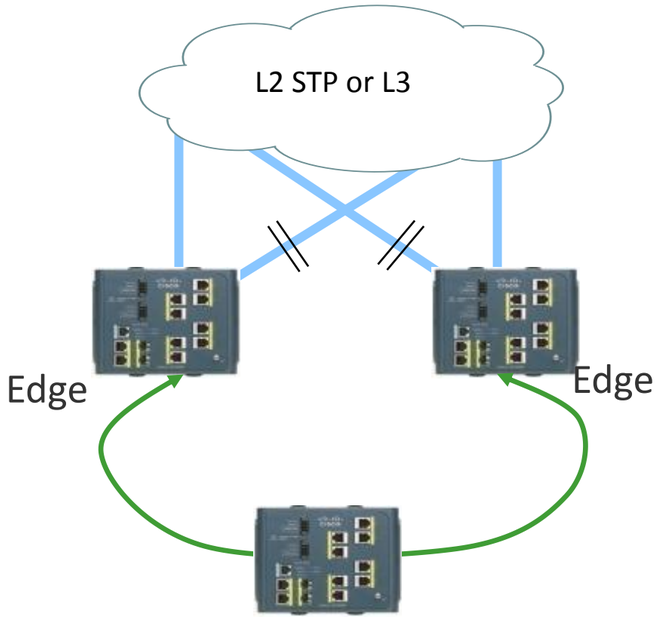
Blocked Port

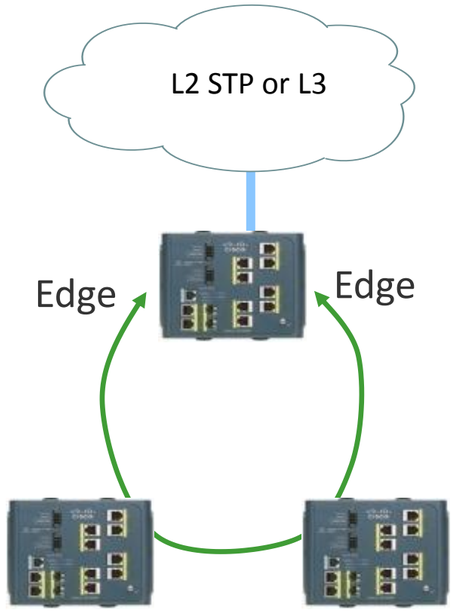
- When all links are operational, a unique port blocks the traffic on the segment. Called the Alternate Port
- If any failure occurs within the segment, the blocked port goes forwarding



Configuring Resilient Ethernet Protocol

- Edge ports on Segments can be wrapped into a ring
- Then connect to higher level distribution layer





Configuring Resilient Ethernet Protocol

- E
- T

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

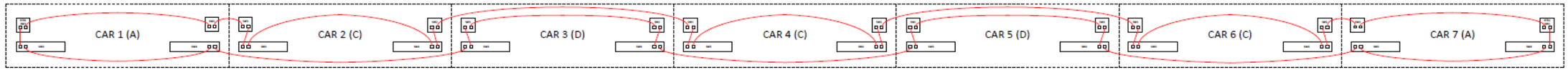
```
interface FastEthernet0/1
 description REP fiberloop1
 switchport trunk
 switchport mode trunk
 switchport nonegotiate
 duplex full
 priority-queue out
 rep segment 10 edge
 mls qos trust dscp
!
interface GigabitEthernet0/1
 description REP substation
 switchport mode trunk
 switchport nonegotiate
 priority-queue out
 rep segment 11
mls qos trust dscp
```

Example Topology Layouts – On-board Rail

Requirements: No car isolation if power fails.

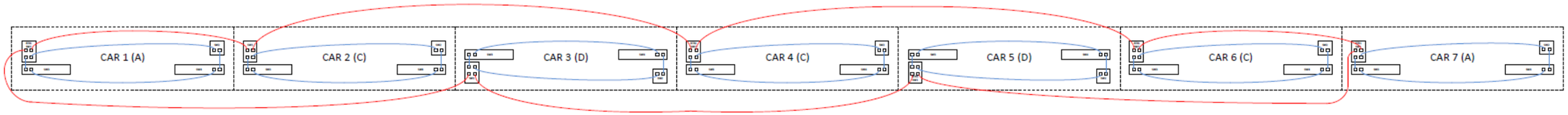
Ring Layout 1

Short cable loop layout. No network isolation if power failure in one car. Single Gigabit fibre ring of 26 switches.



Ring Layout 2

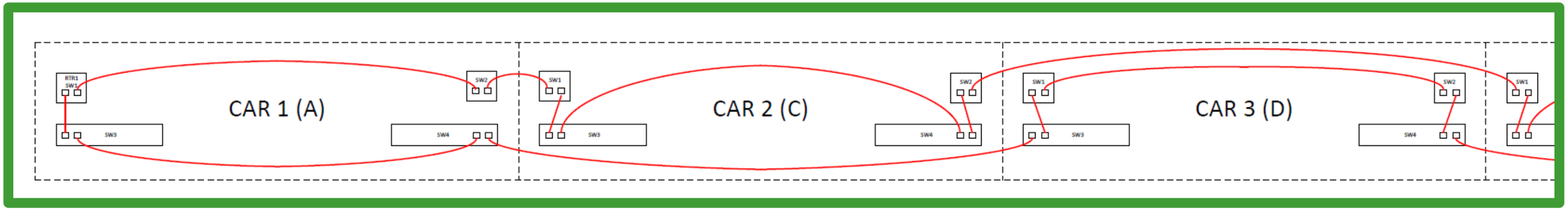
Short cable loop layout. No network isolation if power failure in one car. Gigabit fibre ring of 7 switches. In-car copper 100Mbps ring with 3 or 4 switches



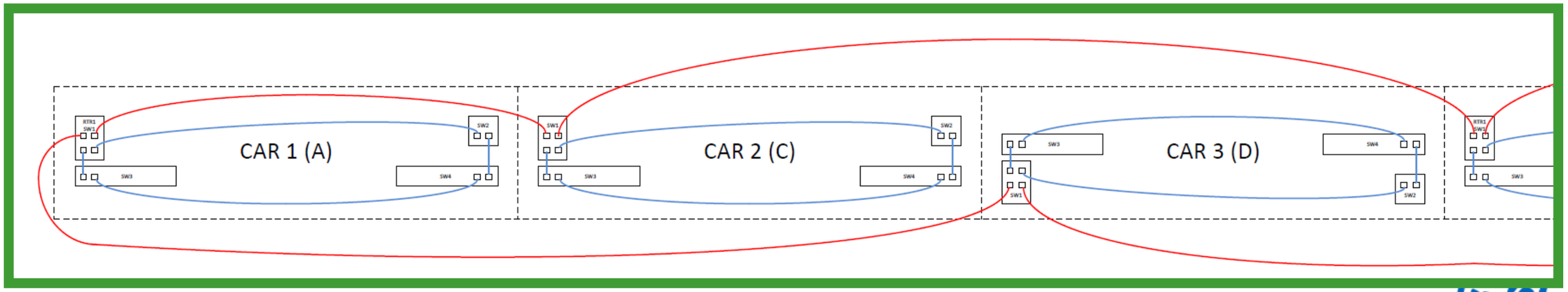
Example Topology Layouts – On-board Rail

Requirements: No car isolation if power fails.

Ring Layout 1

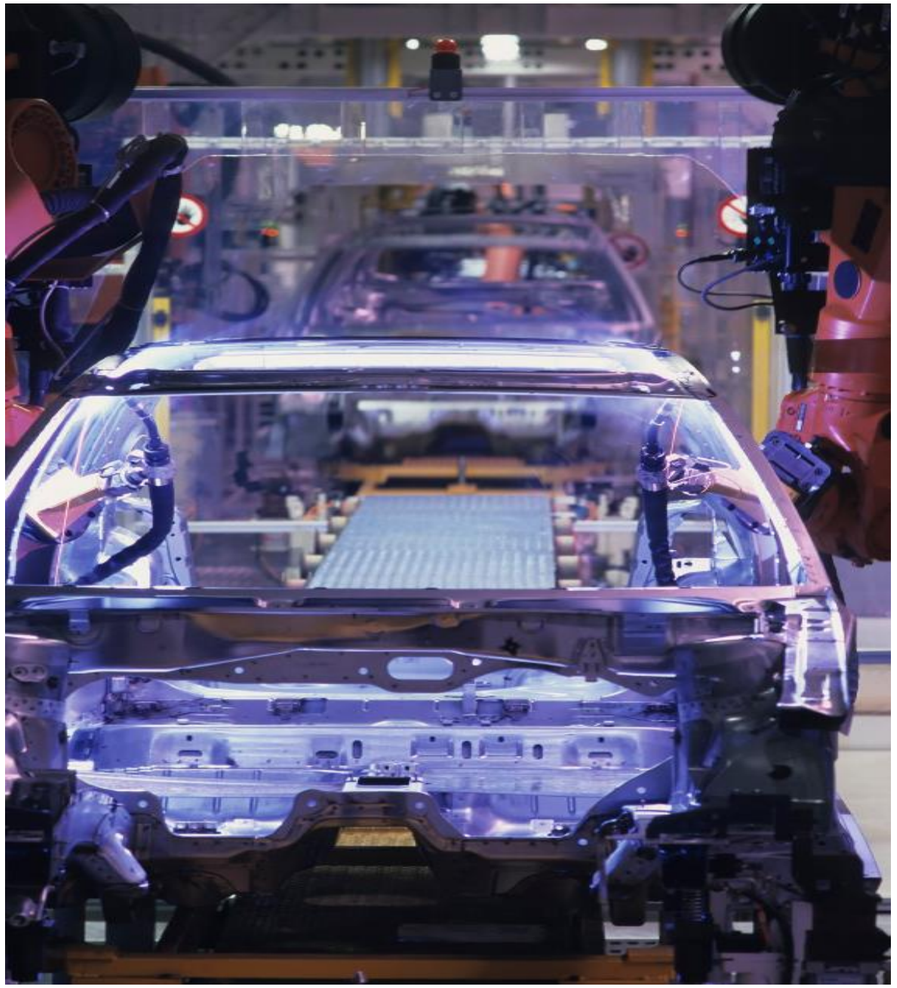


Ring Layout 2



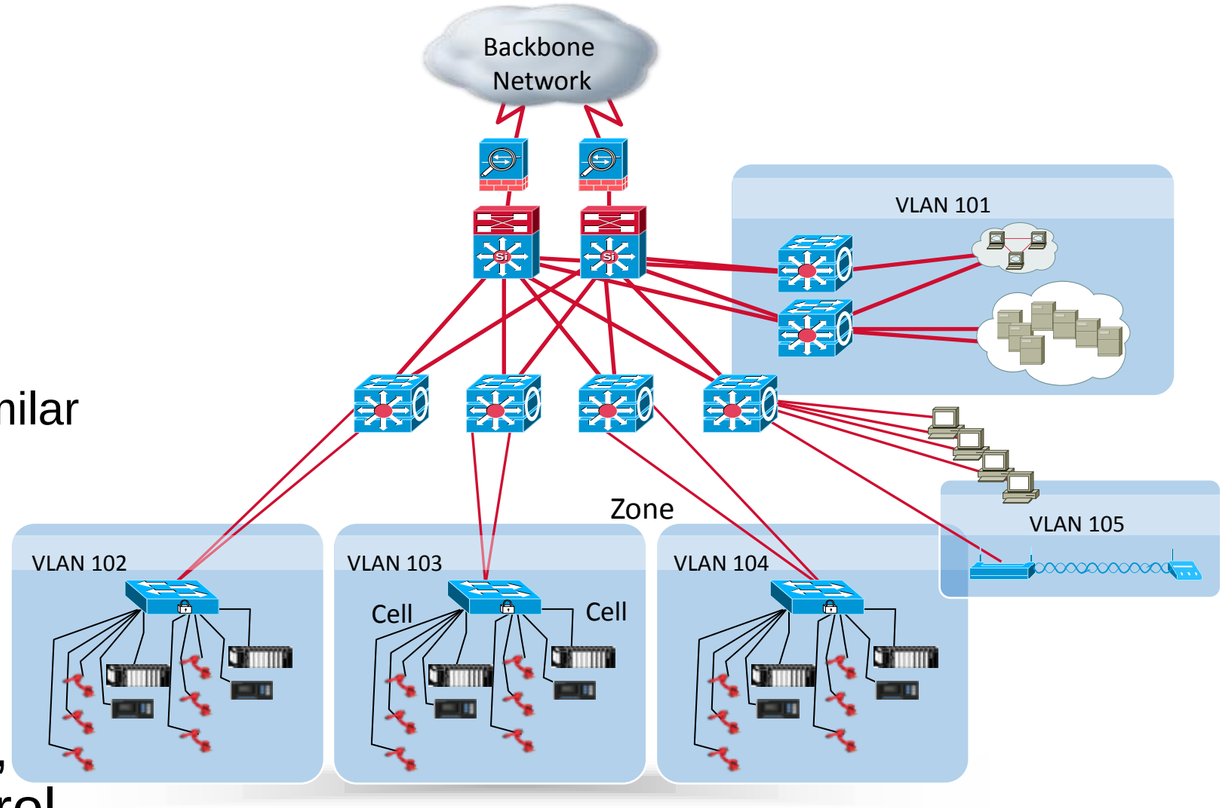
Agenda

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



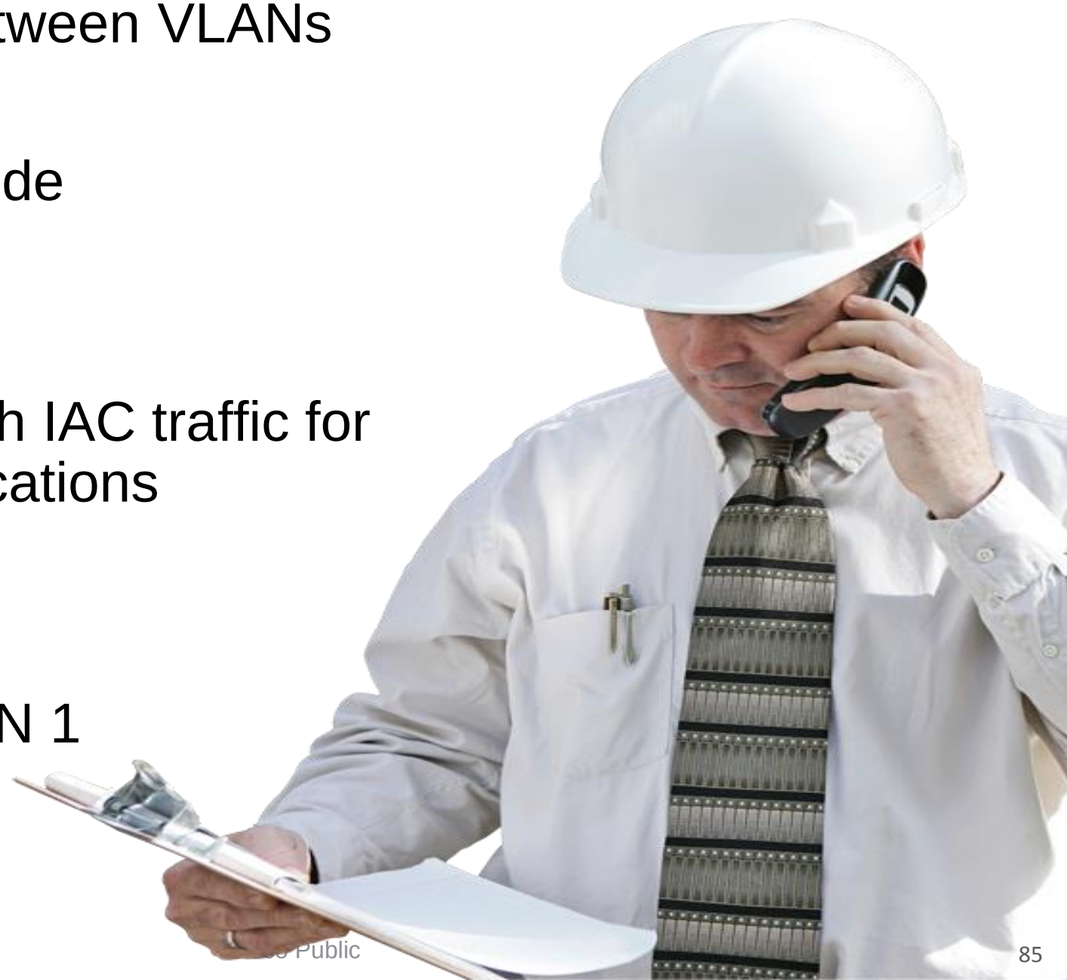
VLANs in an Industrial Ethernet System

- Design Small Cell/Area zones – Segment with VLANs a.k.a smaller 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.



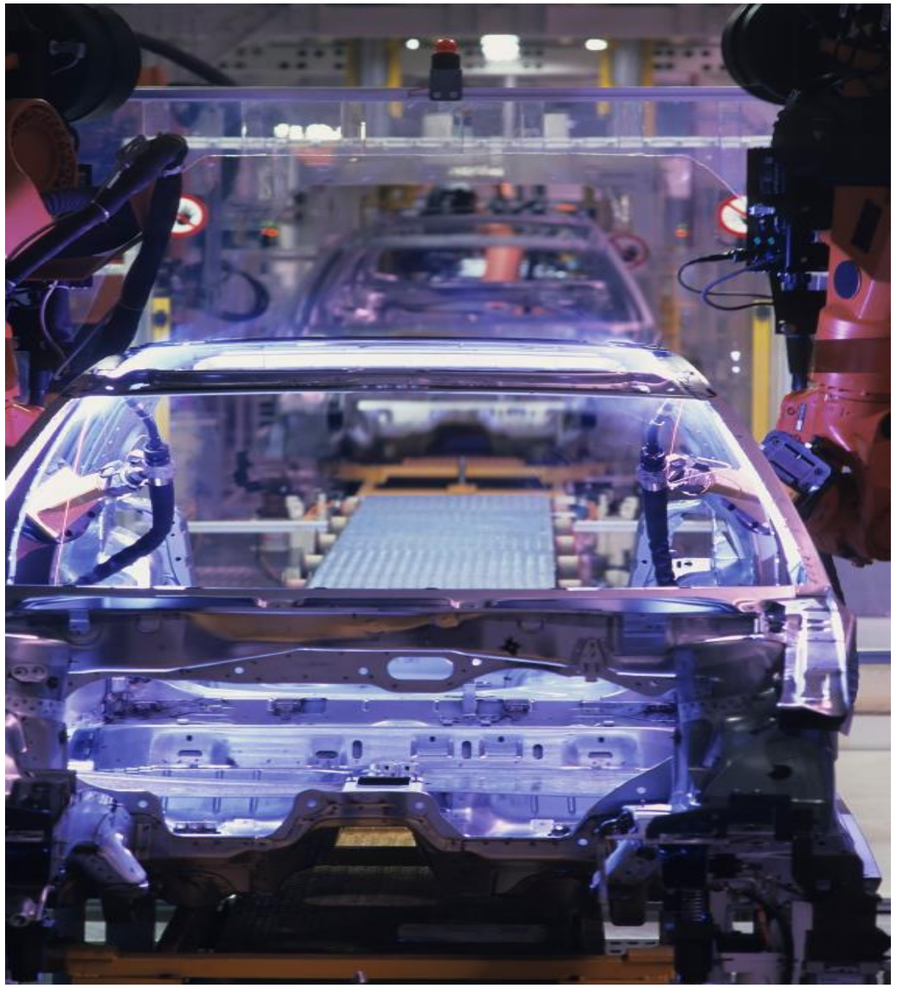
VLAN Considerations for Cell/Area Zone

- 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
- Do not use VLAN 1 for Control & Information Traffic
- Enable IP directed Broadcast on Cell/Area VLANs with IAC traffic for easy configuration and 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
- Recommended Resources
- Q&A



Not All Traffic is Created Equal

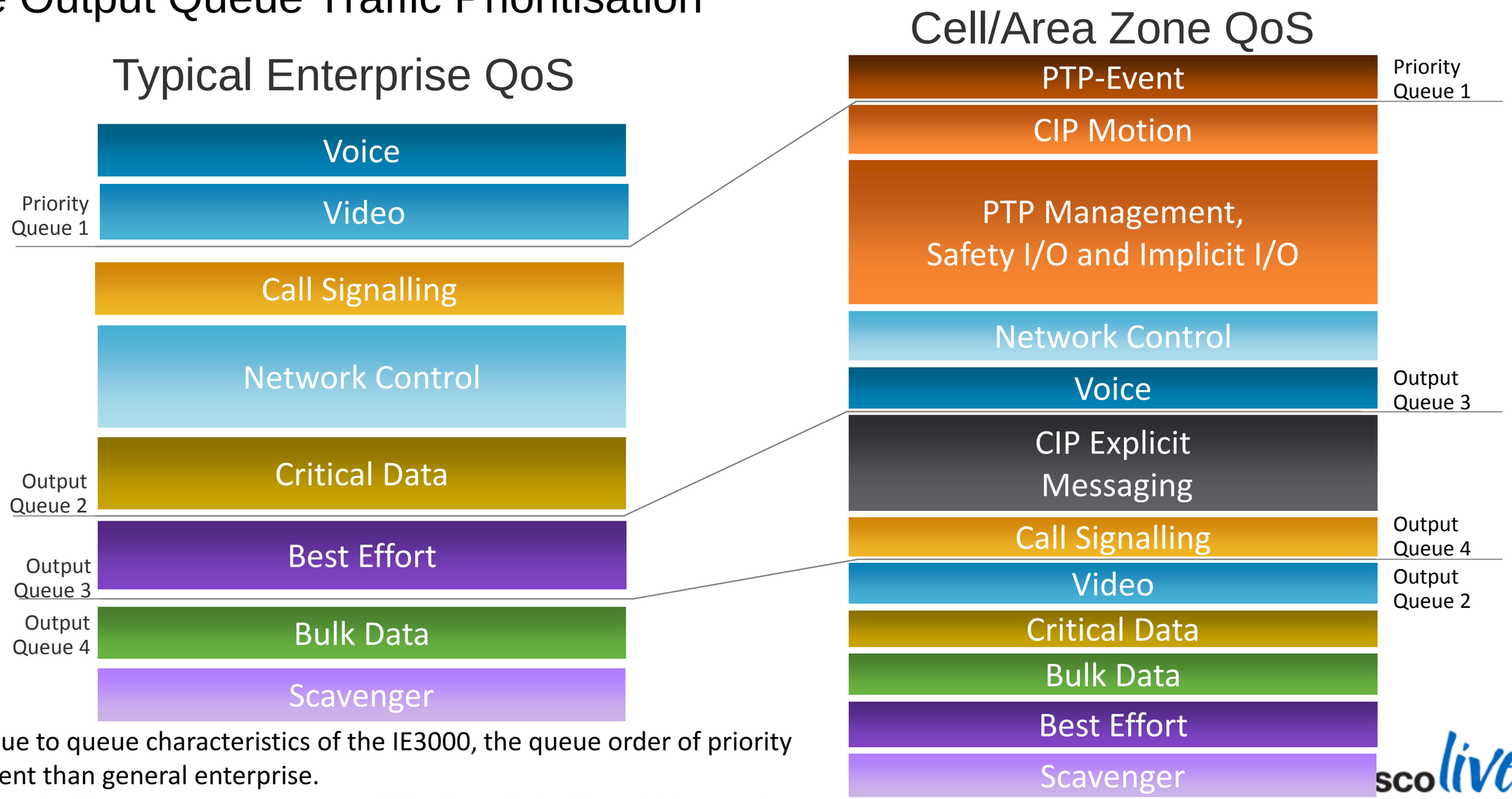
Prioritisation Is Required

	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 Quasi-Deterministic Data Flows with Low Latency and Low Jitter

Cell/Area Zone QoS Priorities

- Example Output Queue Traffic Prioritisation

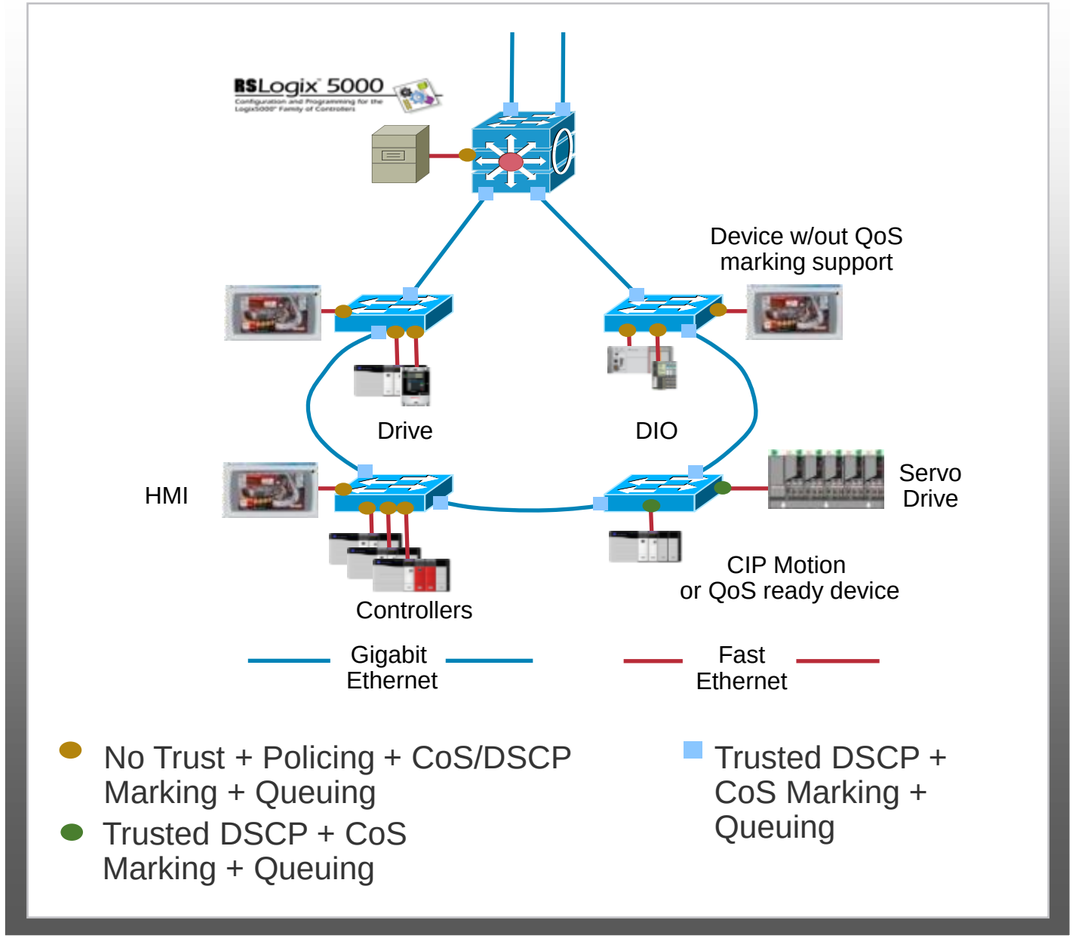


Note: Due to queue characteristics of the IE3000, the queue order of priority is different than general enterprise.

QoS Design 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

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



QoS – SmartPort Macros

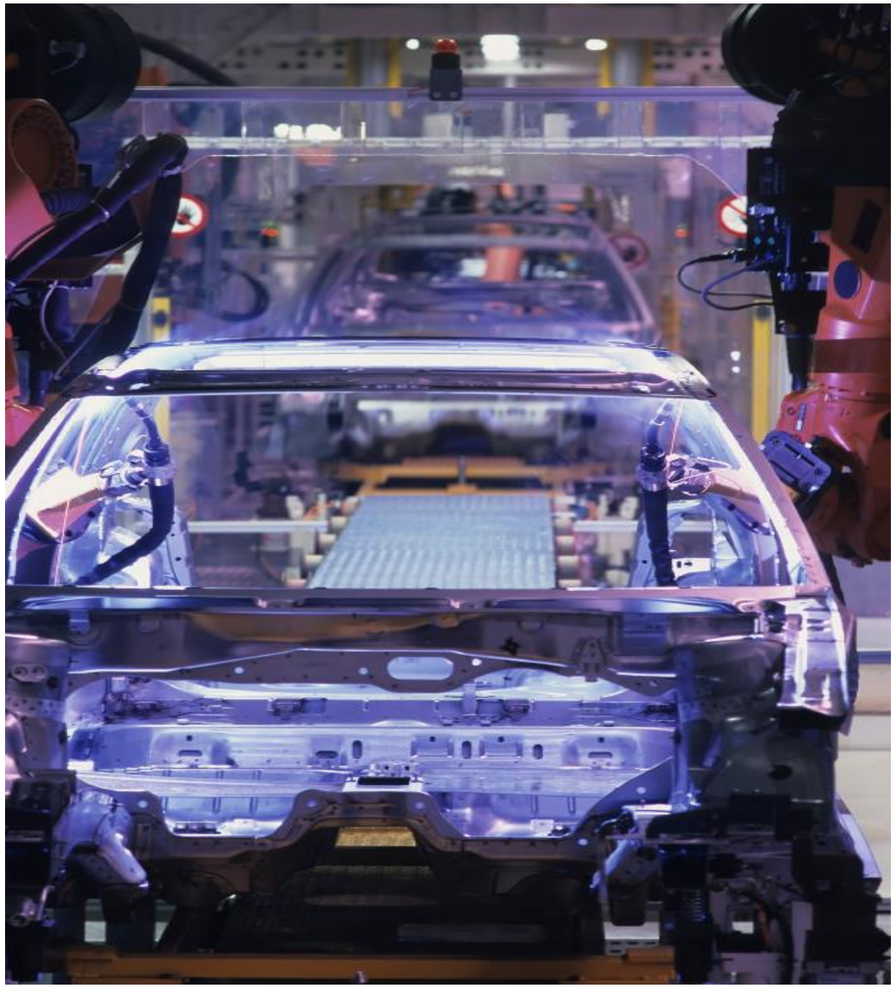
Design and Implementation Considerations

- QoS is integrated into the standard IE switch configurations
- Express Setup macros create the QoS service policy.
- Smartport macros enables QoS on ports:
  - QoS-enabled EtherNet/IP device macro for devices that can mark traffic
  - Regular EtherNet/IP device macro for other automation devices
  - IE-Switch macro applies QoS for trunks and uplinks
  - L2 CoS Markings are honoured.
- Deploy QoS consistently throughout the industrial network.

Quality of Service Does Not Increase Bandwidth. QoS Gives Preferential Treatment to Automation and Control Network Traffic at the Expense Of Others.

Agenda

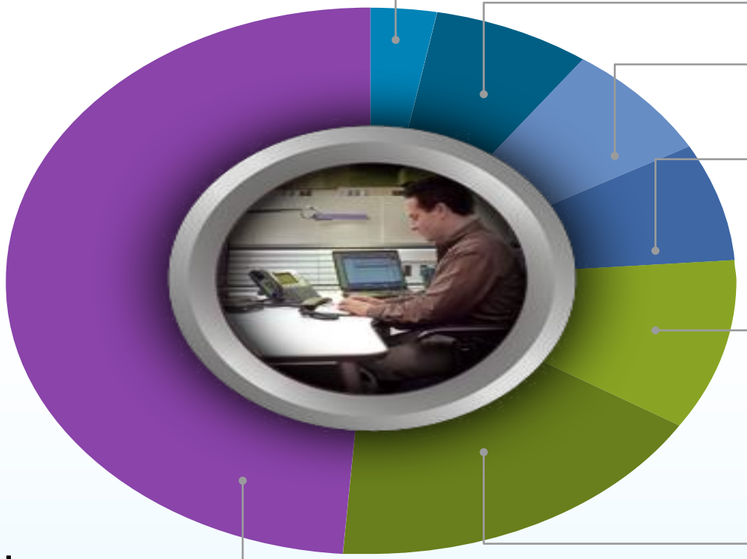
- Industry Trends
- Connected Industry Architectures
- Design Considerations
  - Traffic Flows and Topologies
  - Availability and Resilience
  - Segregation and VLANs
  - QoS
  - Security
- Recommended Resources
- Q&A



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

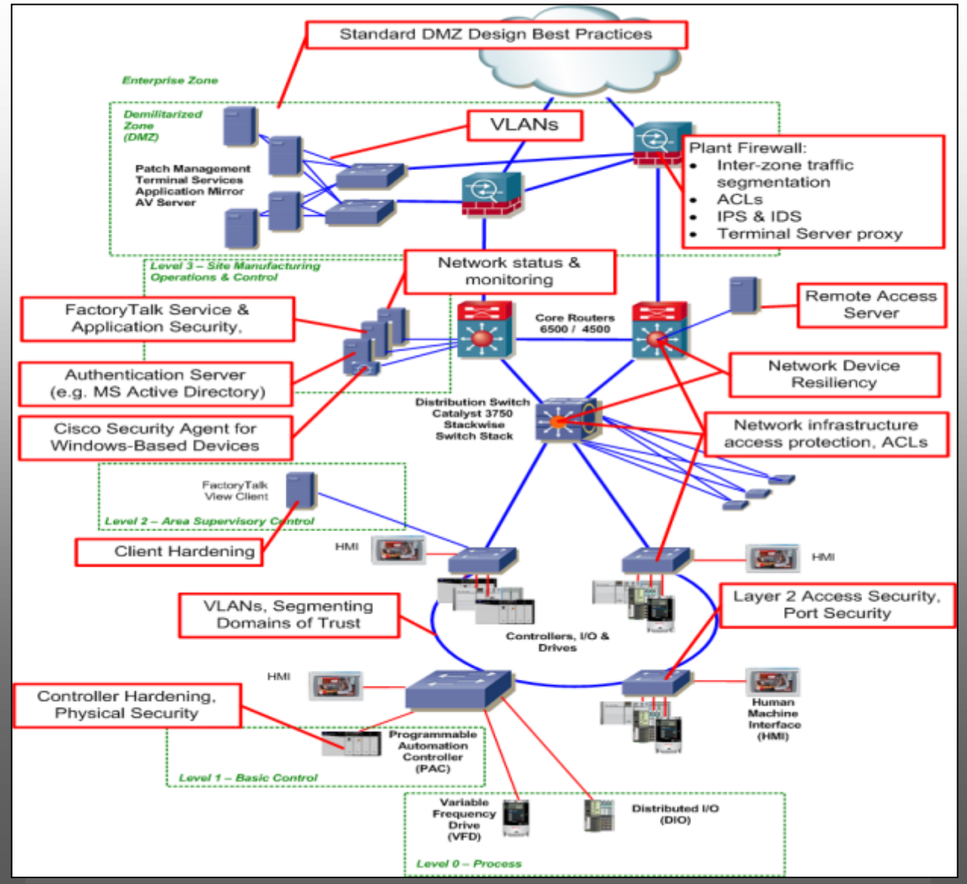
- Fragile TCP/IP Stacks – NMAP, Ping Sweep lockup
- Little or no device level authentication
- Poor network design – daisy chains, hubs
- Windows based IA servers – patching, legacy OS
- Unnecessary services running – FTP, HTTP
- Open environment, no port security, no physical security of switch, Ethernet 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

Staged Cyber-attack

Diesel Generator Control System

Security Guidelines

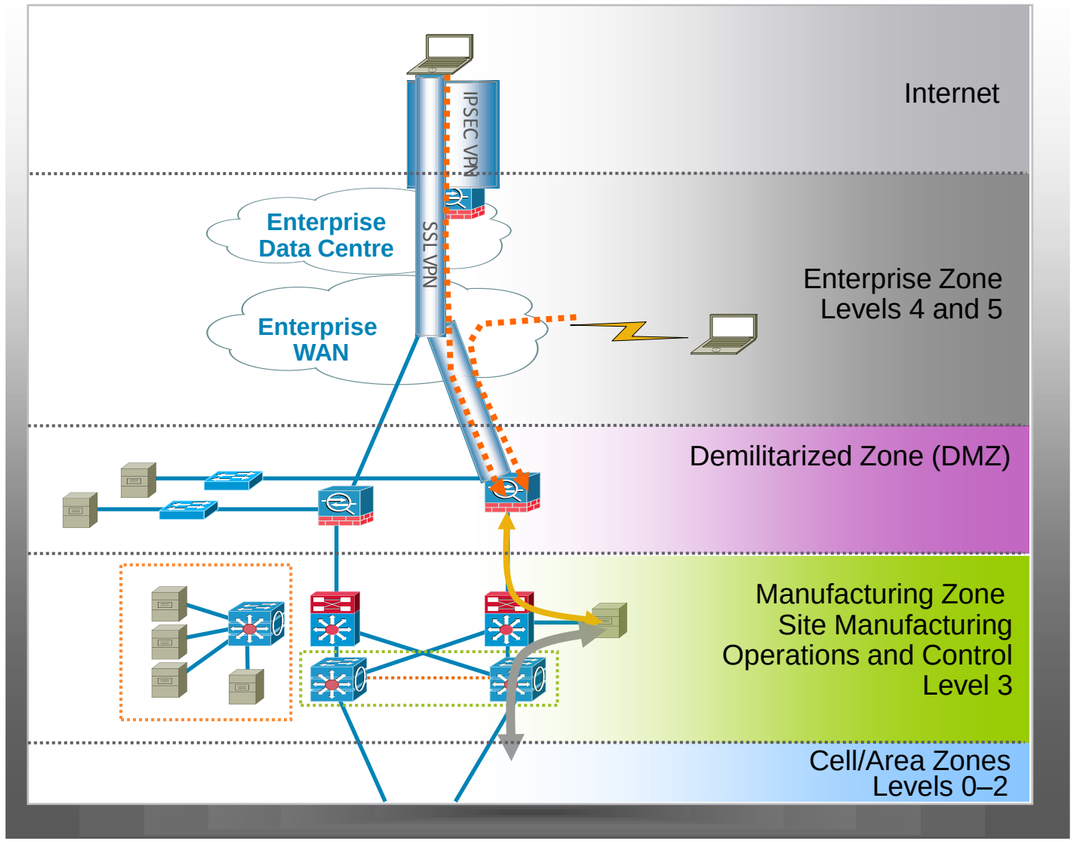
- Controls Security Policy
- Demilitarised Zone (DMZ)
- Defending the Industrial edge (IPS/IDS, ISE)
- Protect the Interior (ACL/Port Security)
- Remote Access Policy
- Endpoint and Network Hardening
- Physical Security



Defend the Industrial Edge

DMZ and Secure Remote Access Guiding Principals

- Firewalling and remote access at levels 0-2 (L2 Transparent Mode) with Industrial IPS/IDS
- Use IT-Approved Access and Authentication
  - VPN for secure remote access
  - Enterprise Access and Authentication servers (e.g Active Directory, Radius, etc.)
- ICS 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 industrial - the firewalls

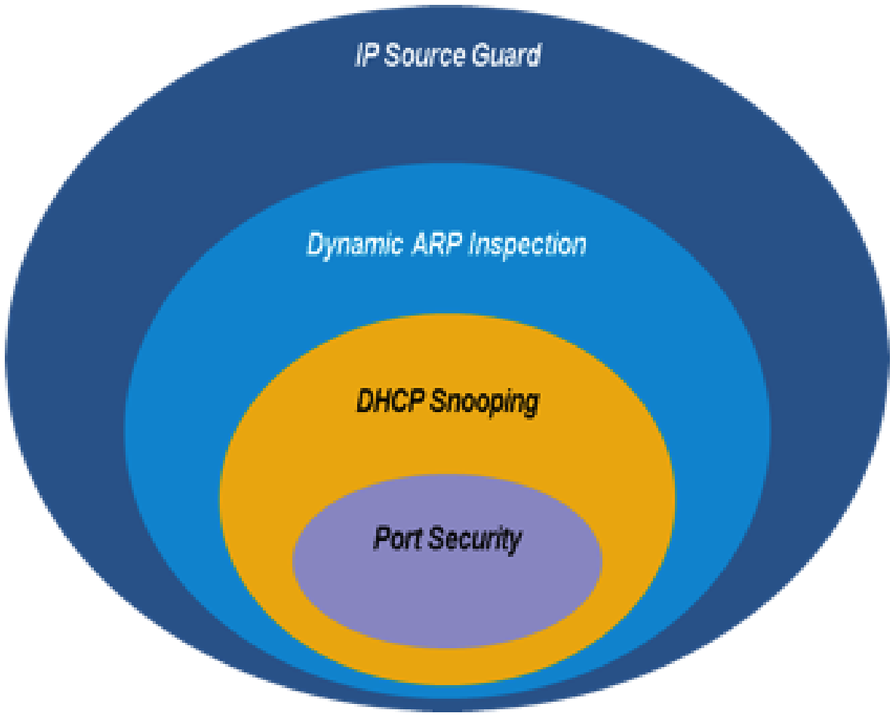


Protect the Interior

L2/3 Network Security Features

- Authentication
  - 802.1x Authentication, WebAuth, MAB
- CISF (Cisco Integrated Security Features):
  - Port Security (Limit MACs)
  - IPv4 and IPv6 DHCP Snooping (Prevent rogues)
  - IP Source Guard (No false IPs)
  - Dynamic Arp Inspection (Prevent rogues)
- Access Control Lists

CISF – Cisco Integrated Security Features



Protect the Interior

Traffic Control – Prevent DoS or accidental storms

- Storm Control
  - small-frame violation-rate 100 (frames less than 67b)
  - storm-control broadcast level pps 5k 4.5k
  - Storm-control broadcast level 20% 15%
  - storm-control multicast level pps 10k 9.5k
  - storm-control unicast level pps 5k 4.5k
  - storm-control action shutdown / trap
- Rate Limiting
  - Rate-limit input rate(bps) burst(bytes)
  - Rate-limit output rate(bps) burst(bytes)

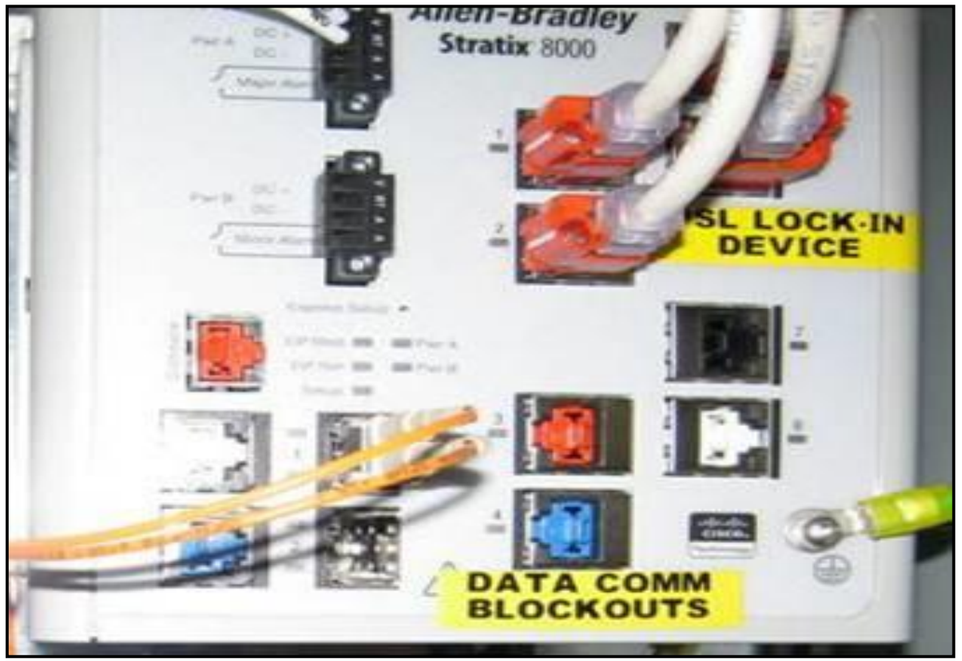
End-point and Network Hardening Procedures

- Use secure protocols on switches and devices(HTTPS, SCP, SNMPv3, SSH)
- Do not implement shared or “backdoor” accounts/password
- Enable password encryption (service password-encryption)
- Disable password recovery (no service password-recovery) CAUTION
- Disable small servers (tod, hello, etc.)
  - no service tcp-small-servers
  - no service udp-small-servers
  - no ip finger
- Enable memory leak detection and threshold alarming
- Comprehensive information here:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Defence-in-Depth

Physical Security - Examples



PANDUIT®

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

Cisco live!

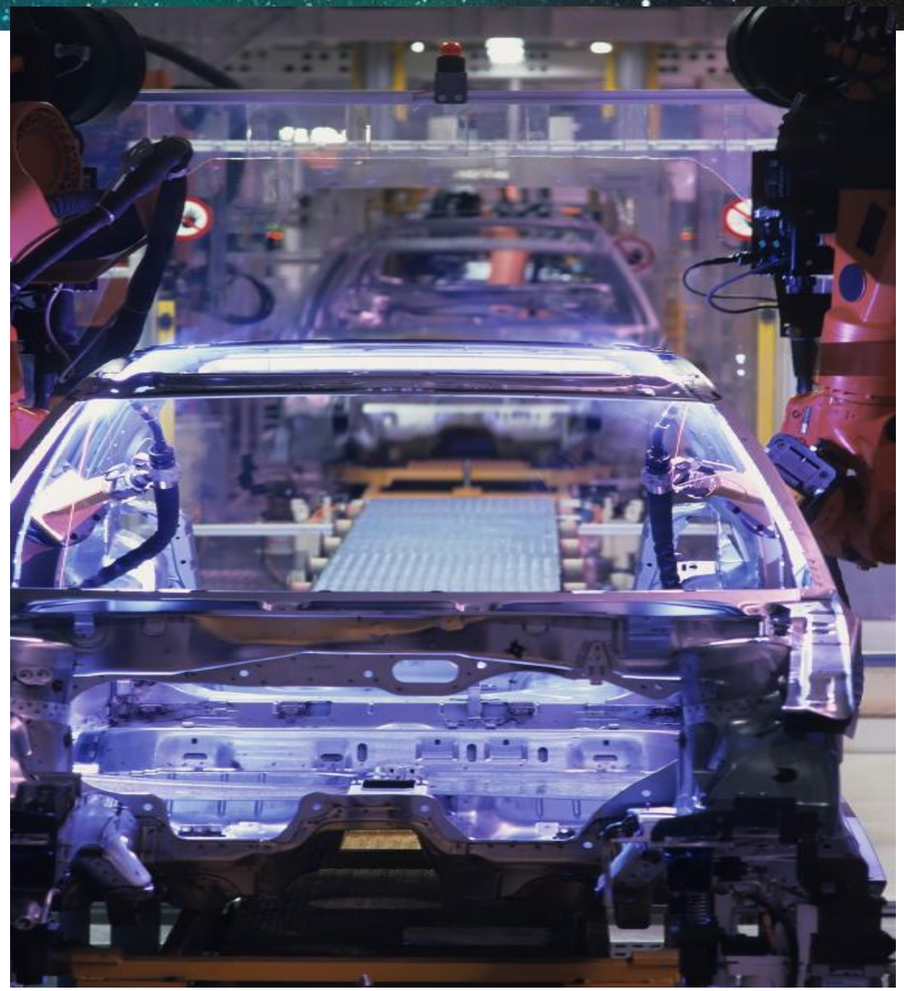
Additional Best Practices

Feature	Description	Mechanism
Network Foundation Protection	Protecting the core network infrastructure and services from unauthorised 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, Authorisation and Accounting	ACLs, MAC-filtering, VLANs, application authorisation
Threat Detection & Mitigation	Continuously and proactively monitor network activity for anomalous behaviour	Firewall, Intrusion Protection, Analysis and Response, Syslog
Layer 2	Employ L2 features to minimise possible network outages	VTP transparency, Loop/Root/BPDU guard, DHCP IPv4 and IPv6 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

In Summary

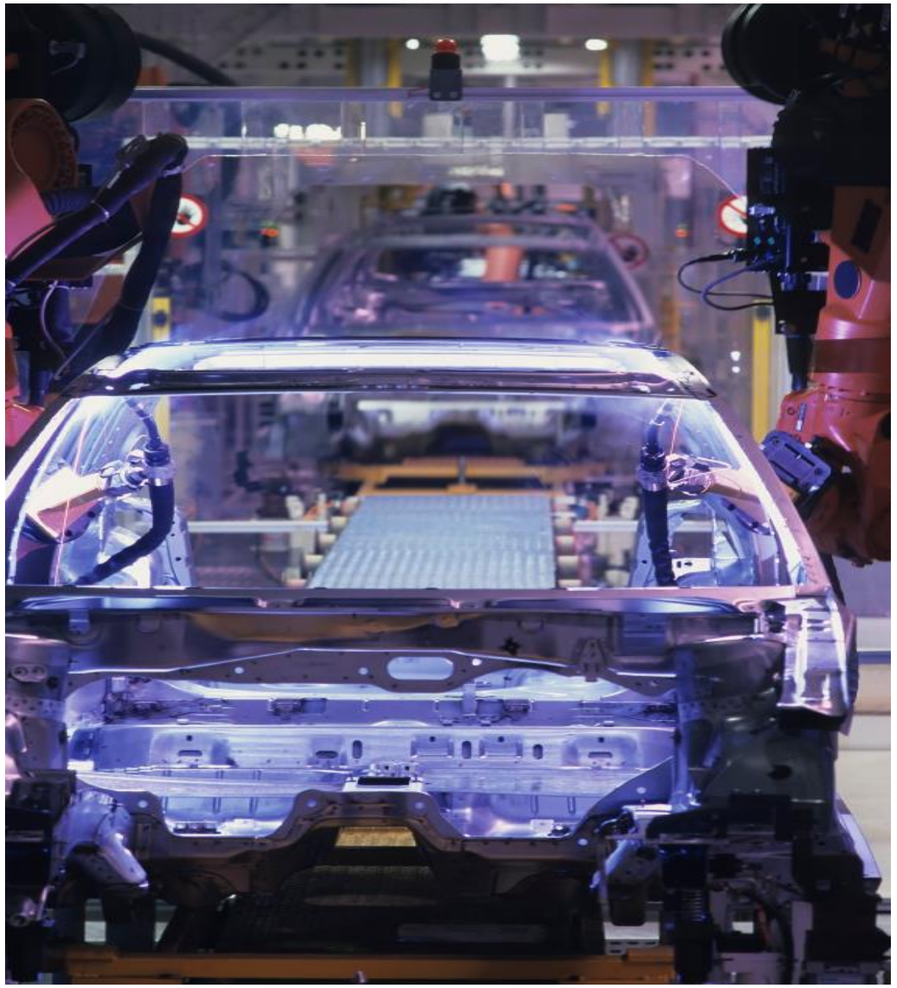
We've talked about

- Industry Trends
  - Convergence
- Connected Industry Architectures
  - Application and Protocols
  - CPwE
- Design Considerations
  - Topologies
  - Redundancy
  - QoS
  - Security



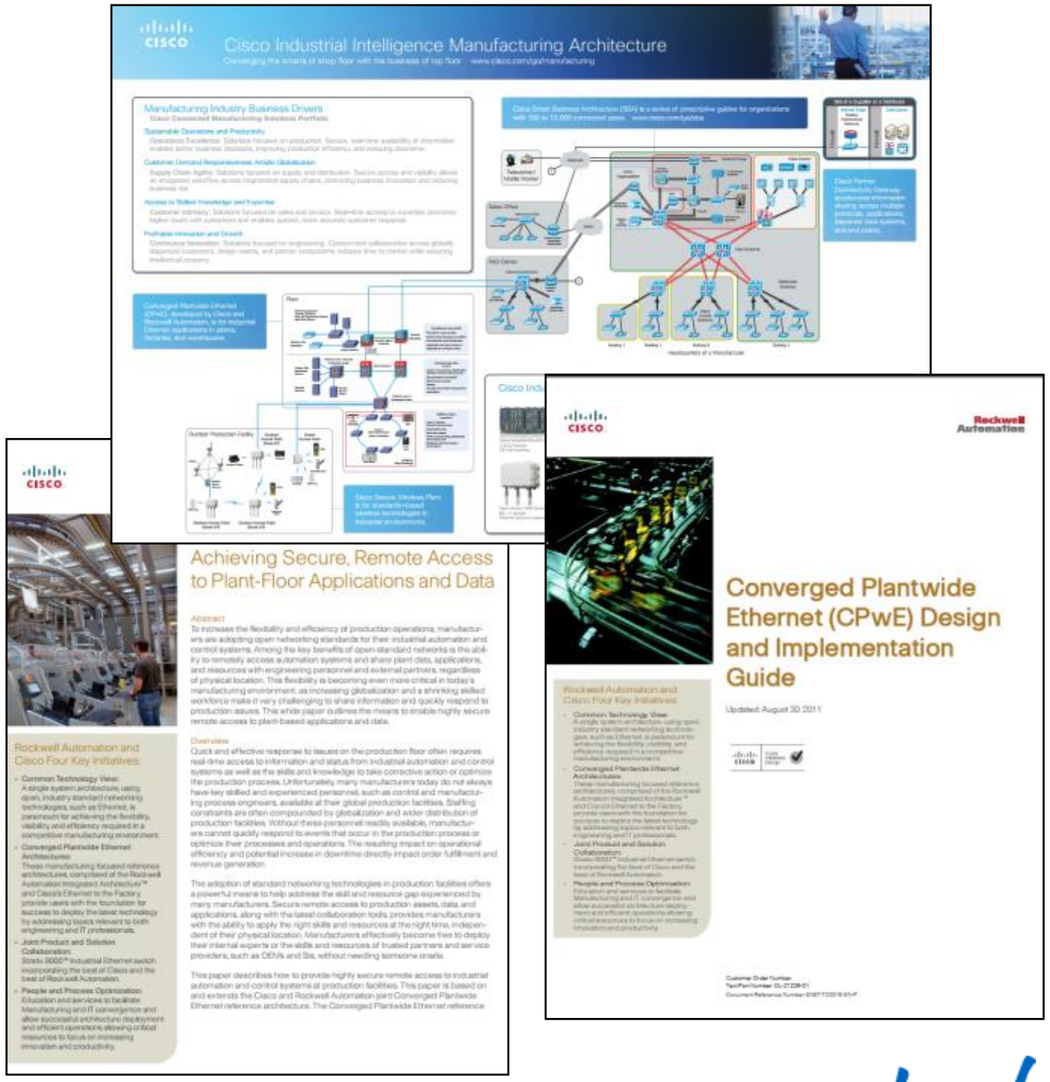
Agenda

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



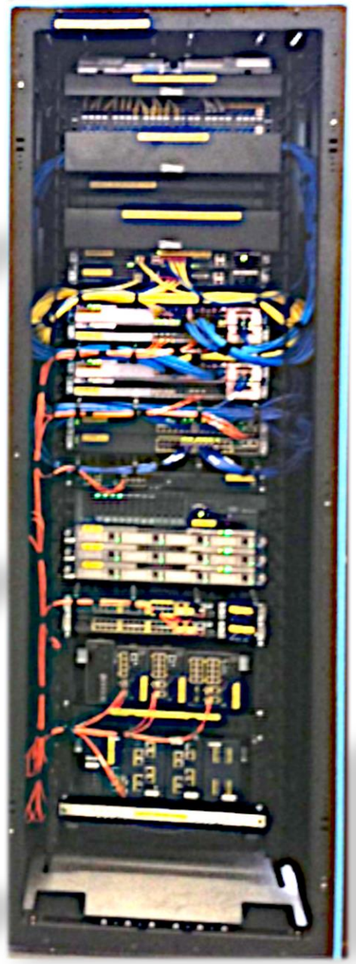
Recommended Resources

- Converged Plant-Wide Ethernet DIG
- Planning for a Converged Plant-wide Ethernet Architecture – ARC Group
- Secure Wireless Plant
- Industrial Intelligence Architecture
- Securing Manufacturing Computer and Controller Assets
- Achieving Secure Remote Access to Plant Floor Applications



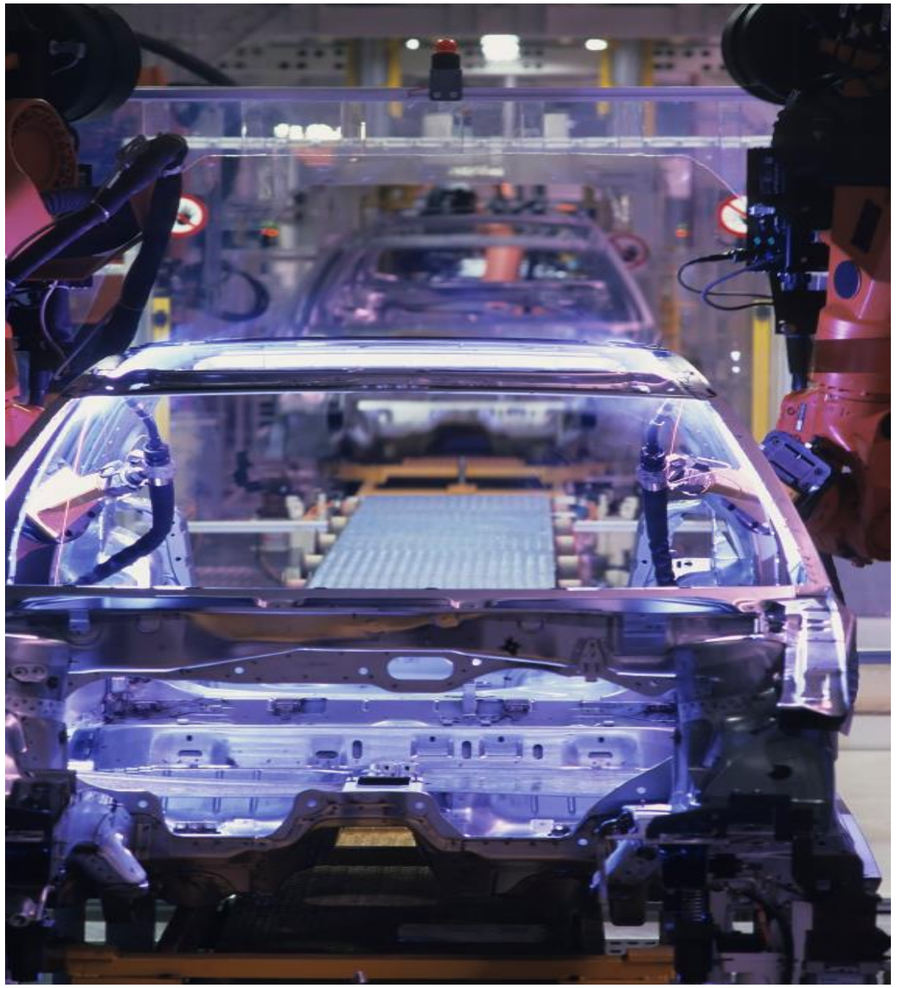
Call to Action

- **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
- Discuss your project's challenges at the **Technical Solutions Clinics**
- Attend one of the **Lunch Time Table Topics**, held in the main Catering Hall
- **Recommended Reading**: For reading material and further resources for this session, please visit www.pearson-books.com
- **CL365** -Visit us online after the event for updated PDFs and on-demand session videos. www.CiscoLiveEU.com



Agenda

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






Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 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 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com


CISCO
TM