We’re ready. Are you?
Industrial Network Concepts, Design, Resilience and Security

David Bell, Solution Architect
Agenda

• Industrial Networking
  • A Quick Introduction
  • Applications and Protocols
  • Products and Architectures: Wired and Wireless
  • Availability and Resilience: REP and MRP
  • CyberSecurity: Firewalling and ISE

• Q&A

• Recommended Resources
Agenda

• Industrial Networking
  • A Quick Introduction
  • Applications and Protocols
  • Products and Architectures: Wired and Wireless
  • Availability and Resilience: REP and MRP
  • CyberSecurity: Firewalls and ISE
• Q&A
• Recommended Resources
In the beginning...
…then along came the PLC…
…which could be “networked” (but not with Ethernet!)
The reason Ethernet got a bad reputation for determinism…

Control Loops Could Not Tolerate This

Legacy 10BASE2/10BASE5 Ethernet: Lots of CSMA/CD Collisions
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 – lots of “standards” everywhere
Agenda

• Industrial Networking
  • A Quick Introduction
  • Applications and Protocols
  • Products and Architectures: Wired and Wireless
  • Availability and Resilience: REP and MRP
  • CyberSecurity: Firewalling and ISE
• Q&A
• Recommended Resources
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 OT Language

**Applications**


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

Historian – Data collection and analysis.

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

HMI - Human Machine Interface. Control and monitoring point.

PLC/PAC - Programmable Logic (Automation) Controller.

I/O - Input / Output.

Actuator/Drive – Makes something happen.

**Devices**

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


- **CIP** - Common Industrial Protocol. Application layer common to DeviceNet, CompoNet, ControlNet and EtherNet/IP.
- **EtherCAT** - An open high performance Ethernet-based fieldbus system.
- **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.
- **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
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

ODVA: www.odva.org
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

- 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 CIP 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!
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
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, HMI updates
  - 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
  - Standard Ethernet kit, no special hardware
  - Around 90% PROFINET Traffic
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 proprietary 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 + khranos time]
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 AND switchports
- 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
  - IE4000/5000 – 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
  profinet vlan xxx
  interface GigabitEthernet1/0/1
  switchport access vlan xxx
  switchport mode access
  spanning-tree portfast
  ```

* Or use “switchport voice vlan dot1p”
Modbus TCP
Modbus - History

- Modicon (Schneider Electric) introduced ModbusRTU in 1979
- Development managed by Modbus Organization 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 Google Translate of the industrial world.
- Not designed for complex motion, I/O or Safety applications

Highly Insecure!
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

• Industrial Networking
  • A Quick Introduction
  • Applications and Protocols
  • Products and Architectures: Wired and Wireless
  • Availability and Resilience: REP and MRP
  • Security: CyberSecurity and Physical Security using EEM
• Q&A
• Recommended Resources
Cisco IOT System Overview

Network Connectivity

Cisco Portfolio
- IE 2000, 3000
- CG 2000
- Field AP 1552
- Manufacturing WAGIAP (Rockwell)
- Industrial AP IW 3700 802.11ac
- Mobile IP Gateway
- IR 809
- IR 910
- ESS Switches
- 5900 ESR
- 5921 Software Router Embedded Networks

Fog Computing

Cisco Portfolio
- GE
- SK Solutions
- Itron
- SAP
- Bit Stew Systems
- Covacs
- OSIsoft

Platforms: CGR, 8x9 Series

Management and Automation

Cisco Portfolio
- AMP, Sourcefire Defense Center, Cloud Security
- IE Portfolio
- Cisco ISE

Physical Access Manager

Cyber and Physical Security

Cisco Portfolio
- IP Cameras
- Video Surveillance Manager
- Physical Access Manager
- IR Portfolio
- Cisco ISA 3000

IOX

Data Analytics

Cisco Portfolio
- Fog Data Services

Cisco Connected Streaming Analytics

IoT Field Network Director

Prime

Fog Director
## Industrial Compliance

<table>
<thead>
<tr>
<th>General Specifications</th>
<th>Industry Specific</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safety And Hazard</strong></td>
<td>• UL 508</td>
</tr>
<tr>
<td>• UL/CSA 60950-1</td>
<td>• CSA C22.2 No.142</td>
</tr>
<tr>
<td>• EN60950-1</td>
<td>• EN 61131-2 (Programmable Controllers)</td>
</tr>
<tr>
<td>• CB to IEC 60950-1</td>
<td>• Protective Coating</td>
</tr>
<tr>
<td>• NOM to NOM-019-SCF1</td>
<td>• Substation (IEEE 1613, IEC 61850-3)</td>
</tr>
<tr>
<td>• CE Marking</td>
<td>• KEMA</td>
</tr>
<tr>
<td><strong>Shock and Vibration</strong></td>
<td>• Marine (DNV)</td>
</tr>
<tr>
<td>• ANSI/ISA 12.12.01 (Class 1, Div 2 A-D)</td>
<td>• Railway EN 50155</td>
</tr>
<tr>
<td>• IEC 60079-0, -15 (Class1, Zone 2 A-D)</td>
<td>• NEMA TS-2</td>
</tr>
<tr>
<td>• EN 60079-0, -15 ATEX certification (Class I, Zone 2 A-D)*</td>
<td>• ODVA Industrial EtherNet/IP</td>
</tr>
<tr>
<td><strong>EMC</strong></td>
<td>• PROFINETv2</td>
</tr>
<tr>
<td>• FCC, IEC/EN 61000-4, RoHS, World wide EMC</td>
<td>• ISO-12944-6</td>
</tr>
<tr>
<td><strong>Shock and Vibration</strong></td>
<td>• ODVA Industrial EtherNet/IP</td>
</tr>
<tr>
<td>• IEC 60068-2-27 (Operational Shock: 30G 11ms, half sine)</td>
<td>• PROFINETv2</td>
</tr>
<tr>
<td>• IEC 60068-2-27 (Non-Operational Shock 55-75G, trapezoidal)</td>
<td>• ISO-12944-6</td>
</tr>
<tr>
<td>• IEC 60068-2-6, IEC 60068-2-64 (Operational Vibration 2g@10-500Hz)</td>
<td>• IEC-60068-2-6</td>
</tr>
<tr>
<td>• IEC 60068-2-6, IEC 60068-2-64 (Non-operational Vibration)</td>
<td></td>
</tr>
<tr>
<td>• Storage altitude: 15,000 ft (4,570 m)</td>
<td></td>
</tr>
<tr>
<td><strong>Relative Humidity</strong></td>
<td></td>
</tr>
<tr>
<td>• IEC 60068-52-2 (salt Fog Mist, Test Kb) Marine environments</td>
<td></td>
</tr>
<tr>
<td>• IEC 60068-2-3</td>
<td></td>
</tr>
<tr>
<td>• IEC 60068-2-30</td>
<td></td>
</tr>
<tr>
<td>• Relative Humidity of 5% or 95% Non-condensing</td>
<td></td>
</tr>
</tbody>
</table>
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 device configs
Wired Architecture
Security Framework, ISA99 / IEC 62443

Strong Segmentation

Level 5
Enterprise Network
Level 4
E-Mail, Intranet, etc.
Site Business Planning and Logistics Network
Level 3
Terminal Services
Patch Management
AV Server
Web Services Operations
Application Server
Level 2
Level 1
Level 0
Enterprise Zone
DMZ
Operations Zone
Cell/Area Zone
Purdue Reference Model, ISA-95
ISA99, Industrial Automation and Control Systems Security

- SCADA Server
- Active Directory
- Engineering Workstation
- Domain Controller
- Site Operations and Control
- SCADA Client
- Operator Interface
- Engineering Workstation
- Operator Interface
- Batch Control
- Discrete Control
- Drive Control
- Continuous Process Control
- Safety Control
- Sensors
- Drives
- Actuators
- Robots
- Process

Web E-Mail IA
Firewall
Firewall
Converged Plant-wide Ethernet Architecture 3.0

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

Plant Firewalls:
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services – Remote Site Access
- Portal and Remote Desktop Services proxy

Enterprise Zone Levels 4–5
- Enterprise/IT Integration
- Collaboration
- Wireless Application Optimisation
- Application and Data share
- Access Control
- Threat Protection

Industrial Demilitarised Zone
- Real-Time Control
- Fast Convergence
- Traffic Segmentation and Management

Industrial Zone
- Multisite Operations
- Multi-Service Networks
- Network and Security Management
- Routing

Level 3
- Site Operations
- Multi-Service Networks
- Network and Security Management
- Routing

Industrial Wired LAN Access
- Physical or Virtualised Servers
- ERP, Email
- Active Directory (AD), AAA – Radius
- Call Manager, etc.

Enterprise Wired LAN Access Configurations Introduced w/ CPwE - REP

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.
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
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

<table>
<thead>
<tr>
<th>Unified WLAN Architecture</th>
<th>Autonomous WLAN Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Large number of APs (&gt;10)</td>
<td>• Small number of APs (&lt;10)</td>
</tr>
<tr>
<td>• Plant-wide coverage</td>
<td>• Larger number of WGBs per AP</td>
</tr>
<tr>
<td>• Existing infrastructure, IT practices and security policies that call for Unified architecture</td>
<td>• Stand-alone applications</td>
</tr>
<tr>
<td>• Applications that <strong>require fast wireless roaming</strong></td>
<td>• Applications with no roaming</td>
</tr>
<tr>
<td>• WLAN is managed jointly by IT and control engineers – greater level of expertise</td>
<td>• WLAN is integrated into a stand-alone OEM machine and delivered to a plant</td>
</tr>
<tr>
<td></td>
<td>• WLAN is managed mostly by control engineers – lower level of expertise</td>
</tr>
<tr>
<td></td>
<td>• Lower initial cost</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>5 GHz Channels</th>
<th>No DFS</th>
<th>DFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S., Canada, Australia</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Europe</td>
<td>4</td>
<td>15</td>
</tr>
<tr>
<td>China</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

### Just an example: free space signal propagation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio sensitivity</td>
<td>-85 dBm</td>
</tr>
<tr>
<td>Transmit power</td>
<td>5 dBm</td>
</tr>
<tr>
<td>Tx / Rx antenna gain</td>
<td>4 dBi</td>
</tr>
<tr>
<td>Re-use distance (5180 MHz)</td>
<td>350 meters</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>DSCP</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP event</td>
<td>59</td>
<td>Voice</td>
</tr>
<tr>
<td>PTP management</td>
<td>47</td>
<td></td>
</tr>
<tr>
<td>CIP class 0 / 1 (I/O, P/C, Safety, Motion)</td>
<td>55</td>
<td>Video</td>
</tr>
<tr>
<td>CIP class 3 (MSG, HMI)</td>
<td>27</td>
<td>Best Effort</td>
</tr>
<tr>
<td>Unclassified</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Classification

- BK
- BE
- VI
- VO

Internal contention between queues

Media contention between stations
Agenda

• Industrial Networking
  • A Quick Introduction
  • Applications and Protocols
  • Products and Architectures: Wired and Wireless
  • Availability and Resilience: REP and MRP
  • CyberSecurity: Firewalling and ISE

• Q&A

• Recommended Resources
Industrial Network Topologies

Cell/Area Zone Topology Options

<table>
<thead>
<tr>
<th></th>
<th>Redundant Star</th>
<th>Ring</th>
<th>Star/Bus Linear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cabling Requirements</td>
<td>Worst</td>
<td>Best</td>
<td>OK</td>
</tr>
<tr>
<td>East of Configuration</td>
<td>Worst</td>
<td>Best</td>
<td>OK</td>
</tr>
<tr>
<td>Implementation Costs</td>
<td>Worst</td>
<td>Best</td>
<td>OK</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Worst</td>
<td>Best</td>
<td>OK</td>
</tr>
<tr>
<td>Redundancy and Convergence</td>
<td>Worst</td>
<td>Best</td>
<td>OK</td>
</tr>
<tr>
<td>Disruption During Network Upgrade</td>
<td>Worst</td>
<td>Best</td>
<td>OK</td>
</tr>
<tr>
<td>Readiness for Network Convergence</td>
<td>Worst</td>
<td>Best</td>
<td>OK</td>
</tr>
<tr>
<td>Overall in Network TCO and Performance</td>
<td>Worst</td>
<td>Best</td>
<td>OK</td>
</tr>
</tbody>
</table>

Cisco Catalyst 3750 Stackwise Switches

HMI
Controllers, Drives, and Distributed I/O

Redundant Star
Flex Links
EtherChannel

Ring
Resilient Ethernet Protocol (REP)

Star/Bus Linear
# Performance Requirements

## Industrial Automation & Control Applications

<table>
<thead>
<tr>
<th>Function</th>
<th>Process Automation</th>
<th>Discrete Automation</th>
<th>Motion Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info. Int.</td>
<td>Information Integration, Slower Process Automation</td>
<td>Time-critical Factory Automation</td>
<td>Multi-axis Motion Control</td>
</tr>
<tr>
<td>Comm. Tech.</td>
<td>.Net, DCOM, TCP/IP</td>
<td>Industrial Protocols, CIP, Profinet</td>
<td>Hardware and Software solutions, e.g. CIP Motion, IRT</td>
</tr>
<tr>
<td>Period</td>
<td>1 second or longer</td>
<td>10 ms to 100 ms</td>
<td>&lt;5 ms</td>
</tr>
<tr>
<td>Industries</td>
<td>Oil &amp; gas, chemicals, energy, water</td>
<td>Auto, food and bev, electrical assembly, semiconductor, metals, pharmaceutical</td>
<td>Subset of Discrete automation</td>
</tr>
<tr>
<td>Applications</td>
<td>Pumps, compressors, mixers; monitoring of temperature, pressure, flow</td>
<td>Material handling, filling, labeling, palletising, packaging; welding, stamping, cutting, metal forming, soldering, sorting</td>
<td>Synchronisation of multiple axes: printing presses, wire drawing, web making, picking and placing</td>
</tr>
</tbody>
</table>

Source: ARC Advisory Group
## Network Resiliency Protocols

Selection Is Application Driven

<table>
<thead>
<tr>
<th>Resiliency Protocol</th>
<th>Mixed Vendor</th>
<th>Ring</th>
<th>Redundant Star</th>
<th>Net Conv &gt;250 ms</th>
<th>Net Conv 50-100 ms</th>
<th>Net Conv &lt; 10 ms</th>
<th>Layer 3</th>
<th>Layer 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP (802.1D)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSTP (802.1w)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSTP (802.1s)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PVST+</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REP</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>EtherChannel (LACP 802.3ad)</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>MRP (IEC 62439-2)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Flex Links</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DLR (IEC &amp; ODVA)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>StackWise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HSRP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VRRP (IETF RFC 5768)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
## Network Resiliency Protocols

Selection Is Application Driven

<table>
<thead>
<tr>
<th>Resiliency Protocol</th>
<th>Mixed Vendor</th>
<th>Ring</th>
<th>Redundant Star</th>
<th>Net Conv &gt;250 ms</th>
<th>Net Conv 50-100 ms</th>
<th>Net Conv &lt; 10 ms</th>
<th>Layer 3</th>
<th>Layer 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP (802.1D)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>RSTP (802.1w)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>MSTP (802.1s)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>PVST+</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>REP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>EtherChannel (LACP 802.3ad)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>MRP (IEC 62439-2)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Flex Links</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>DLR (IEC &amp; ODVA)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>StackWise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>HSRP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VRRP (IETF RFC 3768)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
## Network Resiliency Protocols

Selection Is Application Driven

<table>
<thead>
<tr>
<th>Resiliency Protocol</th>
<th>Mixed Vendor</th>
<th>Ring</th>
<th>Redundant Star</th>
<th>Net Conv &gt;250 ms</th>
<th>Net Conv 50-100 ms</th>
<th>Net Conv &lt; 10 ms</th>
<th>Layer 3</th>
<th>Layer 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP (802.1D)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>RSTP (802.1w)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>MSTP (802.1s)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>PVST+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>REP</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>EtherChannel (LACP 802.3ad)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>MRP (IEC 62439-2)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Flex Links</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>DLR (IEC &amp; ODVA)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>StackWise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>HSRP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VRRP (IETF RFC 3768)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
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 are 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 into forwarding state.
REP Segment 1 - Basic Configuration

Note: Trunk port configuration mandatory before configuring REP
**Show REP Topology Command**

```
IE-SWITCH-9 # show rep topology
```

<table>
<thead>
<tr>
<th>REP Segment 1</th>
<th>BridgeName</th>
<th>PortName</th>
<th>Edge Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE-SWITCH-9</td>
<td>Gi0/2</td>
<td>Pri</td>
<td>Open</td>
</tr>
<tr>
<td>IE-SWITCH-10</td>
<td>Gi0/1</td>
<td></td>
<td>Open</td>
</tr>
<tr>
<td>IE-SWITCH-10</td>
<td>Gi0/2</td>
<td></td>
<td>Open</td>
</tr>
<tr>
<td>IE-SWITCH-11</td>
<td>Gi0/1</td>
<td></td>
<td>Open</td>
</tr>
<tr>
<td>IE-SWITCH-11</td>
<td>Gi0/2</td>
<td>Alt</td>
<td></td>
</tr>
<tr>
<td>IE-SWITCH-12</td>
<td>Gi0/1</td>
<td></td>
<td>Open</td>
</tr>
<tr>
<td>IE-SWITCH-12</td>
<td>Gi0/2</td>
<td></td>
<td>Open</td>
</tr>
<tr>
<td>IE-SWITCH-9</td>
<td>Gi0/1</td>
<td>Sec</td>
<td>Open</td>
</tr>
</tbody>
</table>

- **REP Edge Port**
- **REP Transit Port**
- **REP Alternate Port**

This is the primary edge port

This is the preferred alternate port blocking
Media Redundancy Protocol (MRP)
Media Redundancy Protocol - MRP

- L2 ring redundancy protocol, utilised extensively in PROFINET environments
- Standardised as IEC 62439-2:2010
- Limited to single ring topology
- MRP switches enable multiple rings to be joined
- Two logical components per ring:
  - MRC: MRP client,
  - MRM: MRP manager
- A MRP ring has a unique domain ID defined
- Defines 2 specific recovery time limits:
  - \(<200\text{ms for max of 50 switches}\)
  - \(<500\text{ms for max of 50 switches}\)
Media Redundancy Protocol - MRP

- **MRM** – Medium Redundancy Master
  - Controls the ring, sends test frames, LLDP
  - Provides logical break in the ring
  - Closes the ring if failure detected
  - One per ring

- **MRC** – Medium Redundancy Client
  - Forward test and supervision frames
  - Closes the ring
  - Many per ring

Normal Operation

With Link Failure
Cisco CLI MRP Configuration

Global: mrp ring 1
    mode manager

interface FastEthernet1/1
    switch mode access
    mrp ring 1

interface FastEthernet1/2
    switch mode access
    mrp ring 1

Global: mrp ring 1
    mode client

Interface FastEthernet1/1
    switch mode access
    mrp ring 1

Interface FastEthernet1/2
    switch mode access
    mrp ring 1

Switch(config)# no profinet mrp
Switch(config)# license right-to-use activate mrp-client
OR
Switch(config)# license right-to-use activate mrp-manager

Counterintuitive!
Agenda

• Industrial Networking
  • A Quick Introduction
  • Applications and Protocols
  • Products and Architectures: Wired and Wireless
  • Availability and Resilience: REP and MRP
  • CyberSecurity: Firewalling and ISE
• Q&A
• Recommended Resources
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
A Renewed Focus on Security

The Problem with SCADA / DCS Runs Deep…

• An ICS-CERT advisory 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 advisory 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 advisory 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://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."

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…

• 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

Source: osvdb.org.; https://ics-cert.us-cert.gov/advisories/ICSA-14-084-01
Example - Compressor
How do we Implement Industrial Cyber Security?

Follow ISA99 / IEC 62443 Security Guidelines

Recommends:

- Documented Controls Security Policy
- Network Demilitarised Zone (DMZ)
- Defending the Industrial edge (IPS, ISE)
- Protect the Interior (ACLs, Port Security, StormControl)
- Remote Access Policy (VPN)
- Endpoint and Network Hardening
- Physical Security

Lack of policies and procedures that govern access to the control network....

Having the technology to detect/mitigate malicious traffic and the associated procedure to ensure it’s use.

Having the ability to safely/securely control your assets remotely.
Industrial Security - ISA 3000

ISA 3000 Fibre

ISA 3000 Copper

- Industrial, Energy, Marine, Railway Compliance
- Services include Firewall, VPN and SourceFire IPS, DHCP, and NAT
- Two Configurations
  - Copper: 4x10/100/1000BaseT; 2x10/100/1000BaseT
  - Fibre: 2x1GbE (SFP)
  - LED scheme is OT Ready
- DIN Rail mounting with optional Rack Mounting
- Connectors: Management Interface (RJ45 and USB); Power supports 24-12 AWG; Factory Reset
- Thermals: -40C to 60C no airflow; -40C to 70C with 40LFM; -34C to 74C with 200LFM
Access Control

ISE – Identity Services Engine
ISE Use Case #1 - Employee Access

- Employee Remote Access
- External DMZ/Firewall
- Link for Failover Detection
- Firewall (Active)
- Firewall (Standby)
- Industrial Demilitarised Zone (IDMZ)
- Enterprise Zone Levels 4 and 5
- Layer 2 Access Switch
- ASA 5500X
- Catalyst 6500/4500
- Phone Controller
- Camera
- I/O
- Safety Controller
- Instrumentation
- Robot
- Servo Drive
- HMI
- Virtual Machine
- Site Operations Level 3
- dACL
- EXAMINING
- Site Operations Level 0-2
- Primary WLC
- Secondary WLC
- LWAP SSID 5 GHz
- LWAP SSID 2.4 GHz
- WGB AP
- WGB LWAP
- External DMZ/Firewall
- Employee Remote Access
- Employee Access
- PSN
- AD
- ISE ADMIN
- ISE PSN
- EXAMINING
- Site Operations Level 3
- dACL
- EXAMINING
- Site Operations Level 0-2
- Primary WLC
- Secondary WLC
- LWAP SSID 5 GHz
- LWAP SSID 2.4 GHz
- WGB AP
- WGB LWAP
- External DMZ/Firewall
- Employee Remote Access
- Employee Access
- PSN
- AD
- ISE ADMIN
- ISE PSN

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
ISE Use Case #2 - Contractor/Vendor Access via Wireless

Enterprise Zone Levels 4 and 5

Industrial Demilitarised Zone (IDMZ)

Level 3

Level 0-2

Redundant Star Topology

Ring Topology - Linear/Bus/Star Topology
ISE Use Case #3 - Contractor trying switch ports

If running port security on switch, you can shut it down. Contractor thought they might get full access if they disconnected controller, but they still get examined and provided contractor access.
Threat Detection
SourceFire IPS
Increasing Visibility with DPI

Using DPI, we gain visibility of endpoints in use OS’s, ports, applications, etc.

Can span a port and introduce in passive mode

We can look deep into the packet, including MODBUS and DNP3 Traffic, to ensure they are properly formed and no inconsistencies exist.
Anomaly Detection

HMI gets compromised, and starts sending an influx in traffic, or communicating with a new destination.

Baselining the behaviour of endpoints.

Defence Centre manages Sensors, and will alert you of anomalous behaviour.
An IDS is only as strong as the Database it’s using.

Defence Centre communicates With Cisco Threat Intelligence TALOS for updates.
Remote Access
AnyConnect and ASA Firewall
ASA Firewall and AnyConnect
For employees, contractors, vendors

**ANYCONNECT**
Diverse Endpoint Support for Greater Flexibility

**CLIENTLESS**
Browser based VPN Excellent for contractors + vendors

**L2L**
Great for Manufacturing silos, Remote substations Oil and Gas plants

- Data-Loss Prevention
- Threat Prevention
- Access Granted
- Acceptable Use
- Access Control

Remote Substations
Remote plants
Remote Access

Welcome to the Cisco VPN Service

Username: contractor
Password: ********

Login

Demilitarised Zone (IDMZ)

RDP Plugin
Reverse Proxy to HMI
Summary
In Summary

We’ve discussed...

- Industrial Networking Basics
  - Convergence, IP everywhere, Focus on security
- Industry Protocols
  - Ethernet/IP, PROFINET, ModbusTCP
- Design Considerations
  - Wired and wireless considerations
  - Redundancy Mechanisms (REP / MRP)
- Cyber Security
  - Follow published standards
  - Access Control, Threat Detection, Remote Access
Agenda

• Industrial Networking
  • A Quick Introduction
  • Applications and Protocols
  • Products and Architectures: Wired and Wireless
  • Availability and Resilience: REP and MRP
  • CyberSecurity: Firewalling and ISE
• Q&A

• Recommended Resources
Q & A
Complete Your Online Session Evaluation

Give us your feedback and receive a **Cisco 2016 T-Shirt** by completing the Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- Visit any Cisco Live Internet Station located throughout the venue

**T-Shirts can be collected Friday 11 March at Registration**

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations.
[www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)
Call to Action

• Visit the World of Solutions for
  • Cisco Campus – IOT/IOE Demo Zone

• Meet the Engineer – I’m available most days or catch me in WoS

• Lunch and Learn Topics

• DevNet zone related sessions – IOx Fog Computing
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
Thank you