



*TOMORROW
starts here.*

bb

Cisco *live!*



Industrial Networking Concepts, Design, Resilience and Security

BRKRST-2661

Andrew O'Brien

Consulting Systems Engineer

#clmel

Cisco *live!*

Session Abstract

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

- This 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
- Industrial Networking
 - A Quick 101 Guide
 - Applications and Protocols
 - Products and Architectures
 - Availability and Resilience
 - Security
- Q&A
- Recommended Resources



Agenda

- Industry Trends
- Industrial Networking
 - A Quick 101 Guide
 - Applications and Protocols
 - Products and Architectures
 - Availability and Resilience
 - Security
- Q&A
- Recommended Resources





*TOMORROW
starts here.*

*For some 'Things' TOMORROW
actually started 1950*

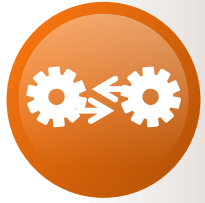
bb

Cisco *live!*



Photo: Australian National Library - <http://nla.gov.au/nla.pic-vn3092827>

Our World is Rapidly Moving to Embrace IoE



Our world is becoming
Instrumented



Sensors



New Data



Our world is becoming
Interconnected



Event
processing
and integration



New Insights



Our world is becoming
Intelligent



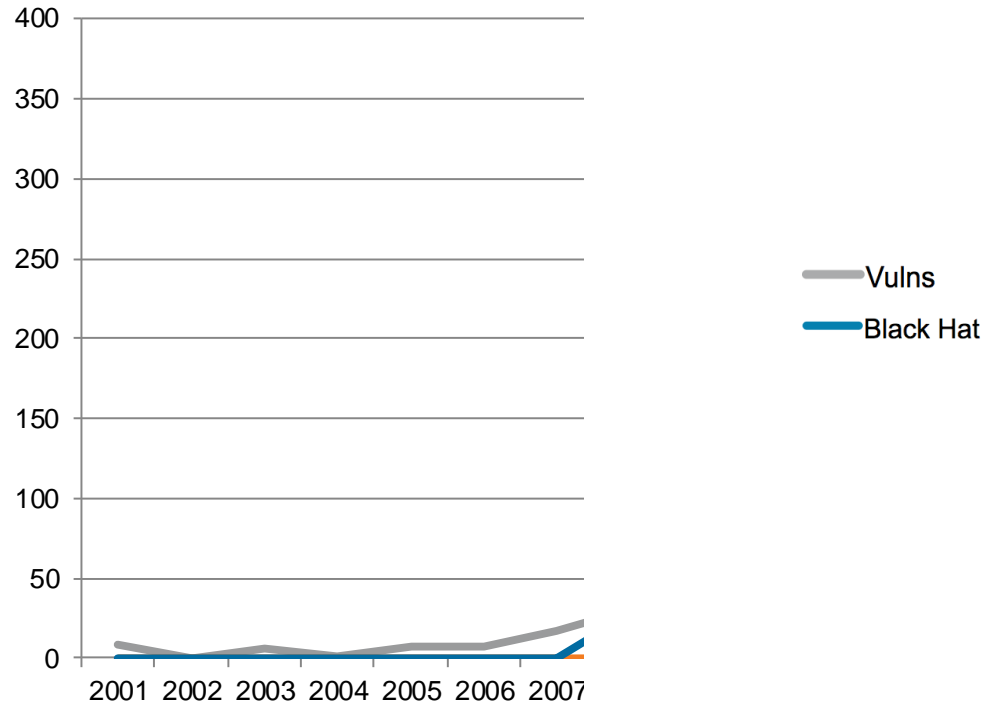
Digitisation
and
automation



**Process
Innovation**

A Renewed Focus on Security

Why Must IoE and OT Security Change?

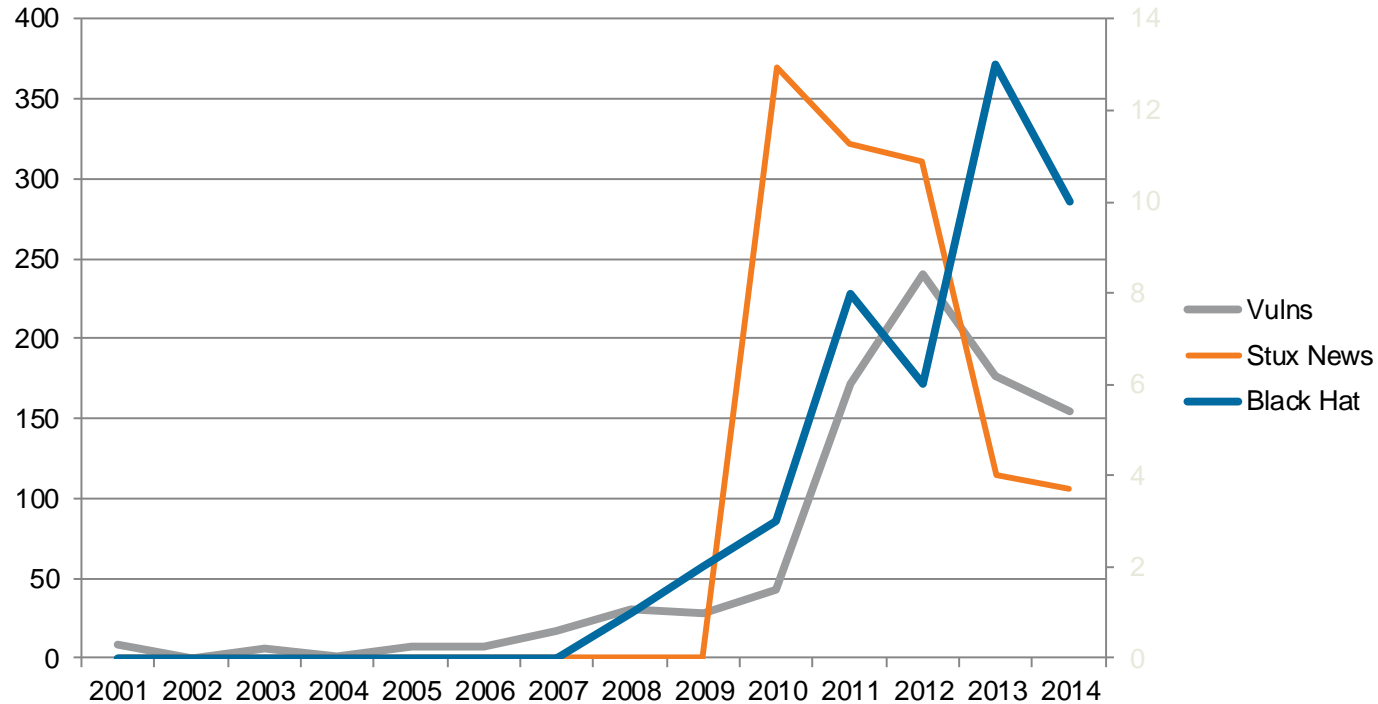


Source: osvdb.org; blackhat; [google news search](#)

A Renewed Focus on Security

Why Must IoE and OT Security Change?

Trends in discovery and correlation with external events.



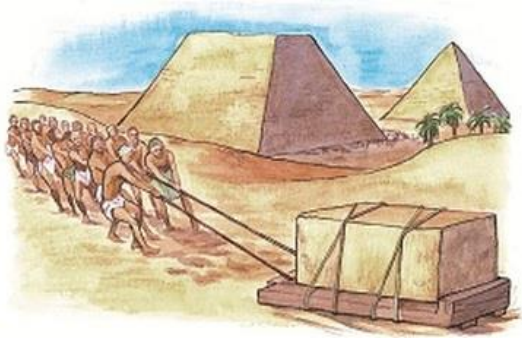
Source: osvdb.org; blackhat; [google news search](http://google.com/news)

Agenda

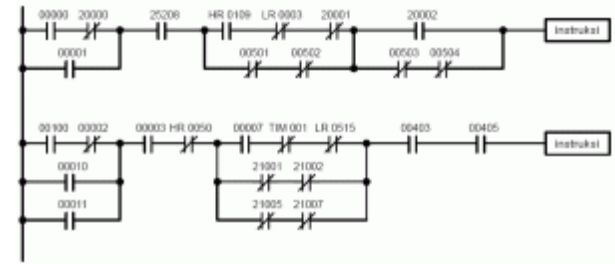
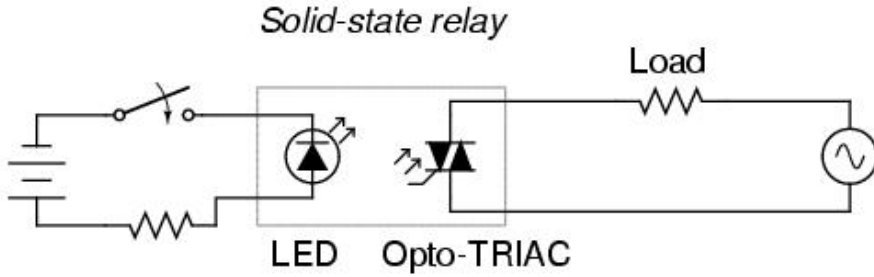
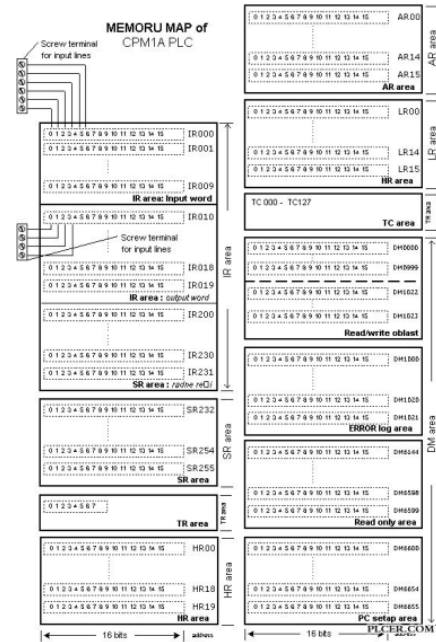
- Industry Trends
- Industrial Networking
 - A Quick 101 Guide
 - Applications and Protocols
 - Products and Architectures
 - Availability and Resilience
 - Security
 - Q&A
- Recommended Resources



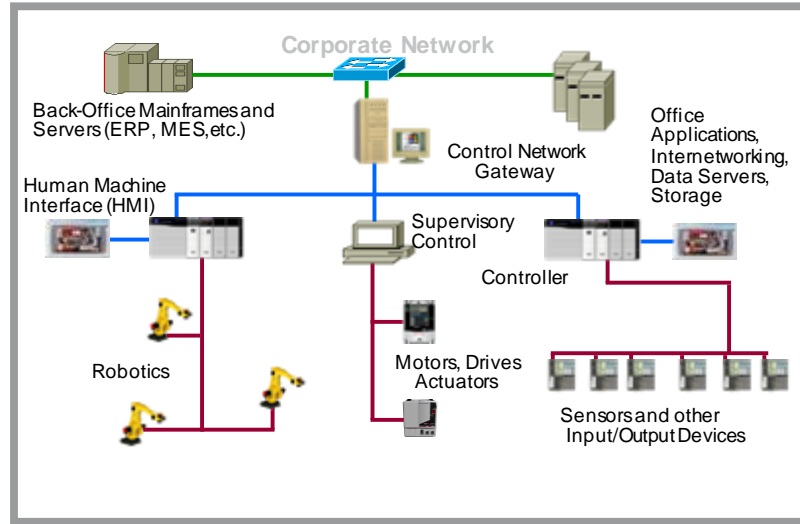
In the beginning...



...then along came the PLC...



...which could be “networked” (not with Ethernet...)



Control Loops Could Not Tolerate This

Legacy 10BASE2/10BASE5 Ethernet: Lots of CSMA/CD Collisions

The reason Ethernet got a bad reputation for determinism...



Evolution of Ethernet

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

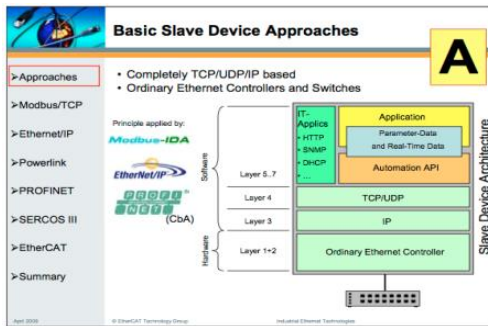
Major Improvements. Add QoS, non-blocking, but still not completely deterministic...



A Plethora of Standards and Protocols

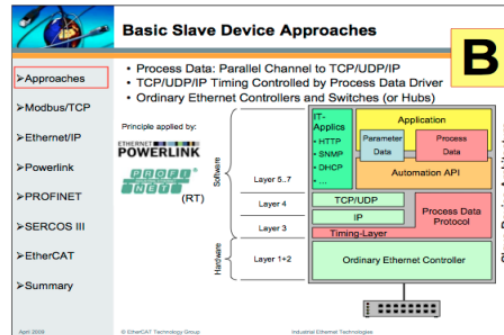
Familiar story – drive to consolidate standards and protocols

Standard Network Stack



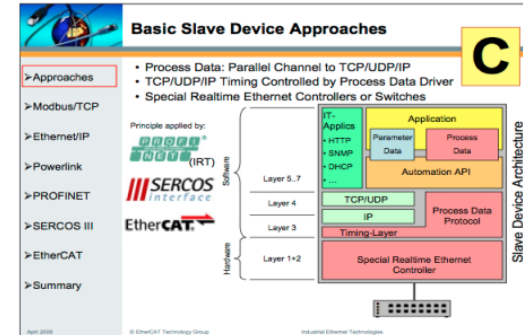
- Based on Open Standards at layers 1-4
- Use of IEEE 1588 Precision Time Protocol (PTP) for further determinism
- Viewed as slow or non-deterministic

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

Agenda

- Industry Trends
- **Industrial Networking**
 - A Quick 101 Guide
 - **Applications and Protocols**
 - Products and Architectures
 - Availability and Resilience
 - Security
- Q&A
- Recommended Resources





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 TCP
- [PROFIBUS/PROFINET](#) – by PNO, Siemens centric.
- [SERCOS](#) – Primarily used by drive systems. Ethernet-based version is SERCOS III
- [OPC](#) – OLE for Process Control.
- [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 electricity.
- [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 TCP
- [PROFIBUS/PROFINET](#) – by PNO, 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 electricity.
- [IEC 61850](#) - A standard for the design of electrical substation automation, including protocols.



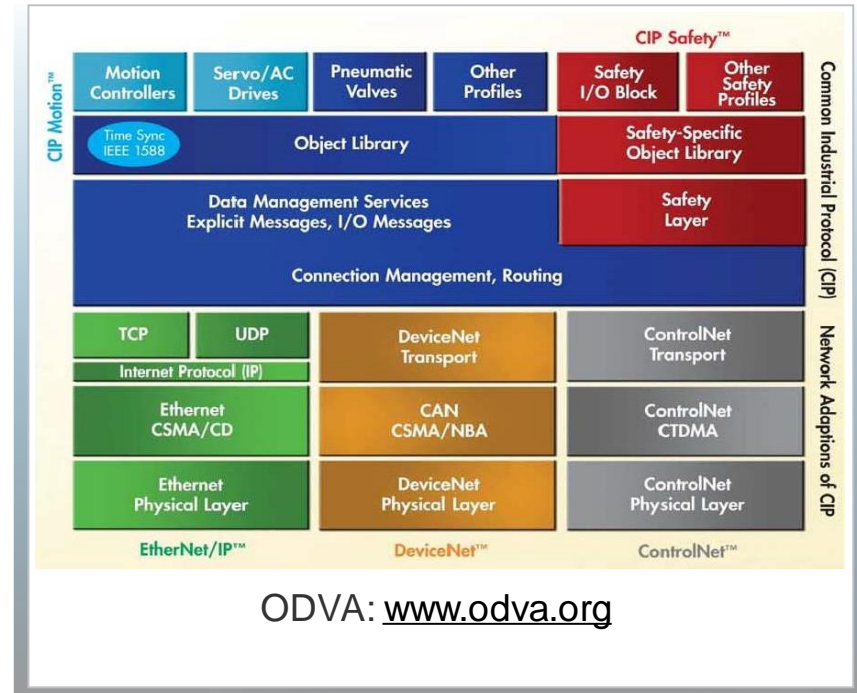
Ethernet/IP

Cisco *live!*

What is EtherNet/IP and CIP

Common Industrial Protocol

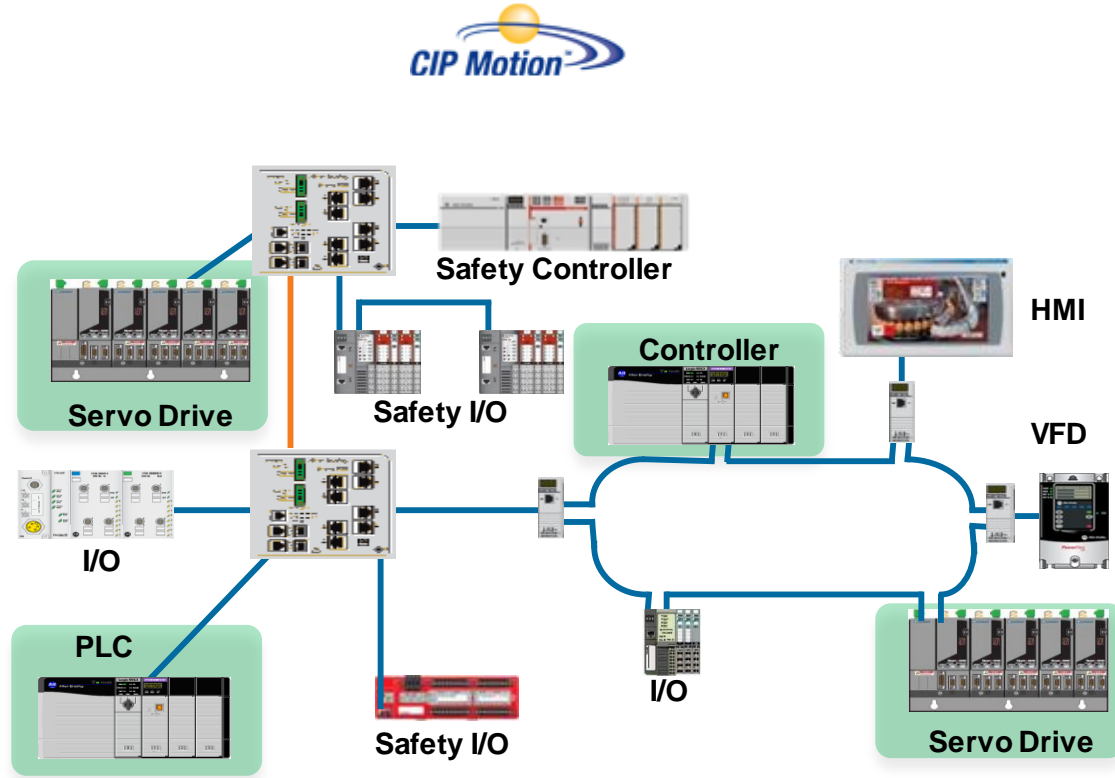
- Standard to integrate I/O control, device configuration and data collection in automation and control systems
- EtherNet/IP is based on Ethernet, IP and TCP/UDP
- Supported by the Open Device Vendor Association
- Defined in Layers 4 to 7. Media independent
- Key communication includes:
 - CIP Control traffic (Implicit): I/O control, drive control
 - CIP: Information traffic (Explicit): HMI, MSG's, Program upload/download
- Other common network 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 switch flash



Ethernet/IP – CIP Extensions

CIP Motion

- Deterministic, Real-time, Closed Loop Motion Control
- Full Standard Ethernet/IEEE 802.3 and TCP/IP Compliance
- Uses IEEE-1588 PTP (Precision Time Protocol) Synchronisation
- Up to 100 Coordinated Servo Axes w/ 1ms Update



Cisco Ethernet/IP Considerations

- For HMI integration: CIP Protocol is off by default – Must be enabled
- CIP can only be enabled on one VLAN

```
Switch(config)#interface vlan 20  
Switch(config-if)#cip enable
```

- CIP's producer/consumer model and I/O implicit messaging is typically multicast
 - Enable IGMP Snooping to prevent flooding
 - Standard setup on IE switch enables IGMP v2, Querier and Snooping
- Enable 1588 PTP Precision Time Protocol for Motion



PROFINET

The PROFIBUS Family

PROFIBUS DP



Decentralised Periphery

- Low cost, simple high speed field level communications
- Generally designed for internal use – i.e. cabinet mounted
- It can use different physical layers such as RS-485, wireless or fibre optics. RS-485 is most common.
- Defined at L1, L2 and L7.



PROFIBUS PA



Process Automation

- Based on PROFIBUS DP
- Developed specifically for the process industry to replace 4-20mA transmissions
- Two-wire connection carrying both power and data
- Generally designed for outdoor use – i.e. field mounted
- Support for hazardous and explosive environments



PROFINET



Industrial Ethernet Protocol

- High speed, highly deterministic networking with a “real-time” channel and TCP/IP for “non-real time” communication
- Standard IEEE802.3 Ethernet at 100Mbps with copper or fibre
- Generally designed for internal use, like PROFIBUS DP
- It is **not** PROFIBUS over Ethernet!



PROFIBUS and PROFINET in IEC 61158 and IEC 61784

Communication Medium	IEC 61158 protocol name (IEC 61158-2)	IEC 61784 protocol name (IEC 61784-2)
1	DP	PROFINET
2	GP	PROFINET
3	PA	PROFINET
4	PA	PROFINET
5	PA	PROFINET
6	PA	PROFINET
7	PA	PROFINET
8	PA	PROFINET

For PROFIBUS and PROFINET the communication channels are implemented in CP 5. For PROFIBUS in Layer 2 and PROFINET Layer 1 of IEC 61784-2. Actually, more than 20 physical types exist.



PROFINET Defines Two Application Classes

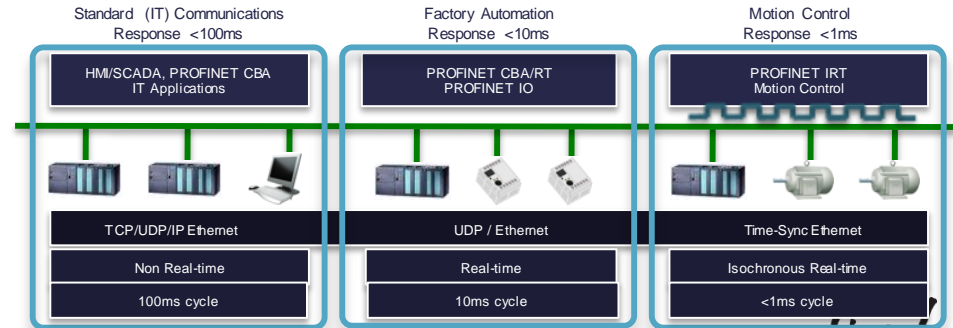
PROFINET CBA

- Component Based Automation
- Built on DCOM (Distributed Component Object Model) and RPC (Remote Procedure Call) technologies
- Object oriented approach to communications between distributed islands of automation
- Provides a scalable architecture for dealing with complex distributed automation and control systems

PROFINET IO

- Connection between distributed IO Devices and Controllers.
- Defines three communication channels
 - PROFINET NRT – Non-Real-Time
 - PROFINET RT – Real-Time
 - PROFINET IRT – Isochronous Real-Time
- IP application protocols for configuration and maintenance functions: DHCP, DNS, SNMP, HTTP/S

Intelligent Data Exchange Between Machines

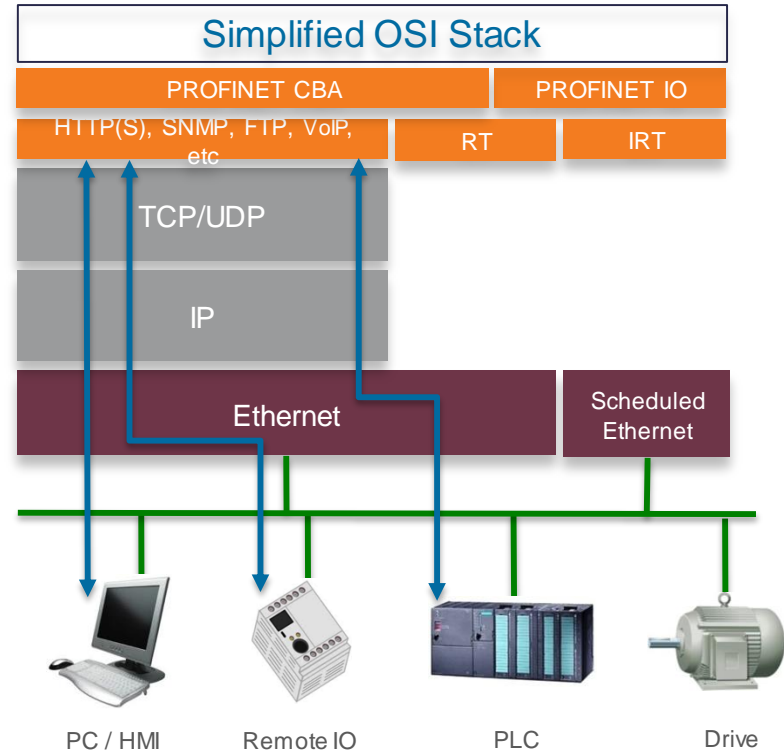


CiscoLive!

PROFINET IO – Communication Channels

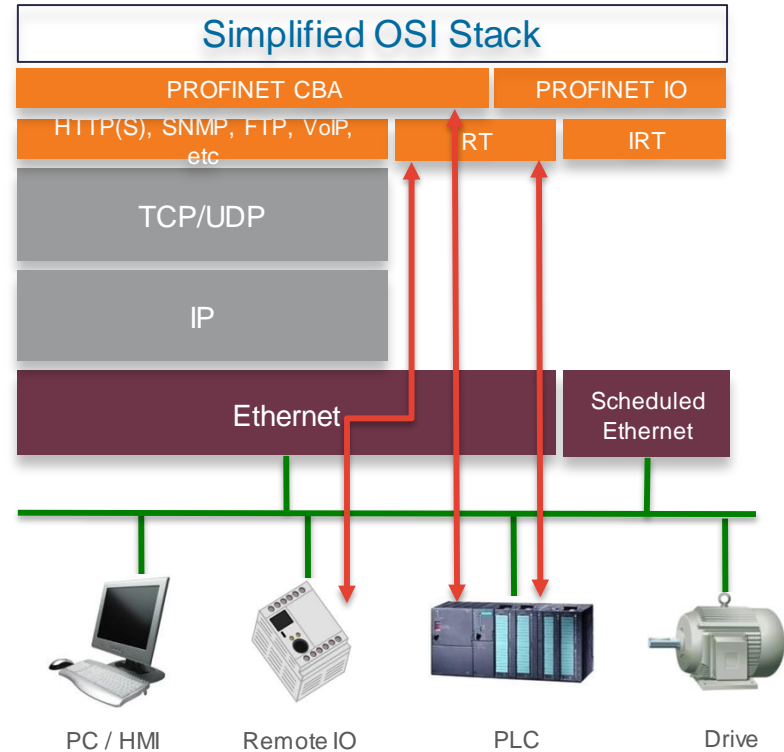
- PROFINET NRT (Non Real-Time)
 - Response (cycle) times of typically 100ms
 - Standard TCP(UDP)/IP
 - Used by PROFINET CBA and PROFINET IO
 - Configuration downloads, diagnostics, management
 - Non time critical status information

- Port 34964 UDP/TCP for PROFINET Context Manager
- Port 34962 UDP/TCP for PROFINET IO Unicast
- Port 34963 UDP/TCP for PROFINET IO Multicast
- Context manager creates and manages communication relationships



PROFINET IO – Communication Channels

- PROFINET RT (Real Time or Soft Real-Time)
 - Cycle times of typically 10ms
 - Removed TCP(UDP)/IP header
 - 802.1Q tagged L2 Frame, **VLAN ID = 0**
 - Primarily PROFINET IO, some PROFINET CBA
 - Control traffic, time critical alarms and messaging



PROFINET IO – Communication Channels

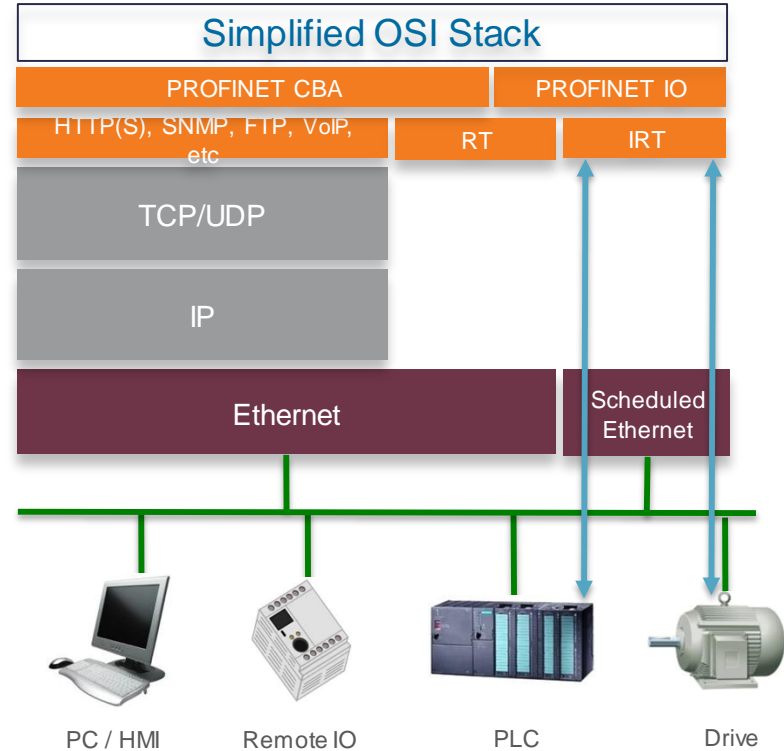
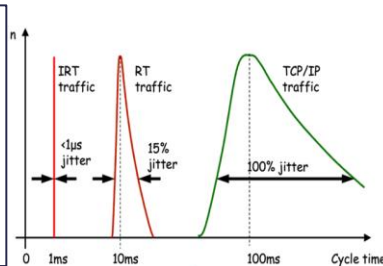
- PROFINET IRT (Isochronous Real-Time)
 - Cycle times of up to 1ms with less than 1µs jitter
 - All device clock/bus cycles synchronised
 - Standard L2 Frame
 - Uses IEEE 1588 PTP – with non-standard extensions
 - Requires **proprietary** ASIC and FPGA!
 - PROFINET IO for complex motion control traffic
 - Niche applications - <5% typically in a factory/plant
 - Not supported by Cisco switches

Definition:
Isochronal or **isochronous** (ahy-sok-ruh-nuhs)

-adj

1. Having the same time duration; equal in time
2. Occurring at equal time intervals; having a uniform period of vibration or oscillation

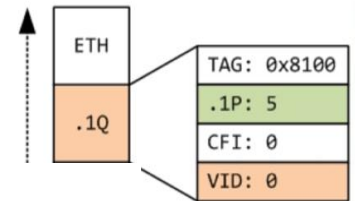
[From Greek isokhronos, iso + khronos time]



Cisco *live!*

Cisco PROFINET Considerations

- PROFINET uses GSD file (General Station Description) to describe functions of field devices.
- GSD files are pre-installed and configured on Cisco IE switch flash
- PROFINET uses 802.1p to prioritise frames
 - Ensure L2 QoS is enabled on the switch
- Be aware of how we handle 802.1Q tag with:
 - VLAN ID = 0
 - PCP (COS) = 6
- Depending on switch ASIC, VLAN 0 handled differently:
 - Legacy 2950/3550 – Accepted on access port, retagged
 - 2960/3560/3750/3850/IE3010 – Dropped on access port
 - On IE2000/IE3000 – Dropped – UNLESS!
 - Enable “profinet vlan <xxx>” command
 - IE4000 – Accepted
 - PROFINET enabled on VLAN 1 by default



Cisco PROFINET Considerations

- On 2960/3560/3750/3850 (IE3010) Switches

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



- On IE2000/IE3000 Switch

```
profinet vlan xxx

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





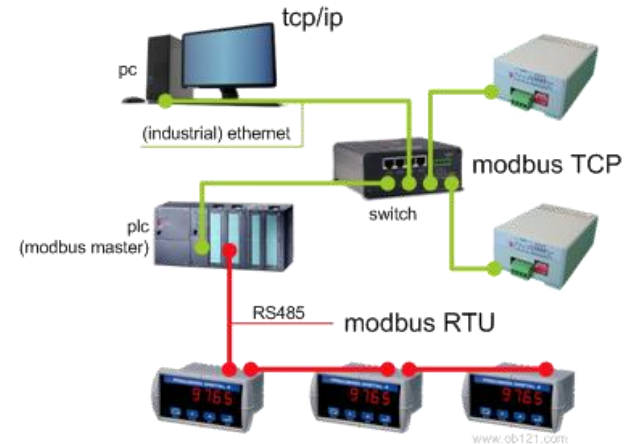
ModbusTCP

Modbus - History

- Modicon (Schneider Electric) introduced ModbusRTU in 1979
- Development managed by Modbus Organisation since 2004
- **Master-slave/client-server**. RS485 multi-drop network
- ModbusRTU/ASCII – Simple frame format: address, function, data
- ModbusTCP – Same frame format **over TCP/IP, Port 502**
- Truly open and royalty free. Widely deployed.
 - Simplicity lends itself to
 - Building automation
 - Simple telemetry
 - Low bit rate applications – e.g. O&G telemetry over UHF/VHF radio
- Hundreds of vendors. Thousands of devices.
- It's the **Babel Fish** of the industrial world.
- Not designed for complex motion, I/O or Safety applications



Modbus TCP frame format		
Name	Length (bytes)	Function
Transaction identifier	2	For synchronization between messages of server & client
Protocol identifier	2	Zero for Modbus/TCP
Length field	2	Number of remaining bytes in this frame
Unit identifier	1	Slave address (255 if not used)
Function code	1	Function codes as in other variants
Data bytes	n	Data as response or commands



CiscoLive!

Cisco ModbusTCP Considerations

- Cisco Connected Grid Products (CGR, CGS) allow ModbusTCP client to read certain information – Known as registers. E.g. IOS version, port statistics, etc.
- Cannot **write** to any registers (i.e. make changes!)
- Enabling Modbus Server
 - `Switch(config)#scada modbus tcp server <port>`
- Changing default number of connections (default = 1)
 - `Switch(config)#scada modbus tcp server <connection>`
- Show commands for Modbus Server and Client connections
 - `Switch#show scada modbus tcp server <connections>`

Agenda

- Industry Trends
- **Industrial Networking**
 - A Quick 101 Guide
 - Applications and Protocols
 - **Products and Architectures**
 - Availability and Resilience
 - Security: Using EEM
- Q&A
- Recommended Resources



Cisco Internet of Things Portfolio



Manufacturing



Mining



Energy-Utility



Oil and Gas



Transportation



City



Defence



SP/M2M

Plantwide Ethernet, Intelligent Transportation, Smart Cities, S&C Refinery, Smart Connected Vehicle, Smart Grid

IE 2000
IE 3000
CGS 1000
CGS 2500



Plant Switching

CGR 2000



ASR 903

Plant Routing



1552
Rugged
Wireless

CGR 1000



819H M2M ISR
Gateway
Router

Field Network

5915/5921/
5940 Rugged
Embedded
Services Routers



ESS2020
Rugged Switch



Embedded Networks

Video
Surveillance
Manager and IP
Cameras



Physical
Access
Manager



IPICS

Physical Security

Network Management and IoT Security

Fog Computing; Cisco IOx

Data Centre/Virtualisation

Industrial Compliance



General Specifications

Safety And Hazard	<ul style="list-style-type: none"> • UL/CSA 60950-1 • EN60950-1 • CB to IEC 60950-1 • NOM to NOM-019-SCF1 • CE Marking
	<ul style="list-style-type: none"> • ANSI/ISA 12.12.01 (Class 1, Div 2 A-D) • IEC 60079-0, -15 (Class1, Zone 2 A-D) • EN 60079-0, -15 ATEX certification (Class I, Zone 2 A-D)*
EMC	<ul style="list-style-type: none"> • FCC, IEC/EN 61000-4, RoHS, World wide EMC
Shock and Vibration	<ul style="list-style-type: none"> • IEC 60068-2-27 (Operational Shock: 30G 11ms, half sine) • IEC 60068-2-27 (Non-Operational Shock 55-75G, trapezoidal) • IEC 60068-2-6, IEC 60068-2-64 (Operational Vibration 2g@10-500Hz) • IEC 60068-2-6, IEC 60068-2-64 (Non-operational Vibration)
	<ul style="list-style-type: none"> • Storage altitude: 15,000 ft (4,570 m)
Relative Humidity	<ul style="list-style-type: none"> • IEC 60068-52-2 (salt Fog Mist, Test Kb) Marine environments • IEC 60068-2-3 • IEC 60068-2-30 • Relative Humidity of 5% or 95% Non-condensing

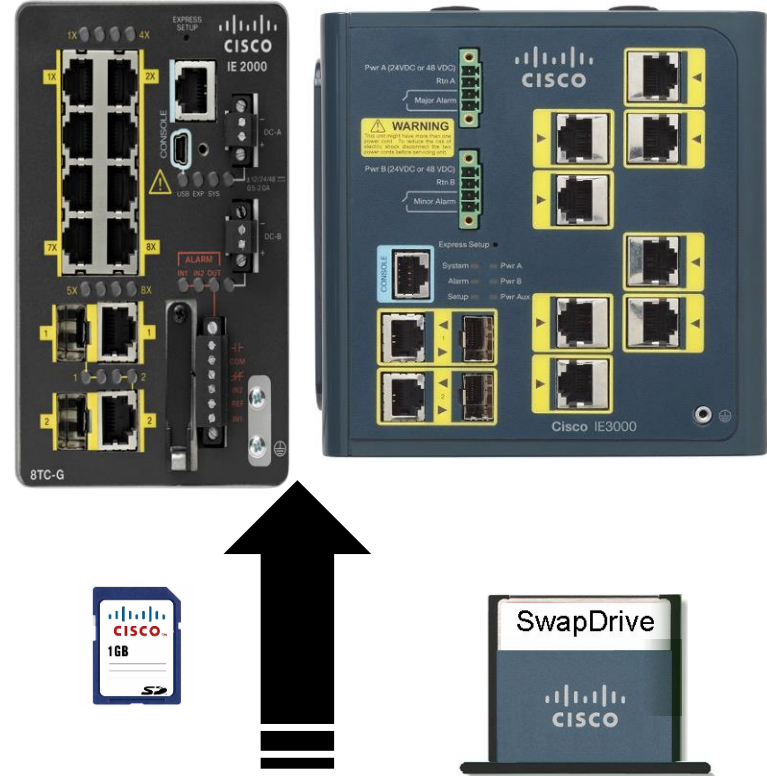
Industry Specific

- UL 508
- CSA C22.2 No.142
- EN 61131-2 (Programmable Controllers)
- Protective Coating
- Substation (IEEE 1613, IEC 61850-3) KEMA
- Marine (DNV)
- Railway EN 50155
- NEMA TS-2
- ODVA Industrial EtherNet/IP
- PROFINETv2
- ISO-12944-6
- IEC-60068-2-6



IE SwapDrive

- “Zero-config” replacement
 - Simple switch replacement in case of a failure
 - No networking expertise required
 - IE SwapDrive ensures fast recovery
- Files stored on the SwapDrive
 - IOS Image – (tar, html) – 2 sets
 - Config text
 - VLAN dat
 - Other devices configs



Cisco live!

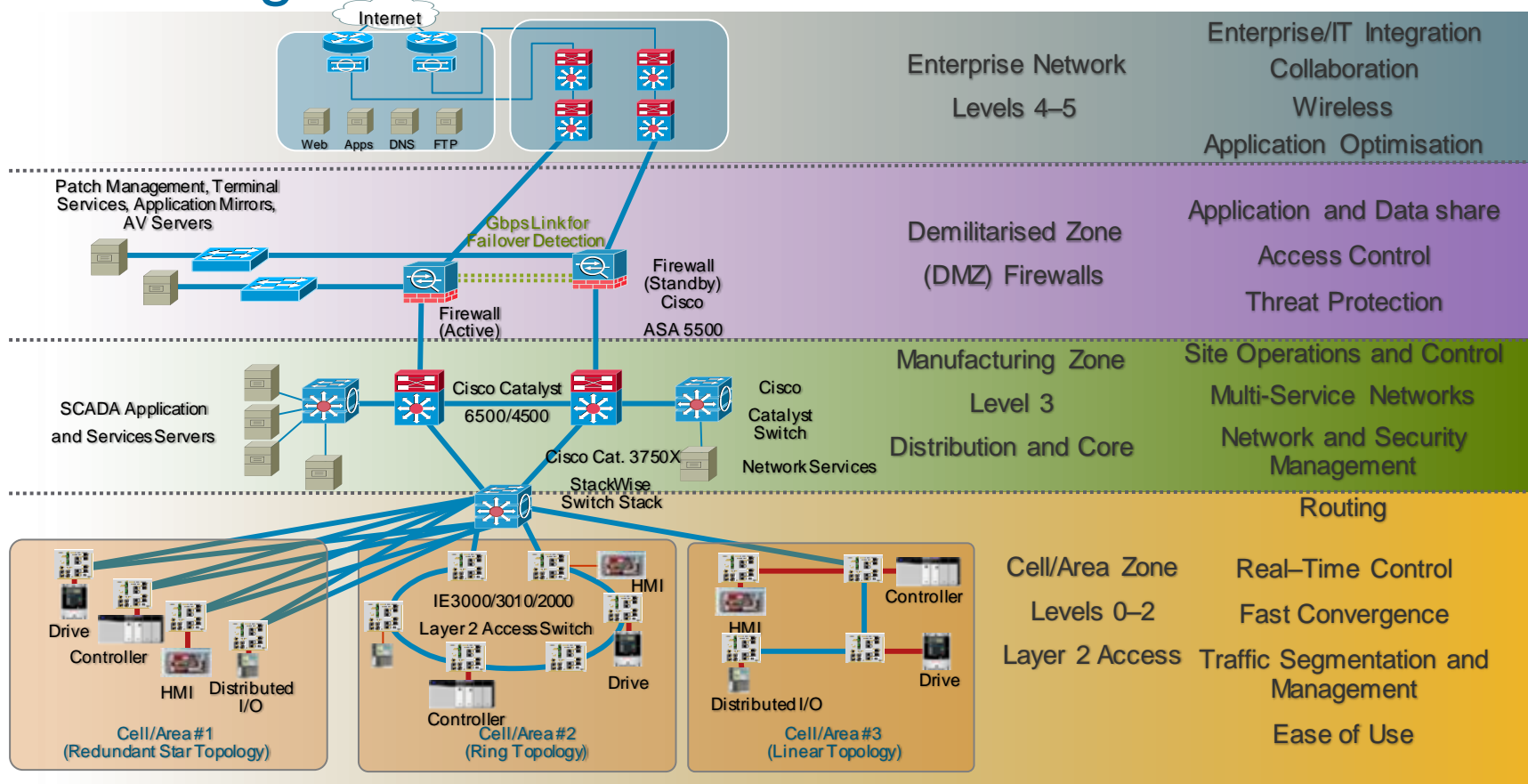
Device Manager – Direct Web Management





Wired

Converged Plant-wide Ethernet Architecture



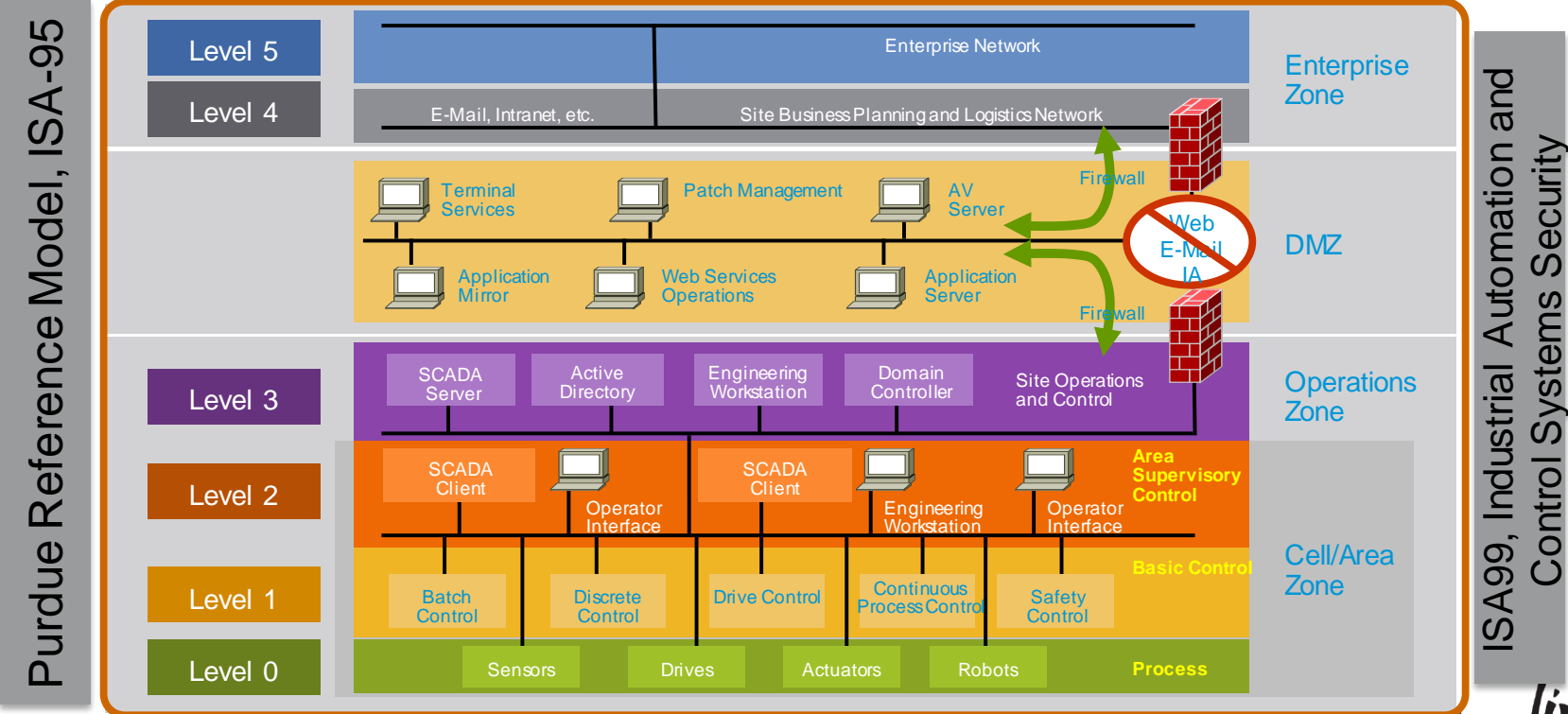
Built on Industry Standards

Purdue Reference Model, ISA95

Enterprise Zone	Enterprise Network	Level 5
	Site Business Planning and Logistics Network	Level 4
DMZ	Demilitarised Zone— Shared Access	
Manufacturing Zone	Site Manufacturing Operations and Control	Level 3
Cell/Area Zone	Area Control	Level 2
	Basic Control	Level 1
	Process	Level 0

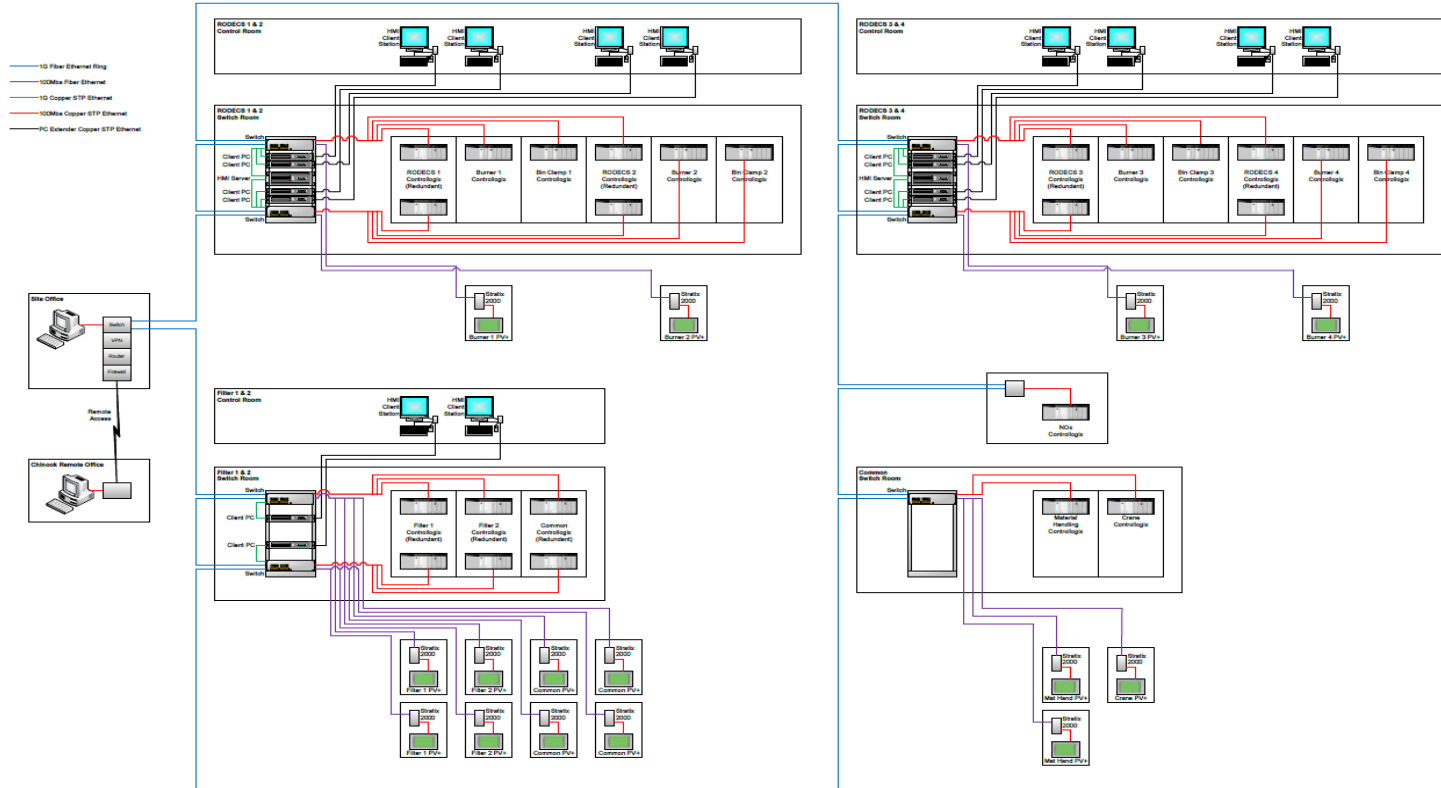
Security Framework, ISA99 / IEC 62443

Strong Segmentation



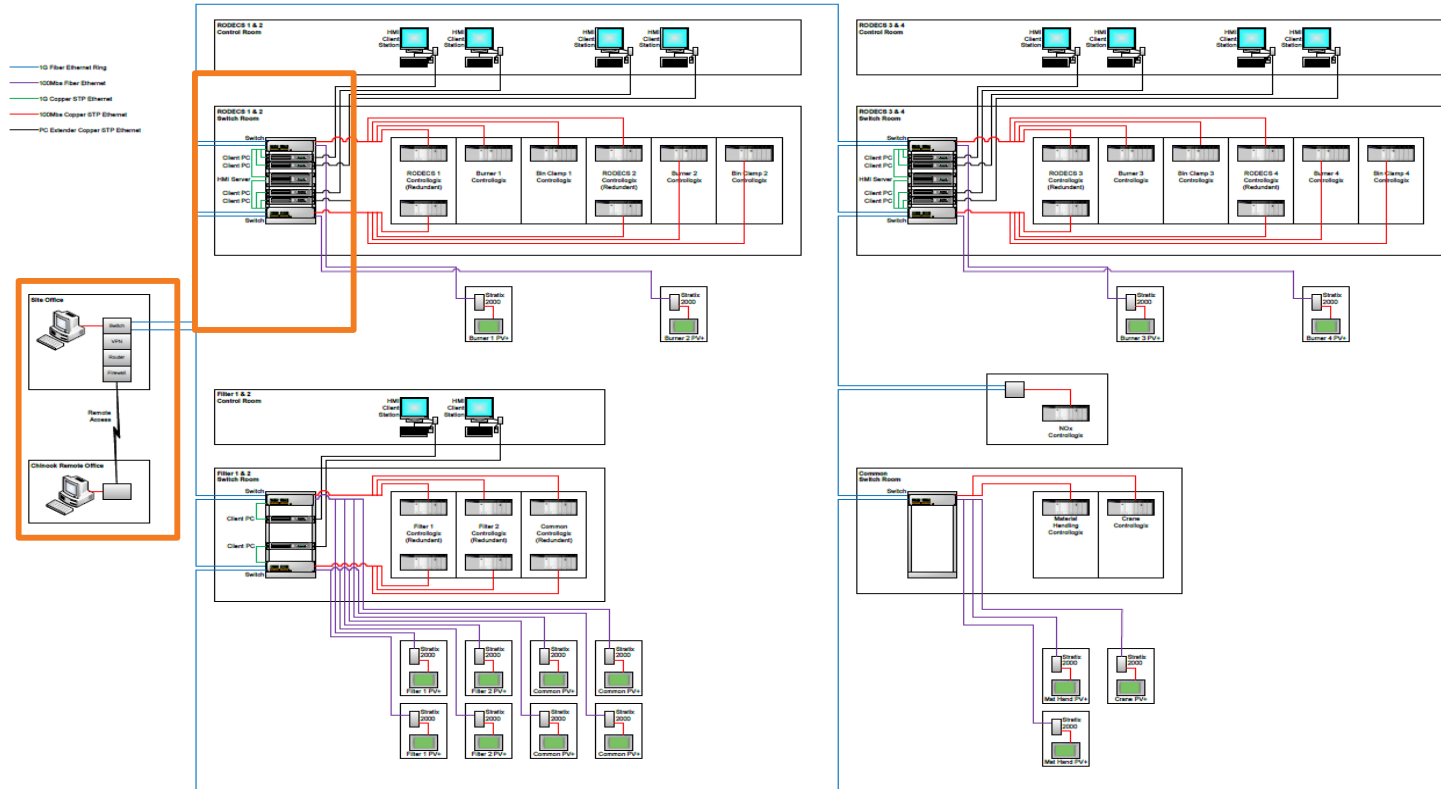
Ethernet and IP Automation Network Example

Material Recycling Plant Control System



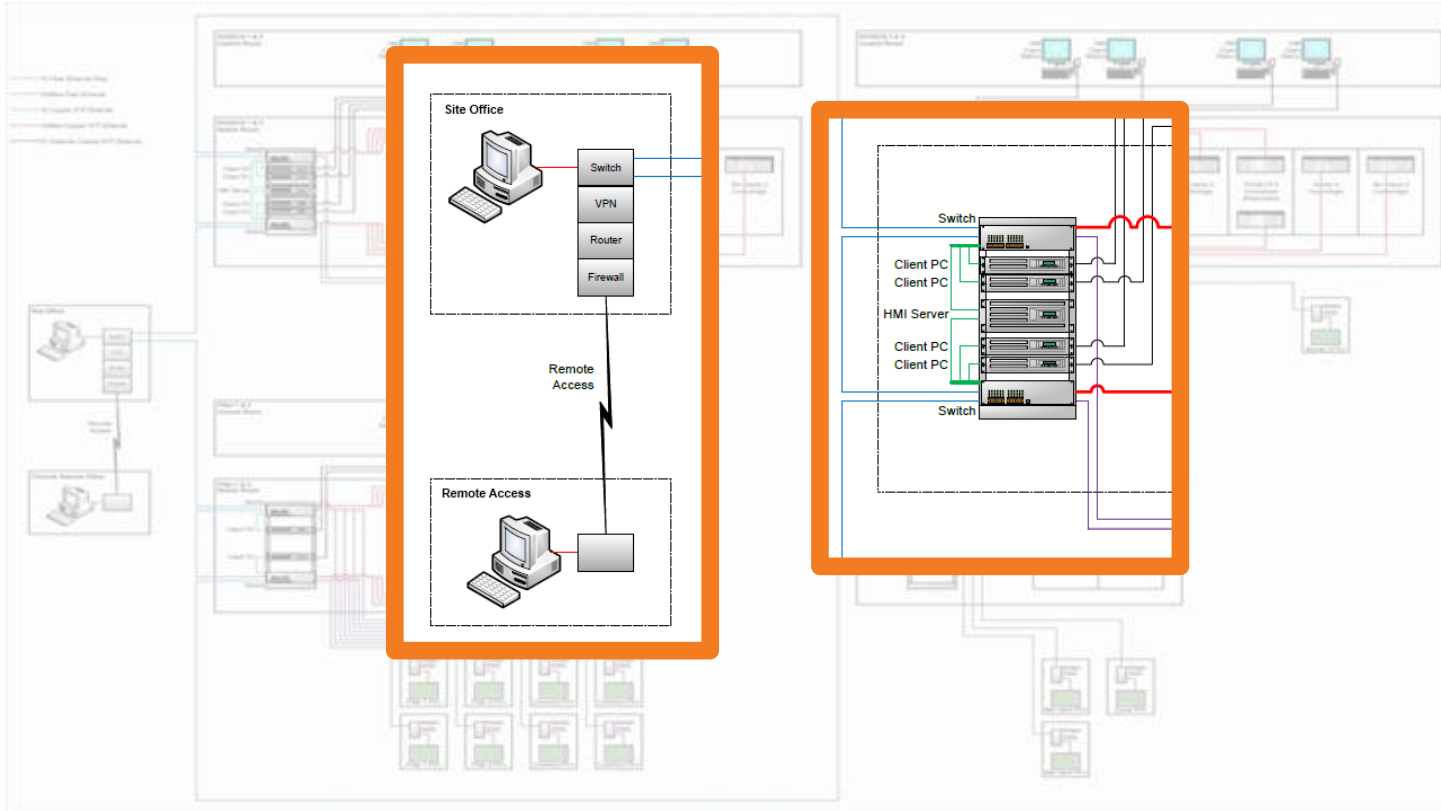
Ethernet and IP Automation Network Example

Material Recycling Plant Control System



Ethernet and IP Automation Network Example

Material Recycling Plant Control System





Wireless

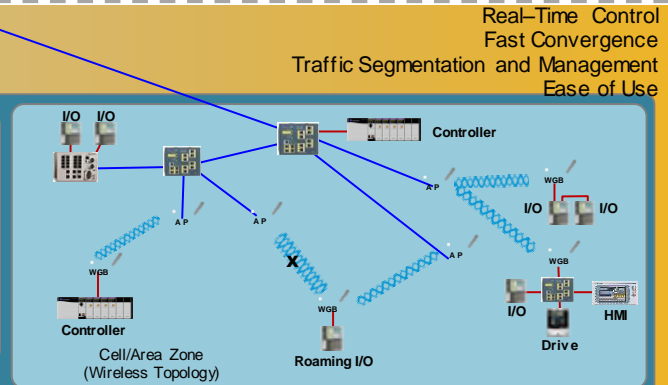
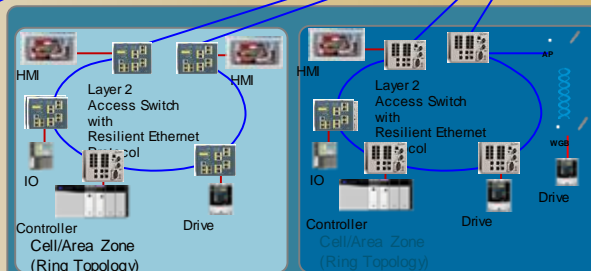
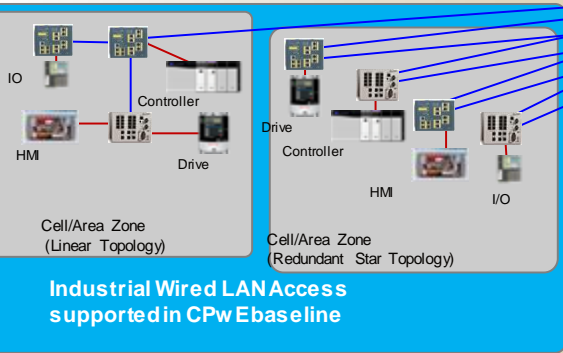
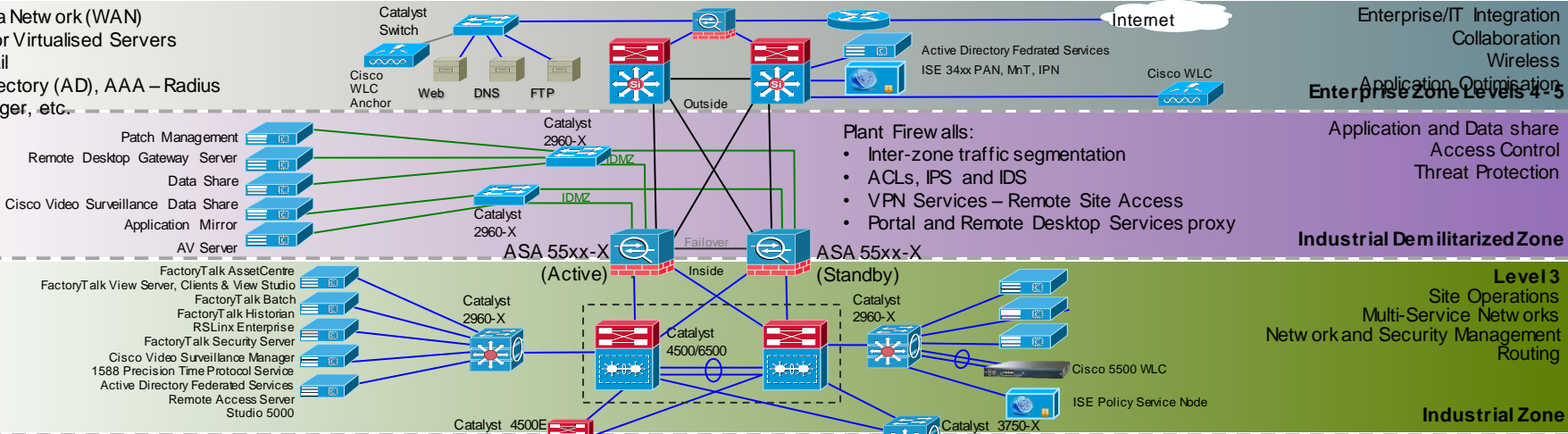
Advantages of Industrial Wireless

- Lower installation and operational costs
 - Cabling and hardware reduction
 - Eliminating cable failures on rotating/moving machinery
- Connection to hard-to-reach and restricted areas
- Equipment mobility
 - New and more efficient applications
 - Personnel mobility
 - Higher productivity and less downtime



CPwE 3.5 Overall Architecture with Wireless

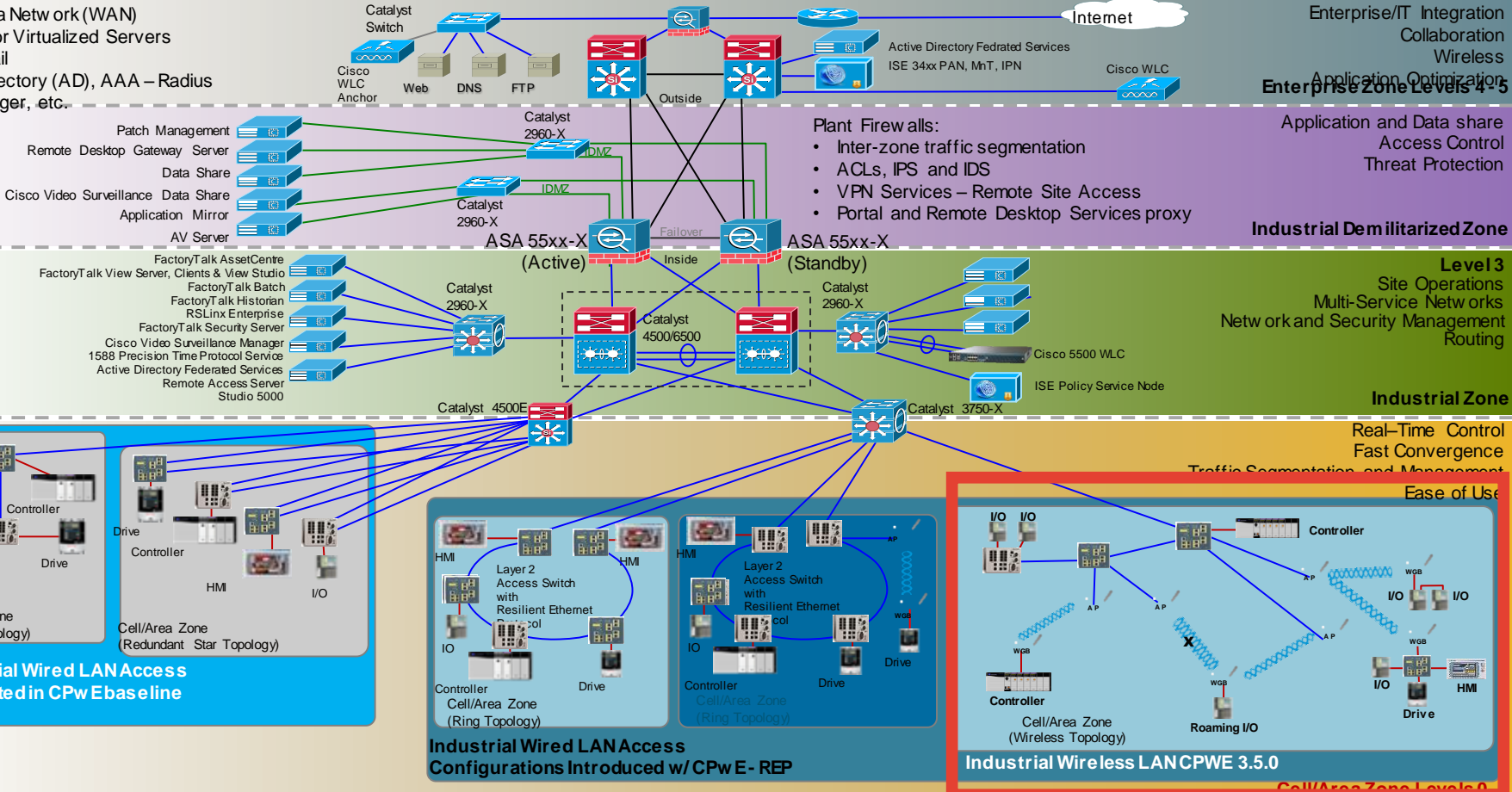
- Wide Area Network (WAN)
- Physical or Virtualised Servers
- ERP, Email
- Active Directory (AD), AAA – Radius
- Call Manager, etc.



- Real-Time Control
- Fast Convergence
- Traffic Segmentation and Management
- Ease of Use

CPwE 3.5 Overall Architecture with Wireless

- Wide Area Network (WAN)
- Physical or Virtualized Servers
- ERP, Email
- Active Directory (AD), AAA – Radius
- Call Manager, etc.



Industrial Wired LAN Access Configurations Introduced w/ CPwE - REP

Industrial Wireless LAN CPwE 3.5.0

Cell/Area Zone Levels 4 & 5

Wireless Overview

Challenges

- Half-duplex shared medium
 - Only one device can transmit at a time
- Wireless coverage area cannot be precisely defined
 - Site survey is required
 - Signal may reach beyond the intended area
- Signal quality may change over time
 - Interference sources and obstructions
- Higher latency and packet loss compared to wired Ethernet



Technology Overview

Choosing the Right Wireless Architecture

Unified WLAN Architecture

- Large number of APs (>10)
- Plant-wide coverage
- Existing infrastructure, IT practices and security policies that call for Unified architecture
- Applications that **require fast wireless roaming**
- WLAN is managed jointly by IT and control engineers – greater level of expertise

Autonomous WLAN Architecture

- Small number of APs (<10)
- Larger number of WGBs per AP
- Stand-alone applications
- Applications with no roaming
- WLAN is integrated into a stand-alone OEM machine and delivered to a plant
- WLAN is managed mostly by control engineers – lower level of expertise
- Lower initial cost

RF Design Recommendations

- RF survey is **critical**. **Prolonged** monitoring required.
- 5 GHz frequency band is recommended
 - 2.4 GHz band: 3 channels in U.S. (1, 6, 11)
 - 5 GHz band: based on regulatory domain
- Avoid DFS channels (Dynamic Frequency Selection)
 - Use channels 36-48 or 149-165 (if available)
 - Weather / military radars cause disruption of service in other channels
 - If DFS channels are used, RF monitoring is required
- Reserve a channel exclusively if possible
- Use static channel assignment
- Do not reuse channels for critical applications unless complete signal separation can be reliably achieved

Country examples	5 GHz Channels	
	No DFS	DFS
U.S., Canada, Australia	9	12
Europe	4	15
China	5	0

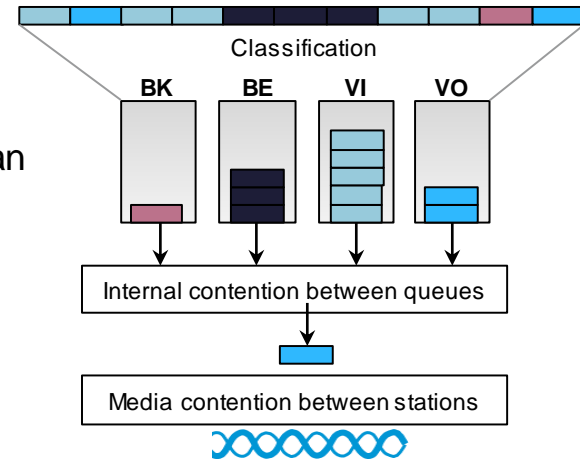
Just an example: free space signal propagation	
Radio sensitivity	-85 dBm
Transmit power	5 dBm
Tx / Rx antenna gain	4 dBi
Re-use distance (5180 MHz)	350 meters

WLAN Design Considerations

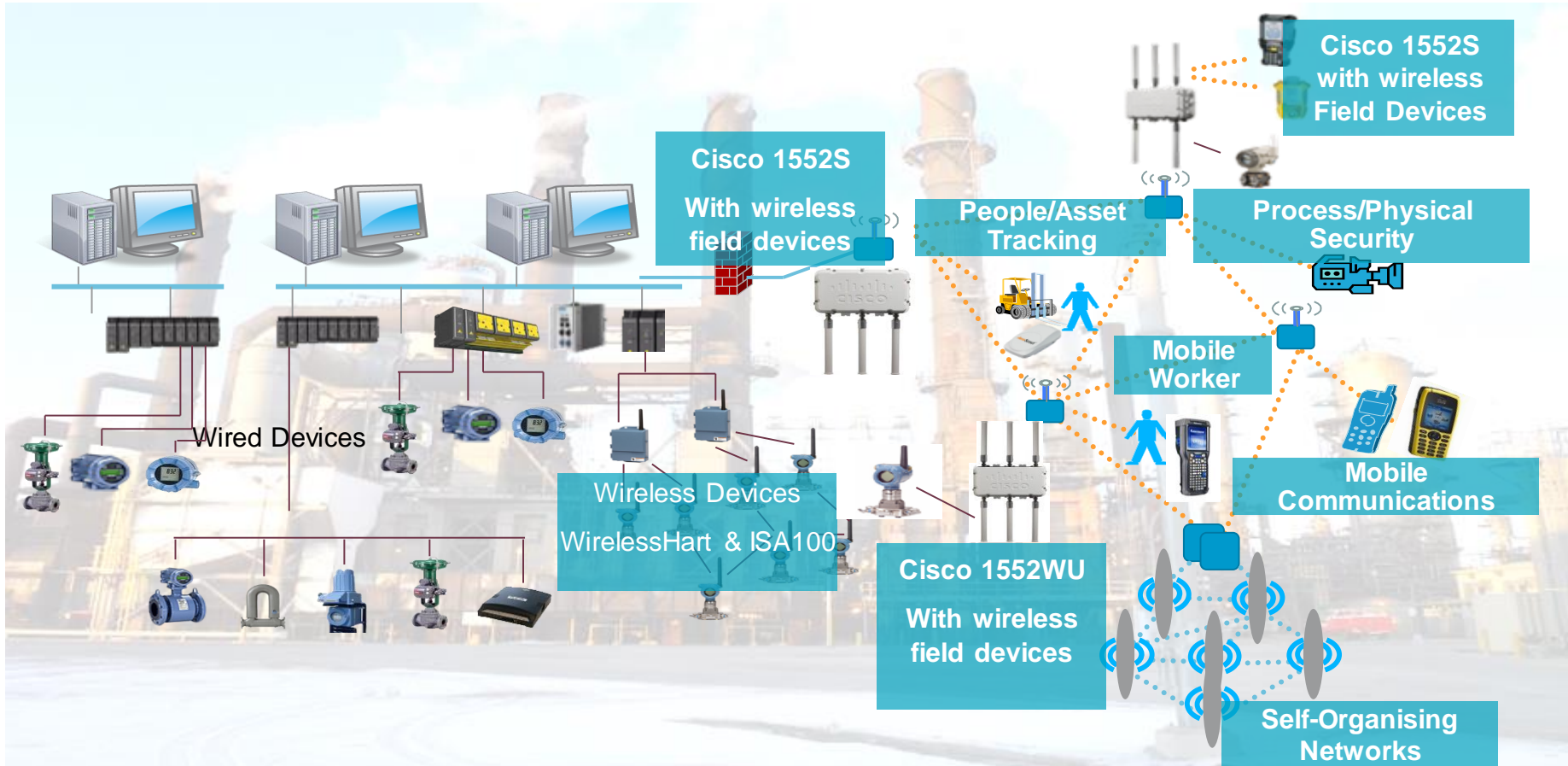
QoS Recommendations

- 802.11 uses statistical QoS to give preference to certain classes of traffic
 - Still half-duplex media: cannot transmit while someone is using the channel
- Autonomous Mode
 - Traffic is placed into queues based on selected criteria
 - DSCP (L3 QoS) is recommended where TCP/UDP port numbers can be used
 - Transmission parameters are adjusted for each queue
 - Backoff time, number of retries, packet timeout
- Unified Mode
 - Transmission parameters are fixed for each queue
 - Use **Platinum** Setting for best performance

Traffic Type	DSCP	Queue
PTP event	59	Voice
PTP management	47	Video
CIP class 0 / 1 (I/O, P/C, Safety, Motion)	55	
	47	
	43	
	31	
CIP class 3 (MSG, HMI)	27	Best Effort
Unclassified	0	



Industrial Wireless Access with Cisco MESH



Agenda

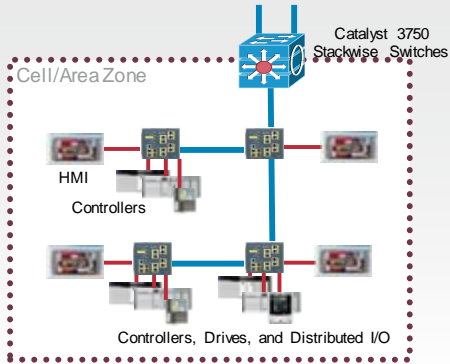
- Industry Trends
- **Industrial Networking**
 - A Quick 101 Guide
 - Applications and Protocols
 - Products and Architectures: Wired and Wireless
 - **Availability and Resilience: REP, MRP, QoS**
 - Security: Using EEM
- Q&A
- Recommended Resources



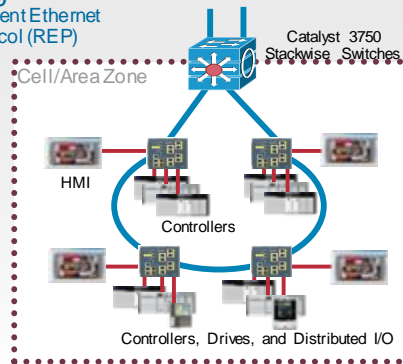
Industrial Network Topologies

Cell/Area Zone Topology Options

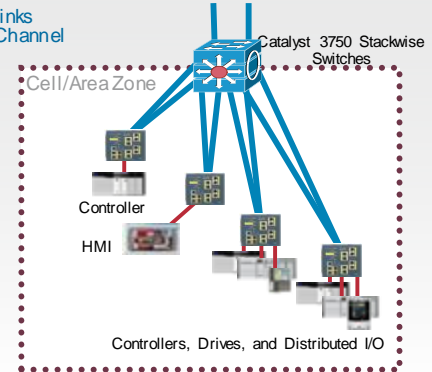
Star/Bus Linear



Ring
Resilient Ethernet Protocol (REP)






Redundant Star
Flex Links
EtherChannel



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

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	<5 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, palletizing, 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 < 10 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
MRP (IEC 62439-2)	X	X		X	X			X
Flex Links			X		X			X
PRP/HSR (IEC xxx)	X	X	X			X		X
DLR (IEC & ODVA)	X	X				X		X
StackWise		X	X	X			X	X
HSRP		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 < 0~10 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
MRP (IEC 62439-2)	X	X		X	X			X
Flex Links			X		X			X
PRP/HSR (IEC 62439)	X	X	X			X		X
DLR (IEC & ODVA)	X	X				X		X
StackWise		X	X	X			X	X
HSRP		X	X	X			X	
VRRP (IETF RFC 3768)	X	X	X	X			X	

← Process and Information

← Time Critical

← Loss Critical

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 < 0~10 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
MRP (IEC 62439-2)	X	X		X	X			X
Flex Links			X		X			X
PRP/HSR (IEC 62439)	X	X	X		X	X		X
DLR (IEC & ODVA)	X	X				X		X
StackWise		X	X	X			X	X
HSRP		X	X	X			X	
VRRP (IETF RFC 3768)	X	X	X	X			X	

A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, modern buildings are illuminated with various lights, and a pedestrian bridge spans across the street. The overall scene is a dynamic urban environment.

REP - Resilient Ethernet Protocol

Resilient Ethernet Protocol

Benefits

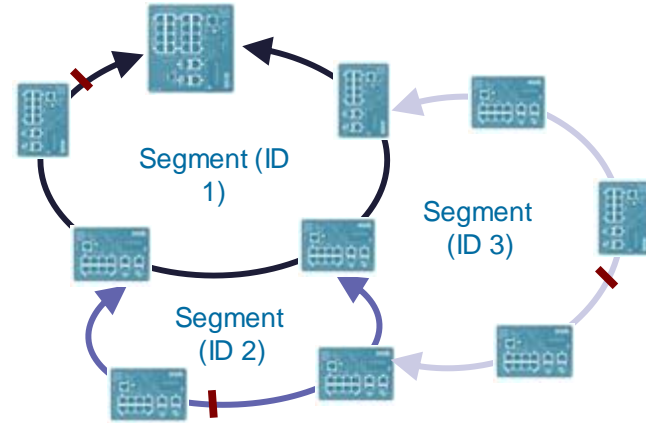
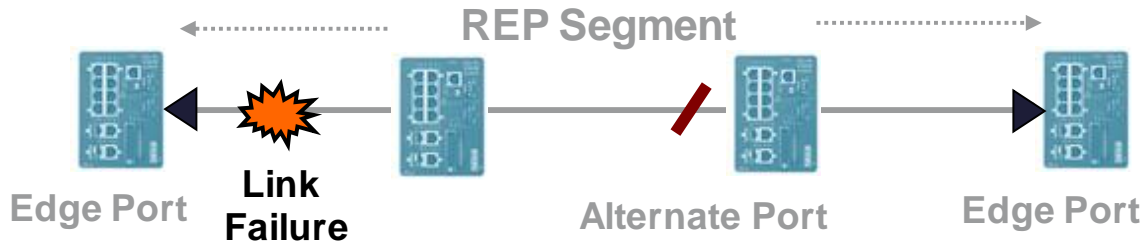
- Provides a **fast and predictable** L2 convergence (50ms - fibre) even in large rings with high number of nodes
- Supported on a large range of Cisco products, including all IE switches and CGR 2010 ESM
- Very easy to configure and troubleshoot
- Co-existence with Spanning Tree (TCN from REP to STP)
- Optimal bandwidth utilisation (VLAN Load balancing)

Limitations

- Does not replace Spanning Tree for complex layer 2 networks (mesh, tree)
- Cisco proprietary
- Supported on Layer 2 Trunk Ports and Etherchannel only
- Does not protect against dual failure in the ring

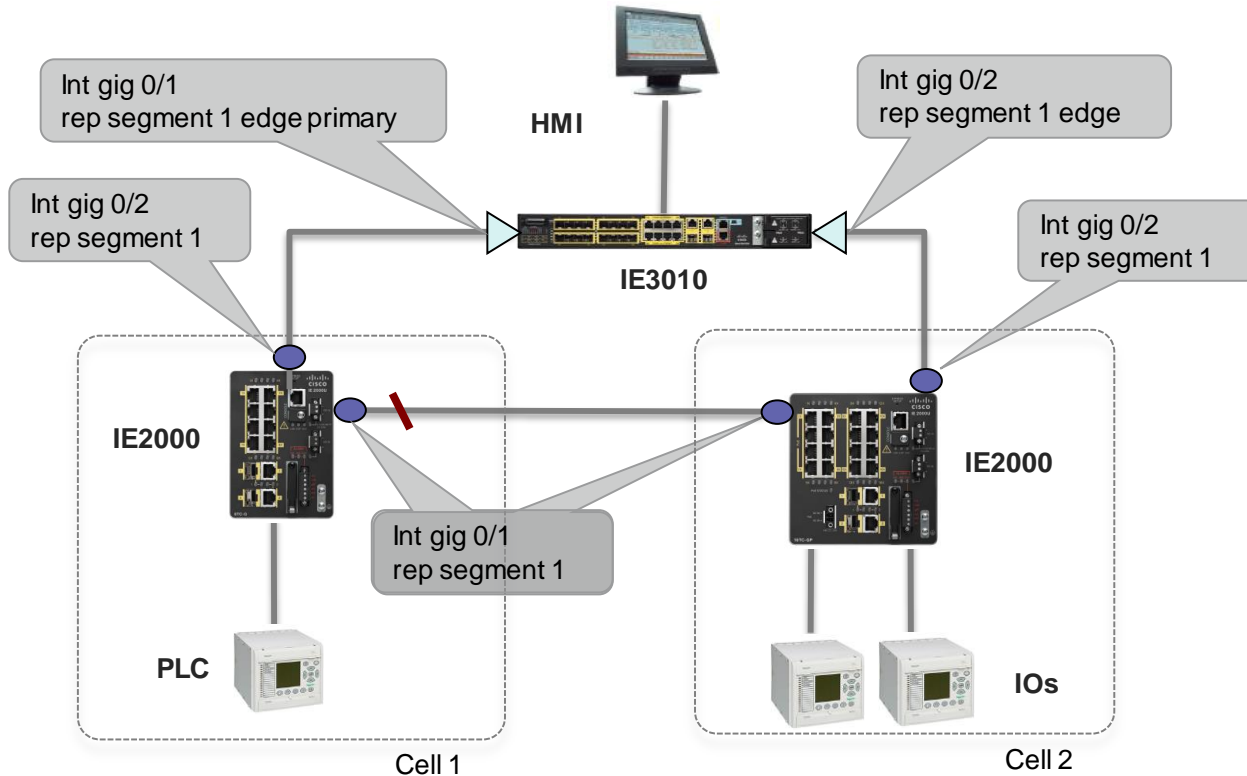
Resilient Ethernet Protocol

How it Works



- A REP **segment** is a **chain of ports** with the **same segment ID**. REP guarantees there is no connectivity between two edge ports on a segment
- The ports where the **segment terminates** is called the **Edge Ports**
- **Alternate** port blocks traffic to prevent loops. May be any interface in the REP ring
- When all interfaces in the segment are UP, the alternate port is blocking
- When a link or switch failure occurs, the blocked port goes forwarding

REP Segment 1 - Basic Configuration



*Trunk Port Configuration Mandatory before configuring REP

Show REP Topology Command

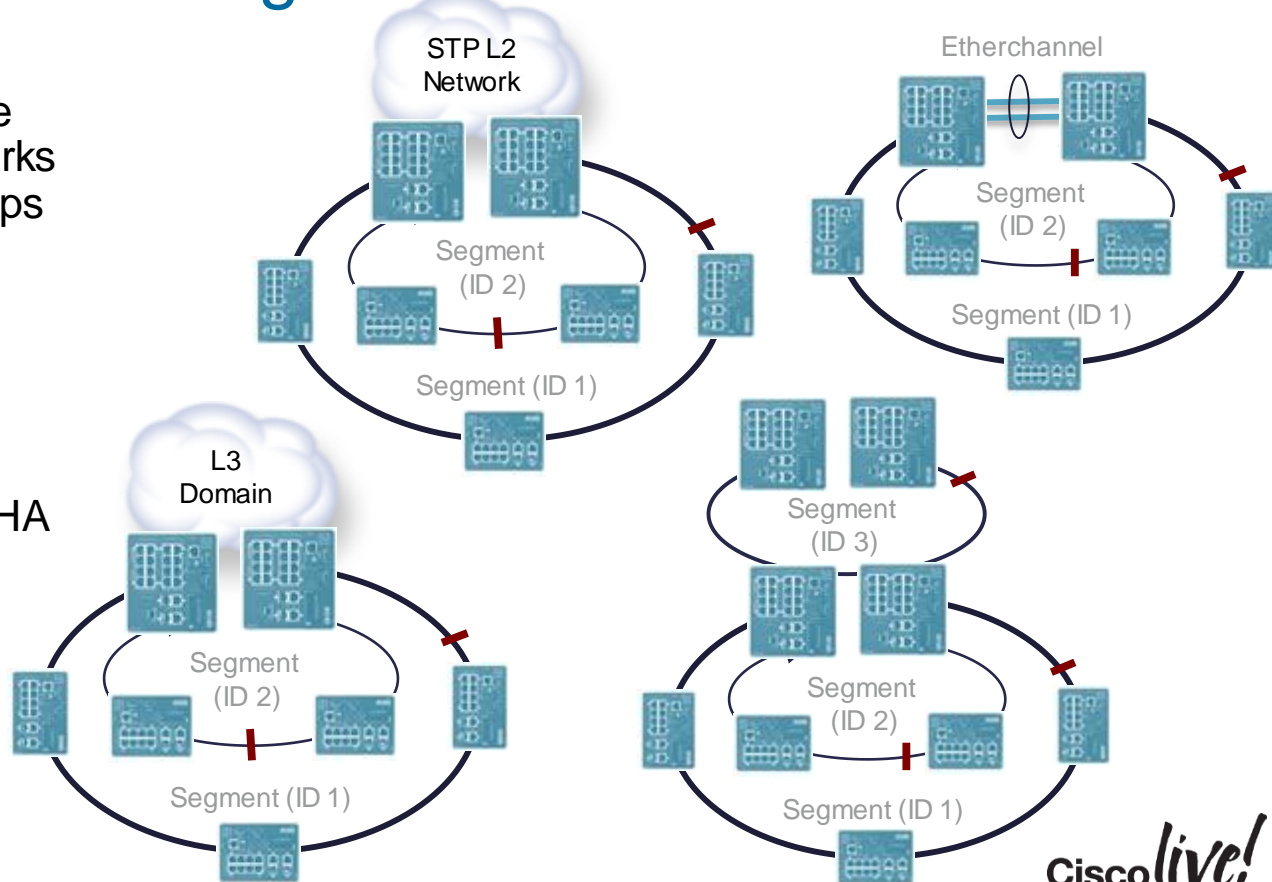
This is the primary edge port

This is the preferred alternate port blocking

```
IE-SWITCH-9# show rep topology
REP Segment 1
BridgeName          PortName    Edge Role
-----
IE-SWITCH-9         Gi0/2       Pri  Open
IE-SWITCH-10        Gi0/1                Open
IE-SWITCH-10        Gi0/2                Open
IE-SWITCH-11        Gi0/1                Open
IE-SWITCH-11        Gi0/2                Alt
IE-SWITCH-12        Gi0/1                Open
IE-SWITCH-12        Gi0/2                Open
IE-SWITCH-9         Gi0/1                Sec  Open
```

Connecting the REP Segments to the Core Network

- The segment edges can be connected to different networks without creating bridging loops
- The link between the edge nodes is the **common link**
- Options for Common Link HA are STP, Etherchannel, L3 Domain or REP



A nighttime photograph of a city street with light trails from cars. In the background, there are modern buildings and a pedestrian bridge. The foreground is dominated by long, curved light trails in yellow, orange, and red, suggesting a long exposure of traffic. The text is overlaid on a dark horizontal band across the middle of the image.

Parallel Redundancy Protocol High Availability Seamless Ring

Parallel Redundancy Protocol (PRP)

Benefits

- Provides zero packet loss convergence
- Supported on a large range of Cisco products.
- Very easy to configure and troubleshoot
- Co-existence with Spanning Tree, REP
Other high availability protocols
- Standards Based (IEC 62439-3)

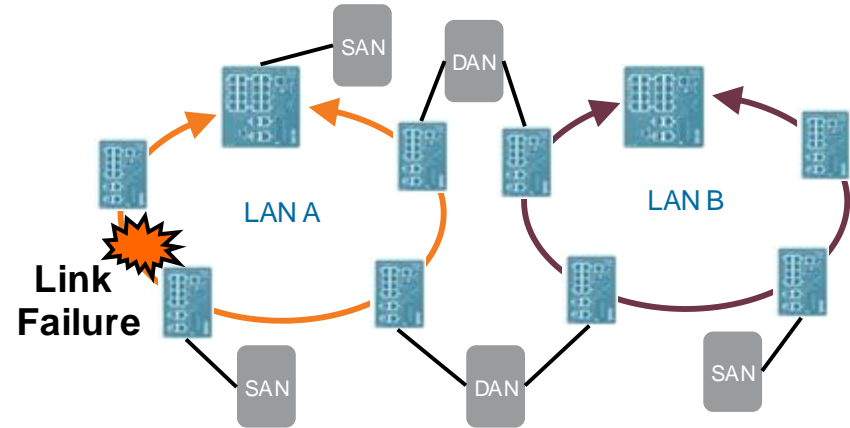
Limitations

- Additional Switching Infrastructure required.
- Additional hardware/software support required for some applications.

Parallel Redundancy Protocol

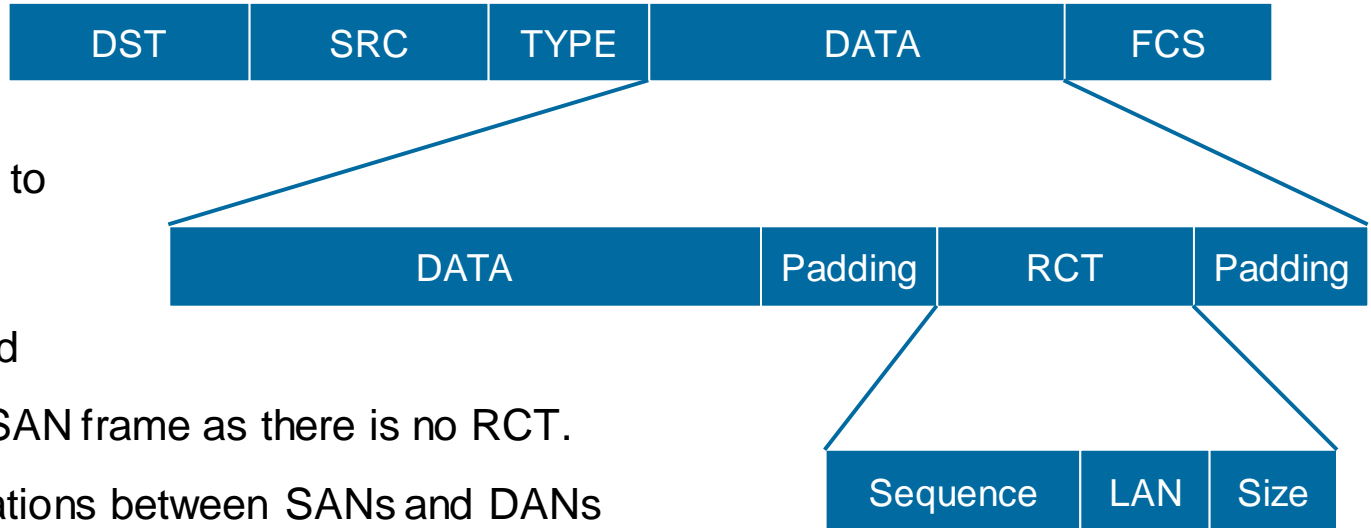
How it Works

- A PRP Network is effectively **two** similar LAN's.
- Arbitrary Topology
- PRP LANs can be different designs.
- DAN's are responsible for the duplication and de-duplication of packets onto both LANs
- De-duplication is done at Link Layer for efficiency
- STP/RSTP/REP etc can be used in conjunction with PRP.



Parallel Redundancy Protocol

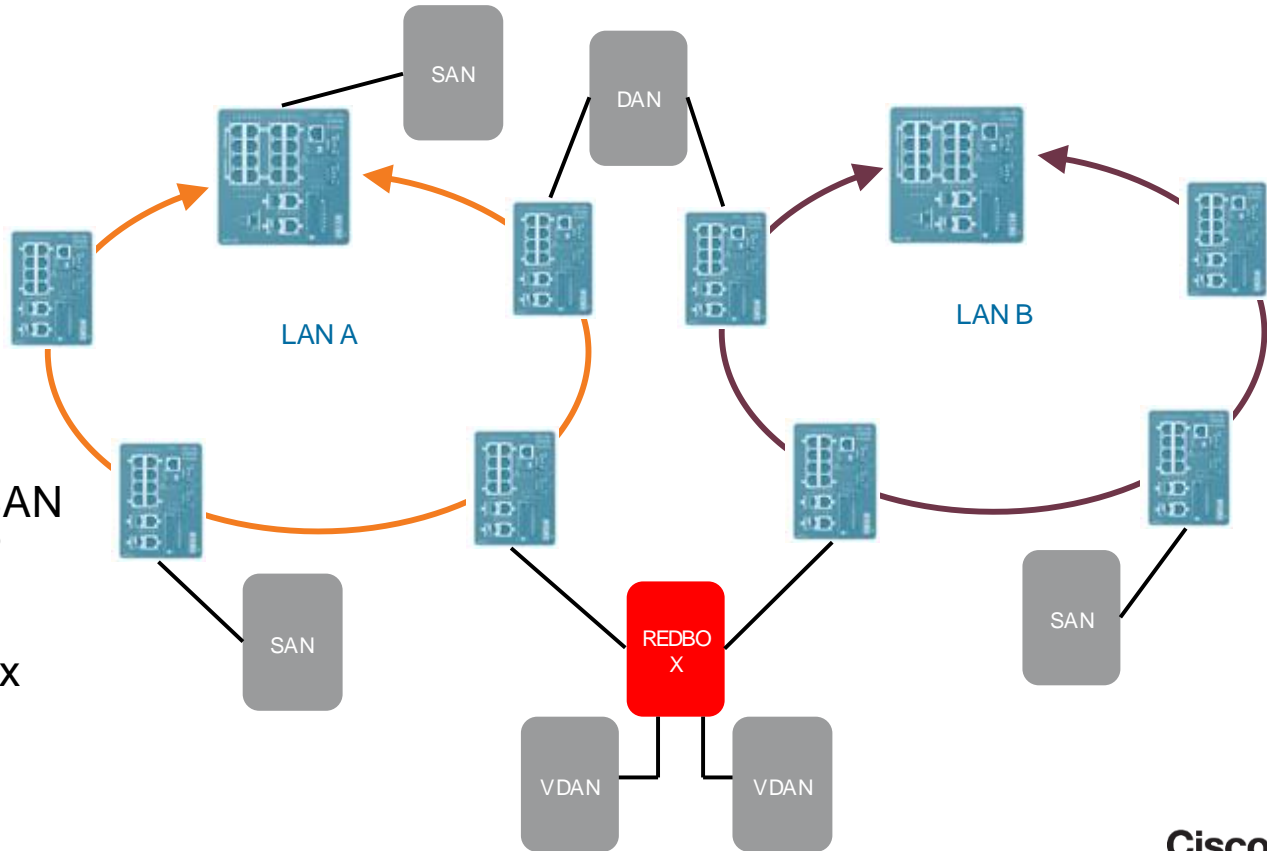
Frame Construct



- DANs append RCT to 802.3 padding
- SANs treat RCT as padding and discard
- DANs understand SAN frame as there is no RCT.
- Permits communications between SANs and DANs (ARP etc)

Parallel Redundancy Protocol

Redundancy Box



- REDBOX permits SAN connectivity to PRP network
- The redundancy box acts as a proxy for SAN.



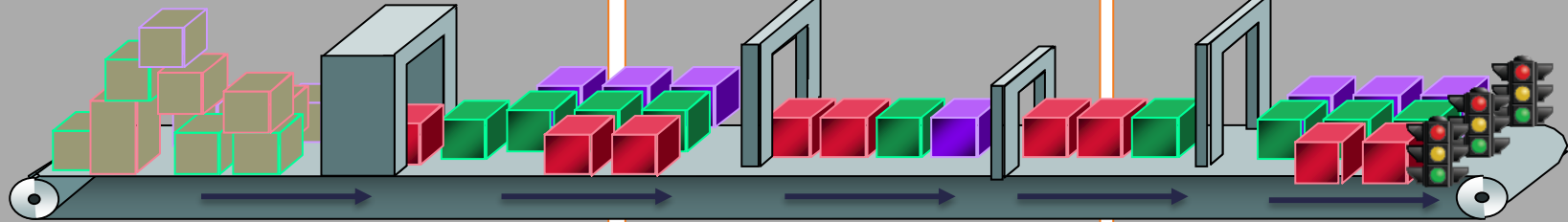
QoS

QoS 101

CLASSIFICATION

MARKING

PRIORITY QUEUING



Classification Is the Separation of Packets Into **Traffic Classes**

Classification Criteria:

- IP precedence
- Differentiated Services Code Point (DSCP)
- Access control list (ACL)
- Packet length
- Class map

Marking Is the a Method to Modify the **QoS Fields of the Outgoing Packets on L3 Interface**

QoS Fields to Be Marked:

- IP precedence
- Differentiated Services Code Point (DSCP)

Priority Queuing

1. **Highest priority:** This traffic is always sent first
2. **Medium priority:** This traffic is sent after priority 1 traffic and before priority 3 and 4 traffic
3. **Best effort priority** (default): This traffic is sent after priority 1 and 2 traffic and before priority 4 traffic
4. **Lowest priority:** Traffic always sent after all other packets in a queue with priority of 1, 2, or 3

Not All Traffic is Created Equal

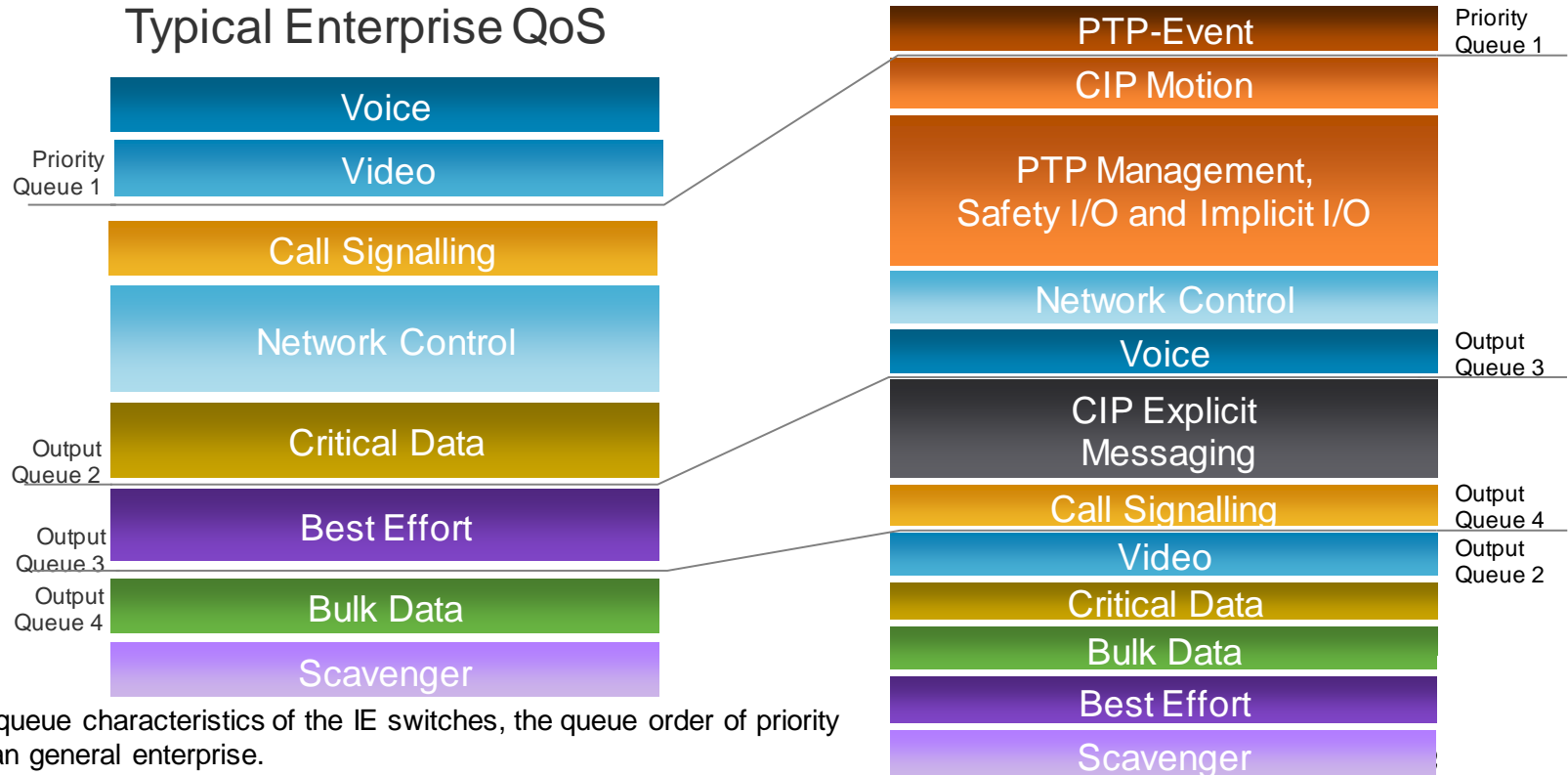
Prioritisation Is Required

	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 IE switches, the queue order of priority is different than general enterprise.

Agenda

- Industry Trends
- **Industrial Networking**
 - A Quick 101 Guide
 - Applications and Protocols
 - Products and Architectures
 - Availability and Resilience
 - **Security**
- Q&A
- Recommended Resources



A Renewed Focus on Security

The Problem with SCADA / DCS Runs Deep...

- An ICS-CERT advisor released Apr 14 identifies vulnerability on **Vendor X's** products

Source: osvdb.org; <https://ics-cert.us-cert.gov/advisories/ICSA-14-084-01>

A Renewed Focus on Security

The Problem with SCADA / DCS Runs Deep...

- An ICS-CERT advisor released Apr 14 identifies vulnerability on **Vendor X's** products
- Product has FTP backdoor allowing unauthenticated access allowing attacker to crash device and run arbitrary code.

Source: osvdb.org; <https://ics-cert.us-cert.gov/advisories/ICSA-14-084-01>

A Renewed Focus on Security

The Problem with SCADA / DCS Runs Deep...

- An ICS-CERT advisor released Apr 14 identifies vulnerability on **Vendor X's** products
- Product has FTP backdoor allowing unauthenticated access allowing attacker to crash device and run arbitrary code.
- From the advisory:

“

This product is used industrywide as a programmable logic controller with inclusion of a multiaxis controller for automated assembly and automated manufacturing. Identified customers are in solar cell manufacturing, automobile assembly, general assembly and parts control, and airframe manufacturing where tolerances are particularly critical to end product operations.

Source: [osvdb.org](https://osvdb.org;).; <https://ics-cert.us-cert.gov/advisories/ICSA-14-084-01>

A Renewed Focus on Security

The Problem with SCADA / DCS Runs Deep...

- And from the Mitigation section (paraphrased):

“

X has decided not to resolve these vulnerabilities, placing critical infrastructure asset owners using this product at risk ... because of compatibility reasons with existing engineering tools.

A Renewed Focus on Security

The Problem with SCADA / DCS Runs Deep...

- And from the Mitigation section (paraphrased):

“

X has decided not to resolve these vulnerabilities, placing critical infrastructure asset owners using this product at risk ... because of compatibility reasons with existing engineering tools.

- **Vendor X** manufactures **vulnerable critical components** that can directly impact safety and has chosen **not to fix them**

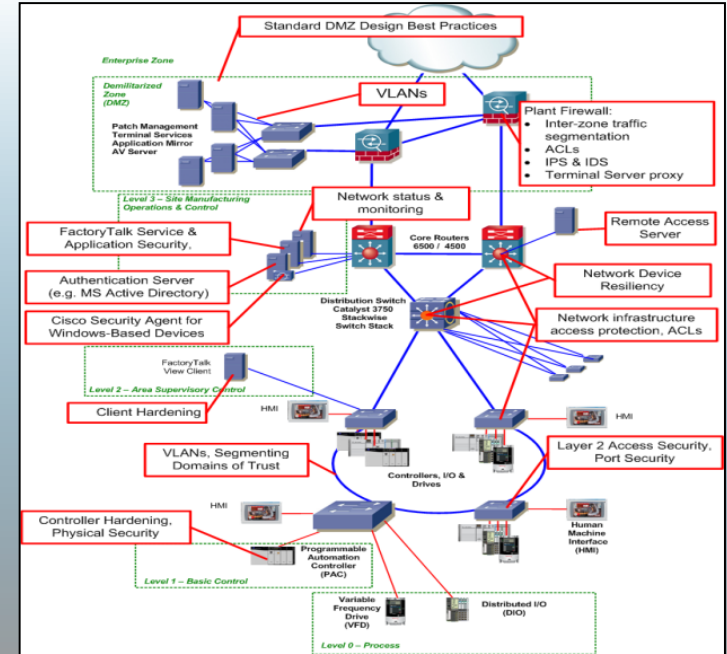
Staged Cyber-attack

Diesel Generator Control System



ISA99 / IEC 62443 Security Guidelines

- 8 Cisco members. Bring networking expertise
- Recommends
 - 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



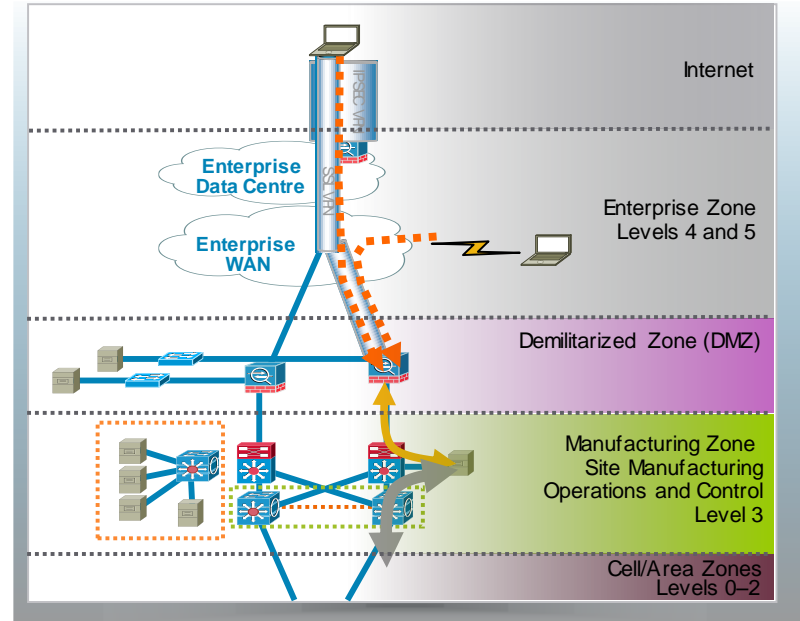
Setting the Standard for Automation™

The International Society of Automation is a nonprofit organization that helps its 30,000 worldwide members and other automation professionals solve difficult technical problems, while enhancing their leadership and personal career capabilities.

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 zone - the firewalls**

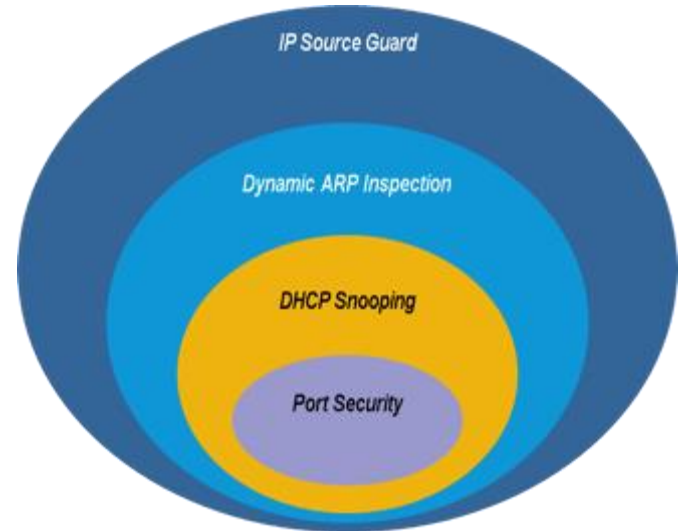


Protect the Interior

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)
 - StormControl
 - Rate Limiting
- Access Control Lists
- Identity Services Engine / TrustSec

CISF – Cisco Integrated Security Features



Cisco *live!*

A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with blue lighting spans across the street. In the background, there are several tall buildings with lit windows and some flags on poles. The overall scene is illuminated by city lights.

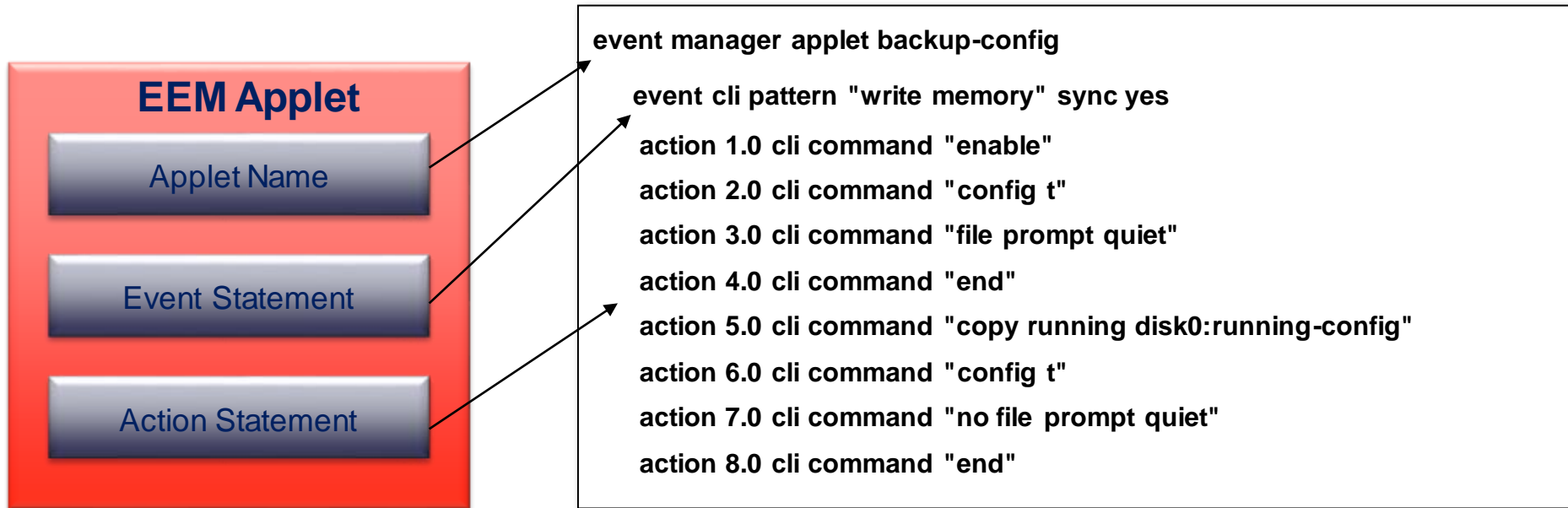
EEM – Embedded Event Manager

What is EEM and why use it?

- A flexible and powerful subsystem within Cisco IOS Software
- Detects and generates events when certain conditions are met in the network devices
- Triggers the execution of custom modules written in **CLI** or **TCL** script
- Adapt device behaviour and insert business logic without IOS upgrade
- Integrate with external systems via web services, syslog, SNMP
- Reduce “polling” for management data, send notifications instead

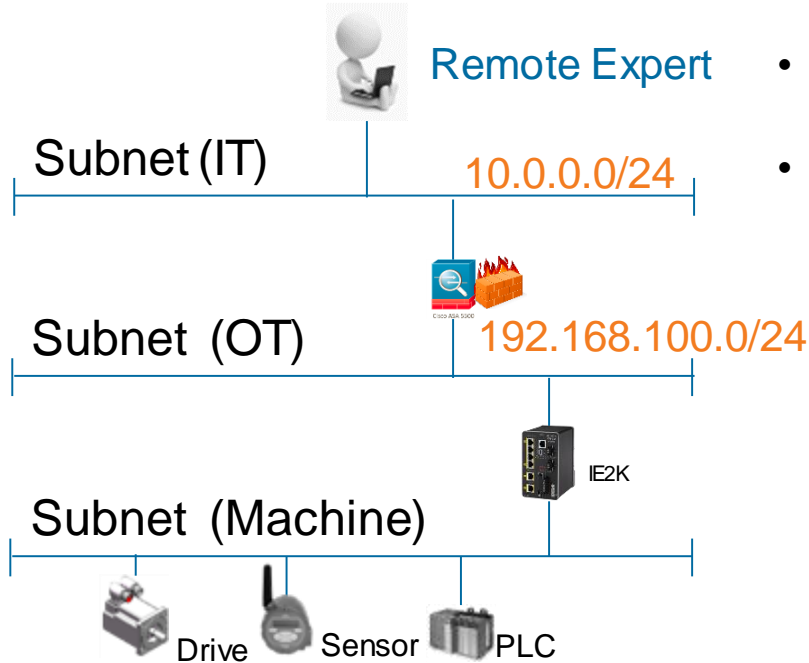
EEM CLI Applet Overview

An applet is defined at the CLI - once entered it becomes part of the configuration



Use Case: Key-Locked Remote Support

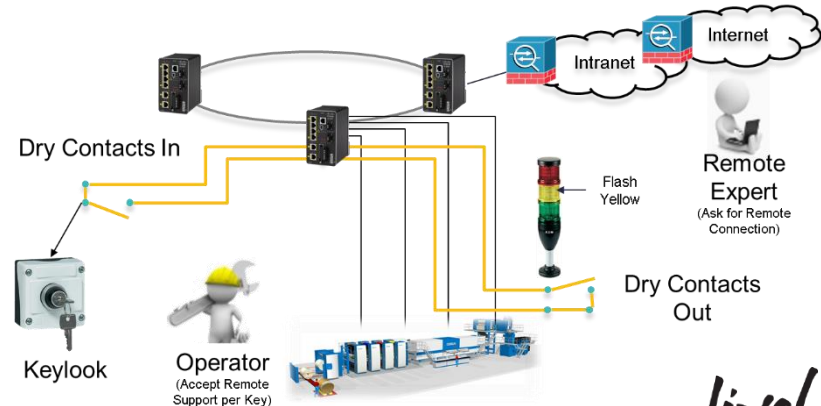
Logical View



Problem Statement

- Manufacturer needs a simplified solution to allow and deny remote support of a machine.
- Local engineer must authorise remote access with a hardware key.

Physical View



Use Case: Key Locked Remote Support

Step 1:



Employee asks for access to machine (Phone/E-Mail)



Step 2:



Key Unlock from operator on the machine
(Access List will be changed)



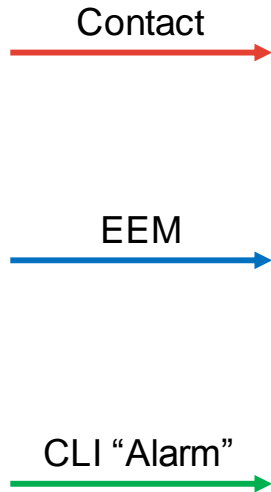
Step 3:



Employee gets access to the machine controller



EEM Logic Chart



Device	T0	T1	T2	T3
Switch ACL	Normal Operation			Remote Operation
Keylock	Open	Closed		
Switch Alarm-In	Off		On	

Transitions are indicated by arrows:

- A red arrow points from "Open" to "Closed" in the Keylock row.
- A green arrow points from "Closed" to "On" in the Switch Alarm-In row.
- A blue arrow points from "On" to "Remote Operation" in the Switch ACL row.

Use Relevant CLI

CLI “Alarm”

```
alarm facility input-alarm 1 relay major
```

EEM Applet

```
event manager applet remote_operation
event syslog pattern "%PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm asserted: external alarm contact 1"
action 1 cli command "enable"
action 2 cli command "conf t"
action 3 cli command "interface GigabitEthernet1/1"
action 4 cli command "ip access-group remote_operation in"
action 7 cli command "exit"
event manager applet normal_operation
event syslog pattern "%PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared: external alarm contact 1"
action 1 cli command "enable"
action 2 cli command "conf t"
action 3 cli command "interface GigabitEthernet1/1"
action 4 cli command "ip access-group normal_operation in"
action 7 cli command "exit"
```

CLI “ACL’s”

```
ip access-list extended normal_operation
permit ip 192.168.100.0 0.0.0.255 any
deny ip any any
ip access-list extended remote_operation
permit ip 192.168.100.0 0.0.0.255 any
permit ip 10.0.0.0 0.255.255.255 any
deny ip any any
```

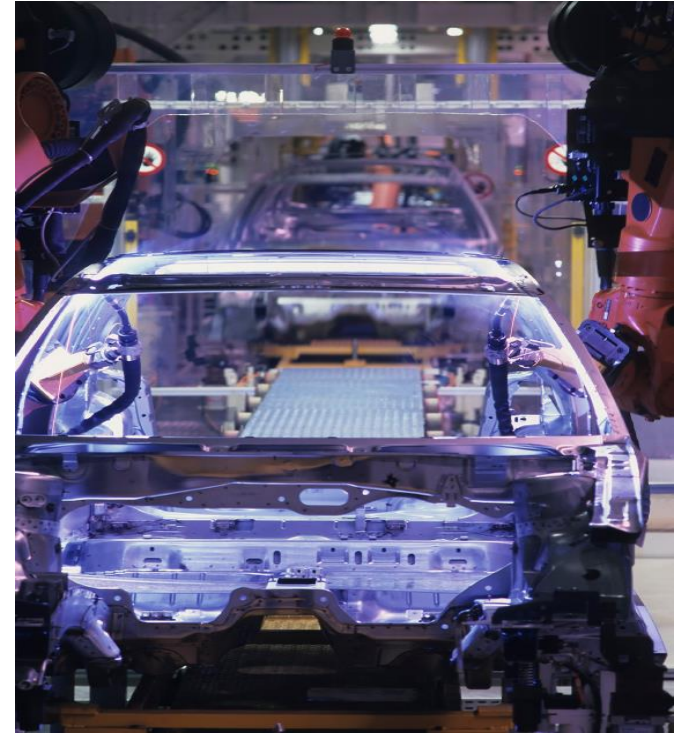


Summary

In Summary

We've discussed...

- Industry Trends
 - Convergence, IP everywhere, Focus on security
- Industry Protocols
 - Ethernet/IP, PROFINET, ModbusTCP
- Design Considerations
 - Wired and wireless considerations
 - Redundancy Mechanisms (REP / PRP)
 - Security



Cisco *live!*

Agenda

- Industry Trends
- Industrial Networking
 - A Quick 101 Guide
 -
 - Products and Architectures
 - Availability and Resilience
 - Security
 - Q&A
- Recommended Resources



Agenda

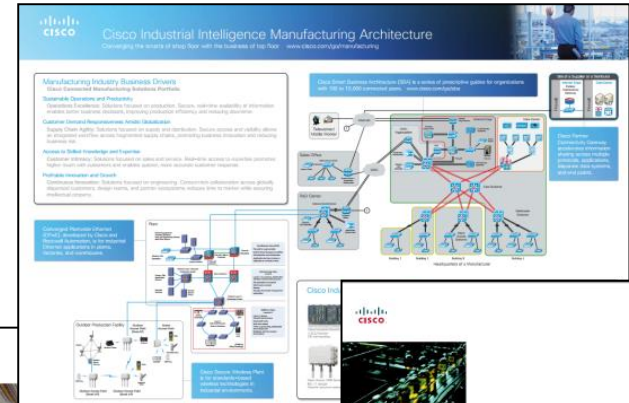
- Industry Trends
- Industrial Networking
 - A Quick 101 Guide
 - Applications and Protocols
 - Products and Architectures
 - Availability and Resilience
 - Security
- Q&A
- Recommended Resources



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](#)



Rockwell Automation and Cisco Four Key Initiatives

Operational Resilience: A single system architecture, using open, industry-standard networking technologies, such as Ethernet, is essential for achieving the highest reliability and efficiency required in an industrial manufacturing environment.

Converged Plantwide Ethernet Architecture: This architecture combines the Rockwell Automation (Rockwell) and Cisco Ethernet (Cisco) and is designed to be the backbone for secure remote access to plant floor applications and data.

Plant Production and Safety: Utilizing 100% Industrial Ethernet switch technology, the use of Cisco and Rockwell Automation.

People and Process Optimization: Utilizing open and secure to enable manufacturing and IT convergence and allow operational architecture deployment and management. Utilizing open and secure to enable manufacturing and IT convergence and allow operational architecture deployment and management. Utilizing open and secure to enable manufacturing and IT convergence and allow operational architecture deployment and management.

Converged Plantwide Ethernet (CPwE) Design and Implementation Guide

Published August 30, 2011

Converged Plantwide Ethernet (CPwE) Design and Implementation Guide

This guide provides a comprehensive overview of the design and implementation of a converged plantwide Ethernet network. It covers the following key areas:

- Design Considerations:** Key factors to consider when designing a CPwE network, including network topology, security, and scalability.
- Implementation Best Practices:** Guidelines for the successful deployment of a CPwE network, including hardware and software requirements.
- Security and Resilience:** Strategies for ensuring the security and reliability of the CPwE network.
- Integration with Existing Systems:** How to integrate the CPwE network with existing industrial systems and applications.





Q & A

Cisco *live!*

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-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
<http://showcase.genie-connect.com/clmelbourne2015>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 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 *live!*



Thank you.

Cisco *live!*



CISCO