NI10

EtherNet I/P Best Practices & Topologies
Tom Steffen – Rockwell Automation
Related Sessions

• NI11 – IT and Plant Floor – Breaking Down the Barriers
• NI13 – The Connected Enterprise
• NI03 - Testing the Physical Layer for Ethernet/IP
• NI04 - When is a good time to have MICE on your plant floor? Structured Cabling Best Practices (Industrial Ethernet)
• NI18 – Remote Access
Agenda

Single Industrial Network Technology

Robust Physical Layer

Segmentation / Structure

Redundant Path Topologies with Resiliency Protocols

Prioritization - Quality of Service (QoS)

Convergence-ready Solutions

Additional Information
### What is real-time?

- Application dependent ..... only you can define what this means for your application.

### Application Requirements

#### Network Technology Convergence - Performance

<table>
<thead>
<tr>
<th>Function</th>
<th>Information Integration, Slower Process Automation</th>
<th>Time-critical Discrete Automation</th>
<th>Motion Control</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication Technology</strong></td>
<td>.Net, DCOM, TCP/IP</td>
<td>Industrial Protocols - CIP</td>
<td>Hardware and Software solutions, e.g. CIP Motion, PTP</td>
</tr>
<tr>
<td><strong>Period</strong></td>
<td>10 ms to 1000 ms</td>
<td>1 ms to 100 ms</td>
<td>100 µs to 10 ms</td>
</tr>
<tr>
<td><strong>Industries</strong></td>
<td>Oil &amp; gas, chemicals, energy, water</td>
<td>Auto, food &amp; beverage, semiconductor, metals, pharmaceutical</td>
<td>Subset of discrete automation</td>
</tr>
<tr>
<td><strong>Applications</strong></td>
<td>Pumps, compressors, mixers, instrumentation</td>
<td>Material handling, filling, labeling, palletizing, packaging</td>
<td>Printing presses, wire drawing, web making, pick &amp; place</td>
</tr>
</tbody>
</table>

Source: ARC Advisory Group
Industrial Network Design Methodology

Why is this important?

- Flat and Open IACS Network Infrastructure
- Structured and Hardened IACS Network Infrastructure

- Enterprise-wide Network
  - Office Applications, Internetworking, Data Servers, Control
  - Physical or Virtualized Servers
  - AAA – Radius
  - USB

- Wide Area Network (WAN)
- Physical or Virtualized Servers
- ERP, Small
- Control

- Plantwide / Site-wide Network Integrated Architecture

POWERED BY WERNER ELECTRIC
Industrial Network Design Methodology

- Understand application and functional requirements
  - Devices to be connected – industrial and non-industrial
  - Data requirements for availability, integrity, and confidentiality
  - Communication patterns, topology, and resiliency requirements
  - Types of traffic – information, control, safety, time synchronization, drive control, voice, video

- Develop a logical framework (roadmap)
  - Migrate from flat networks to structured and hardened networks
  - Define zones and segmentation, place applications and devices in the logical framework based on requirements

- Develop a physical framework to align with and support the logical framework

- Deploy a Holistic Defense-in-Depth Security Model

- Reduce risk, simplify design, and speed deployment:
  - Use information technology (IT) standards
  - Follow industrial automation technology (IAT) standards
  - Utilize reference models and reference architectures

Because Network Infrastructure Matters

Enabling OEM

POWERED BY WERNER ELECTRIC
Networking Design Considerations

Recommendations and guidance to help reduce network **Latency** and **Jitter**, to help increase the **Availability**, **Integrity** and **Confidentiality** of data, and to help design and deploy a **Scalable**, **Robust**, **Secure** and **Future-Ready** EtherNet/IP network infrastructure:

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation / Structure
- Prioritization - Quality of Service (QoS)
- Redundant Path Topologies with Resiliency Protocols
- Time Synchronization – PTP, CIP Sync, CIP Motion
- Multicast Management
- Convergence-ready Solutions
- Security – Holistic Defense-in-Depth
- Scalable Secure Remote Access
- Wireless – Wi-Fi
Networking Design Considerations

Recommendations and guidance to help reduce network **Latency** and **Jitter**, to help increase the **Availability**, **Integrity** and **Confidentiality** of data, and to help design and deploy a **Scalable**, **Robust**, **Secure** and **Future-Ready** EtherNet/IP network infrastructure:

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation / Structure
- Prioritization - Quality of Service (QoS)
- Redundant Path Topologies with Resiliency Protocols
- Time Synchronization – PTP, CIP Sync, CIP Motion
- Multicast Management
- Convergence-ready Solutions
- Security – Holistic Defense-in-Depth
- Scalable Secure Remote Access
- Wireless – Wi-Fi
Single Industrial Network Technology
OSI 7-Layer Reference Model

**Open Systems Interconnection**

<table>
<thead>
<tr>
<th>Layer Name</th>
<th>Layer No.</th>
<th>Function</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Layer 7</td>
<td>Network Services to User App</td>
<td>CIP</td>
</tr>
<tr>
<td>Presentation</td>
<td>Layer 6</td>
<td>Encryption/Other processing</td>
<td>IEC 61158</td>
</tr>
<tr>
<td>Session</td>
<td>Layer 5</td>
<td>Manage Multiple Applications</td>
<td>IEC 61158</td>
</tr>
<tr>
<td>Transport</td>
<td>Layer 4</td>
<td>Reliable End-to-End Delivery Error Correction</td>
<td>IETF TCP/UDP</td>
</tr>
<tr>
<td>Network</td>
<td>Layer 3</td>
<td>Packet Delivery, Routing</td>
<td>IETF IP</td>
</tr>
<tr>
<td>Data Link</td>
<td>Layer 2</td>
<td>Framing of Data, Error Checking</td>
<td>IEEE 802.3/802.1</td>
</tr>
<tr>
<td>Physical</td>
<td>Layer 1</td>
<td>Signal type to transmit bits, pin-outs, cable type</td>
<td>TIA - 1005</td>
</tr>
</tbody>
</table>

**What makes EtherNet/IP industrial?**

- EtherNet/IP is an open systems interconnection technology that provides a reliable, end-to-end delivery mechanism with error correction.
- It supports packet delivery, routing, and error checking at the Network layer.
- At the Physical layer, it ensures the correct signal types and pin-outs for different cabling types.

**5-Layer TCP/IP Model**

- **Physical Layer Hardening**
- **Infrastructure Device Hardening**
- **Common Application Layer Protocol**
Networking Design Considerations

Recommendations and guidance to help reduce network **Latency** and **Jitter**, to help increase the **Availability**, **Integrity** and **Confidentiality** of data, and to help design and deploy a **Scalable**, **Robust**, **Secure** and **Future-Ready** EtherNet/IP network infrastructure:

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation / Structure
- Prioritization - Quality of Service (QoS)
- Redundant Path Topologies with Resiliency Protocols
- Time Synchronization – PTP, CIP Sync, CIP Motion
- Multicast Management
- Convergence-ready Solutions
- Security – Holistic Defense-in-Depth
- Scalable Secure Remote Access
- Wireless – Wi-Fi
Robust Physical Layer
Collaboration of Partners

- Design and implement a robust physical layer
- Environment Classification - MICE
  - More than cable
    - Connectors
    - Patch panels
    - Cable management
    - Noise mitigation
      - Grounding, Bonding and Shielding
- Standard Physical Media
  - Wired vs. Wireless
  - Copper vs. Fiber
  - UTP vs. STP
  - Singlemode vs. Multimode
  - SFP – LC vs. SC
- Standard Topology Choices
  - Switch-Level & Device-Level

Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide
Cable Selection ENET-WP007
ODVA Guide
Fiber Guide ENET-TD003
M.I.C.E. provides a method of categorizing the environmental classes for each plant Cell/Area zone.

This provides for determination of the level of “hardening” required for the network media, connectors, pathways, devices and enclosures.

The MICE environmental classification is a measure of product robustness:

- Specified in ISO/IEC 24702
- Part of TIA-1005 and ANSI/TIA-568-C.0 standards

Examples of rating:

- 1585 Media : $M_3I_3C_3E_3$
- M12: $M_3I_3C_3E_3$
- RJ-45: $M_1I_1C_2E_2$
Networking Design Considerations

Recommendations and guidance to help reduce network **Latency** and **Jitter**, to help increase the **Availability**, **Integrity** and **Confidentiality** of data, and to help design and deploy a **Scalable**, **Robust**, **Secure** and **Future-Ready** EtherNet/IP network infrastructure:

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation / Structure
- Prioritization - Quality of Service (QoS)
- Redundant Path Topologies with Resiliency Protocols
- Time Synchronization – PTP, CIP Sync, CIP Motion
- Multicast Management
- Convergence-ready Solutions
- Security – Holistic Defense-in-Depth
- Scalable Secure Remote Access
- Wireless – Wi-Fi
Segmentation
Structured and Hardened Network Infrastructure

- Smaller modular building blocks to help 1) minimize network sprawl and 2) build scalable, robust and future-ready network infrastructure
  - Smaller fault domains (e.g. Layer 2 loops)
  - Smaller broadcast domains
  - Smaller domains of trust (security)

- Multiple techniques to create smaller network building blocks (Layer 2 domains)
  - Structure and hierarchy
    - Logical model – geographical and functional organization of IACS devices
    - Campus network model - multi-tier switch model – Layer 2 and Layer 3
    - Logical framework
  - Segmentation
    - Multiple network interface cards (NICs) – e.g. CIP bridge
    - Network Address Translation (NAT) appliance
    - Virtual Local Area Networks (VLANs)
    - VLANs with NAT
    - Integrated Services Router
Segmentation Structure and Hierarchy

Logical Model

Industrial Automation and Control System (IACS)
Converged Multi-discipline Industrial Network
Segmentation
Structure and Hierarchy – Campus Network Model

- Hierarchical, modular and scalable building blocks
- Creates small domains - clear demarcations and segmentation
  - Fault domain (e.g. Layer 2 loops), broadcast domain, domains of trust (security)
- Easier to grow, understand and troubleshoot
- Multi-tier switch model
  - Core
    - Aggregates distribution switches
    - Backbone of network
    - Industrial DMZ connectivity
  - Distribution
    - Aggregates access switches
    - Provides Layer 3 services
  - Access
    - Aggregates industrial automation and control system (IACS) devices
    - Provides Layer 2 services
Multiple NIC Segmentation

Plant-wide / Site-wide Network

Enterprise-wide Business Systems

Levels 4 & 5 – Data Center Enterprise Zone

Level 3.5 - IDMZ

Industrial Zone

Physical or Virtualized Servers
- FactoryTalk Application Servers & Services Platform
- Network Services – e.g. DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

Level 3 - Site Operations

Cell/Area Zones

Levels 0-2

Plant-wide Site-wide Operation Systems

Line/Area Controller

Cell/Area Zone #1

Subnet 192.168.1.0/24

Cell/Area Zone #2

Subnet 192.168.1.0/24

Cell/Area Zone #3

Subnet 192.168.1.0/24

Plant LAN – VLAN17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

EtherNet/IP

Copyright © 2014 Rockwell Automation, Inc. All Rights Reserved
NAT Appliance Segmentation
Plant-wide / Site-wide Network

Enterprise-wide Business Systems

Plant-wide Site-wide Operation Systems

Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ
Industrial Zone

Physical or Virtualized Servers
- FactoryTalk Application Servers & Services Platform
- Network Services – e.g. DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

Level 3 - Site Operations

Cell/Area Zones
Levels 0-2

Plant LAN – VLAN17 - Layer 2 Domain
Plant IP - Subnet 10.17.10.0/24

Cell/Area Zone #1
Subnet 192.168.1.0/24

Cell/Area Zone #2
Subnet 192.168.1.0/24

Cell/Area Zone #3
Subnet 192.168.1.0/24

Cell/Area Zones
Levels 0-2

Copyright © 2014 Rockwell Automation, Inc. All Rights Reserved
Integrated Services Router

Segmentation  Plant-wide / Site-wide Network

Enterprise-wide Business Systems

Levels 4 & 5 – Data Center Enterprise Zone

Level 3.5 - IDMZ

Plant-wide Site-wide Network

Level 3 - Site Operations

Industrial Zone

Physical or Virtualized Servers
- FactoryTalk Application Servers & Services Platform
- Network Services – e.g. DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

Cell/Area Zones

Levels 0-2

Plant-wide Site-wide Operation Systems

Cell/Area Zones

Levels 0-2

- Plant LAN – VLAN17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

• Cell/Area Zone #1
  Subnet 192.168.1.0/24

• Cell/Area Zone #2
  Subnet 192.168.1.0/24

• Cell/Area Zone #3
  Subnet 192.168.1.0/24

Copyright © 2014 Rockwell Automation, Inc. All Rights Reserved
VLAN Segmentation without NAT
Plant-wide / Site-wide Network

Enterprise-wide Business Systems

Level 3.5 - IDMZ
Industrial Zone

Levels 4 & 5 – Data Center Enterprise Zone

Plant-wide Site-wide Operation Systems

Physical or Virtualized Servers
- FactoryTalk Application Servers & Services Platform
- Network Services – e.g. DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

Level 3 - Site Operations

Cell/Area Zone #3
VLAN30
Subnet 10.10.30.0/24

Cell/Area Zones Levels 0-2

Cell/Area Zone #1
VLAN10
Subnet 10.10.10.0/24

Cell/Area Zone #2
VLAN20
Subnet 10.10.20.0/24

• Plant LAN – VLAN17 - Layer 2 Domain
• Plant IP - Subnet 10.17.10.0/24, every device requires a unique IP address

EtherNet/IP

Copyright © 2014 Rockwell Automation, Inc. All Rights Reserved
VLAN Segmentation with NAT
Plant-wide / Site-wide Network

- Enterprise-wide Business Systems
- Plant-wide Site-wide Operation Systems
- Physical or Virtualized Servers
  - FactoryTalk Application Servers & Services Platform
  - Network Services – e.g. DNS, AD, DHCP, AAA
  - Remote Access Server (RAS)
  - Call Manager
  - Storage Array

Cell/Area Zones
Levels 0-2

- Plant LAN – VLAN17 - Layer 2 Domain
- Plant IP - Subnet 10.17.10.0/24

- Cell/Area Zone #1
  VLAN10
  Subnet 192.168.1.0/24

- Cell/Area Zone #2
  VLAN20
  Subnet 192.168.1.0/24

- Cell/Area Zone #3
  VLAN30
  Subnet 192.168.1.0/24

Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ
Industrial Zone

Ethernet/IP

Copyright © 2014 Rockwell Automation, Inc. All Rights Reserved
Design smaller modular building blocks to help 1) minimize network sprawl and 2) build scalable, robust and future-ready network infrastructure:

- Smaller fault domains (e.g. Layer 2 loops)
- Smaller broadcast domains
- Smaller domains of trust (security)

- Multiple techniques to create smaller network building blocks (Layer 2 domains):
  - Structure and hierarchy
  - Segmentation
Networking Design Considerations

Recommendations and guidance to help reduce network **Latency** and **Jitter**, to help increase the **Availability**, **Integrity** and **Confidentiality** of data, and to help design and deploy a **Scalable**, **Robust**, **Secure** and **Future-Ready** EtherNet/IP network infrastructure:

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation / Structure
- Prioritization - Quality of Service (QoS)
- Redundant Path Topologies with Resiliency Protocols
- Time Synchronization – PTP, CIP Sync, CIP Motion
- Multicast Management
- Convergence-ready Solutions
- Security – Holistic Defense-in-Depth
- Scalable Secure Remote Access
- Wireless – Wi-Fi
Prioritization

<table>
<thead>
<tr>
<th>Not all traffic is created equal!</th>
<th>Control (e.g., CIP)</th>
<th>Video</th>
<th>Data (Best Effort)</th>
<th>Voice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Low to Moderate</td>
<td>Moderate to High</td>
<td>Moderate to High</td>
<td>Low to Moderate</td>
</tr>
<tr>
<td>Random Drop Sensitivity</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Latency Sensitivity</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Jitter Sensitivity</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

Plant-wide / site-wide networks must prioritize industrial automation and control system (IACS) traffic (CIP) over other traffic types (HTTP, SMTP, etc.) to ensure deterministic data flows with low latency and low jitter.

Different industrial traffic types (HMI, I/O, Safety, Motion) have different requirements for latency, packet loss and jitter.
Prioritization - Quality of Service (QoS)

- QoS helps mitigate the following network issues:
  - End-to-end delay
    - Fixed delay – latency
    - Variable delay – jitter
  - Bandwidth capacity issue
  - Packet loss
- QoS design considerations:
  - QoS prioritizes traffic into different service levels
  - Provides preferential forwarding treatment to some data traffic, at the expense of others
  - Allows for predictable service for different applications and traffic types
Prioritization - Quality of Service (QoS)
QoS - Operations

Classification and Marking  Queuing and (Selective) Dropping  Post-Queuing Operations
## Prioritization - Quality of Service (QoS)

**QoS – ODVA DSCP and CoS Priority Values**

- ODVA has specified QoS markings for CIP and PTP traffic
- Stratix 5700/8000/8300 initial configuration sets up the policing, queuing and scheduling

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>CIP Priority</th>
<th>DSCP Layer 3</th>
<th>CoS Layer 2</th>
<th>CIP Traffic Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP event (IEEE 1588)</td>
<td>n/a</td>
<td>59</td>
<td>7</td>
<td>PTP event messages, used by CIP Sync</td>
</tr>
<tr>
<td>PTP General (IEEE 1588)</td>
<td>n/a</td>
<td>47</td>
<td>5</td>
<td>PTP management messages, used by CIP Sync</td>
</tr>
<tr>
<td>CIP class 0 / 1</td>
<td>Urgent (3)</td>
<td>55</td>
<td>6</td>
<td>CIP Motion</td>
</tr>
<tr>
<td>Scheduled (2)</td>
<td>47</td>
<td>5</td>
<td></td>
<td>Safety I/O</td>
</tr>
<tr>
<td>High (1)</td>
<td>43</td>
<td>5</td>
<td></td>
<td>I/O</td>
</tr>
<tr>
<td>Low (0)</td>
<td>31</td>
<td>3</td>
<td></td>
<td>No recommendations at present</td>
</tr>
</tbody>
</table>

**CIP UCMM CIP class 3**

| All | 27 | 3 | CIP messaging |

[ODVA has specified QoS markings for CIP and PTP traffic](#).

[Stratix 5700/8000/8300 initial configuration sets up the policing, queuing and scheduling](#).
Prioritization - Quality of Service (QoS)

QoS – ODVA DSCP and CoS Priority Values

- Embedded Switch Technology – Linear and Ring Topologies
- ODVA has specified QoS markings for CIP and PTP traffic

<table>
<thead>
<tr>
<th>CIP Priority</th>
<th>DSCP Layer 3</th>
<th>CoS Layer 2</th>
<th>CIP Traffic Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highest</td>
<td>59</td>
<td>7</td>
<td>Beacon, PTP Event</td>
</tr>
<tr>
<td>High</td>
<td>55</td>
<td></td>
<td>CIP Motion</td>
</tr>
<tr>
<td>Low</td>
<td>43, 47</td>
<td></td>
<td>I/O, Safety I/O, PTP General</td>
</tr>
<tr>
<td>Lowest</td>
<td>0-42, 44-46, 48-54, 56-58, 60-63</td>
<td>1, 2, 3, 4, 5, 6</td>
<td>Best effort</td>
</tr>
</tbody>
</table>
Prioritization - Quality of Service (QoS)

QoS – Industrial Zone Priorities

Typical Enterprise QoS

- Priority Queue, Queue 1
  - Voice
  - Video
  - Call Signaling
  - Network Control
  - Critical Data
  - Best Effort
  - Bulk Data
  - Scavenger

IACS QoS

- Priority Queue, Queue 1
  - PTP-Event
  - CIP Motion
  - PTP Management, Safety I/O & I/O
  - Network Control
  - Voice
  - CIP Explicit Messaging
  - Call Signaling
  - Video
  - Critical Data
  - Bulk Data
  - Best Effort
  - Scavenger

POWERED BY WERNER ELECTRIC
Prioritization - Quality of Service (QoS)

Design and Implementation Considerations

- QoS trust boundary moving from switch access ports to QoS-capable CIP devices
  - Stratix 5700/8000/8300 Smartport enables Trusted Markings
- For existing CIP devices, marking at the switch access port is based on port number
  - CIP I/O UDP 2222
  - CIP Explicit TCP 44818
  - Established through Stratix Express Setup
- Prioritize traffic to reduce latency and jitter for CIP I/O traffic
  - Prioritized traffic delivery for CIP Sync and CIP Motion
  - Minimize impacts by DDoS attacks
- Deploy QoS throughout the IACS network to take better advantage of QoS features
• Plant-wide / site-wide networks must prioritize industrial automation and control system (IACS) traffic (CIP) over other traffic types (HTTP, SMTP, etc.) to ensure deterministic data flows with low latency and low jitter.

• Quality of Service does not increase bandwidth.
  – QoS gives preferential treatment to EtherNet/IP IACS network traffic at the expense of other network traffic types.

• QoS is integrated into the Stratix 5700/8000/8300 switch configurations.
  – The Stratix 5700/8000/8300 recognizes or ‘trusts’ QoS capable devices and prioritizes CIP traffic as it exits from the switch.

• Deploy QoS consistently throughout the EtherNet/IP IACS Network.
  – The more IACS devices that implement QoS, the better that the network infrastructure devices (switches, routers) can take advantage of QoS features.
Networking Design Considerations

Recommendations and guidance to help reduce network **Latency** and **Jitter**, to help increase the **Availability**, **Integrity** and **Confidentiality** of data, and to help design and deploy a **Scalable**, **Robust**, **Secure** and **Future-Ready** EtherNet/IP network infrastructure:

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation / Structure
- Prioritization - Quality of Service (QoS)
- Redundant Path Topologies with Resiliency Protocols
- Time Synchronization – PTP, CIP Sync, CIP Motion
- Multicast Management
- Convergence-ready Solutions
- Security – Holistic Defense-in-Depth
- Scalable Secure Remote Access
- Wireless – Wi-Fi
Resiliency Protocols and Redundant Topologies

Switch-level Topologies

- **Redundant Star**
  - Flex Links
  - Cisco Catalyst 3750 StackWise Switch Stack
  - Controllers, Drives, and Distributed I/O
  - Cell/Area Zone

- **Ring**
  - Resilient Ethernet Protocol (REP)
  - Cisco Catalyst 3750 StackWise Switch Stack
  - Controllers, Drives, and Distributed I/O
  - Cell/Area Zone

- **Star/Bus Linear**
  - Cisco Catalyst 3750 StackWise Switch Stack
  - Controllers, Drives, and Distributed I/O
  - Cell/Area Zone

Device-level Topologies
Redundant paths create a switching (bridging) loop

- Without proper configuration, a loop will lead to a broadcast storm, flooding the network, which will consume available bandwidth, and take down a Layer 2 switched (bridged) network
  - Layer 2 Ethernet frames do not have a time-to-live (TTL)
  - A Layer 2 frame can loop forever
• A Layer 2 resiliency protocol maintains redundant paths while avoiding switching (bridging) loop
Resiliency Protocols and Redundant Topologies: Layer 2 – Loop Avoidance

- Network convergence (healing, recovery, etc.) must occur before the Industrial Automation and Control System (IACS) application is impacted.
Resiliency Protocols and Redundant Topologies: Layer 2 – Loop Avoidance

- Network convergence must occur quickly enough to avoid a Logix Controller connection timeout:
  - Message (MSG) instruction - Explicit, CIP Class 3
    - Instruction timeout - 30 second default
  - I/O and Producer/Consumer - Implicit, CIP Class 1
    - Connection timeout - 4 x RPI, with a minimum of 100 ms
  - Safety I/O - Implicit, CIP Class 1
    - Connection timeout - 4 x RPI by default
Don’t forget about potential loops on the switch itself
## Resiliency Protocols and Redundant Topologies

- **Industrial versus COTS - Panel & DIN Rail Mounting vs. Table & Rack (e.g. 1RU)**
- **Managed versus Unmanaged**

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Managed Switches</strong></td>
<td></td>
</tr>
<tr>
<td>▪ Loop prevention</td>
<td>▪ More expensive</td>
</tr>
<tr>
<td>▪ Security services</td>
<td>▪ Requires some level of support and configuration to start up</td>
</tr>
<tr>
<td>▪ Diagnostic information</td>
<td></td>
</tr>
<tr>
<td>▪ Segmentation services (VLANs)</td>
<td></td>
</tr>
<tr>
<td>▪ Prioritization services (QoS)</td>
<td></td>
</tr>
<tr>
<td>▪ Network resiliency</td>
<td></td>
</tr>
<tr>
<td>▪ Multicast management services</td>
<td></td>
</tr>
<tr>
<td><strong>Unmanaged Switches</strong></td>
<td></td>
</tr>
<tr>
<td>▪ Inexpensive</td>
<td>▪ No loop prevention</td>
</tr>
<tr>
<td>▪ Simple to set up</td>
<td>▪ No security services</td>
</tr>
<tr>
<td></td>
<td>▪ No diagnostic information</td>
</tr>
<tr>
<td></td>
<td>▪ No segmentation or prioritization services</td>
</tr>
<tr>
<td></td>
<td>▪ Difficult to troubleshoot</td>
</tr>
<tr>
<td></td>
<td>▪ No network resiliency support</td>
</tr>
<tr>
<td><strong>ODVA Embedded Switch Technology</strong></td>
<td></td>
</tr>
<tr>
<td>▪ Cable simplification with reduced cost</td>
<td>▪ Limited management capabilities</td>
</tr>
<tr>
<td>▪ Ring loop prevention &amp; Network resiliency</td>
<td>▪ May require minimal configuration</td>
</tr>
<tr>
<td>▪ Prioritization services (QoS)</td>
<td></td>
</tr>
<tr>
<td>▪ Time Sync Services (IEEE 1588 PTP Transparent Clock)</td>
<td></td>
</tr>
<tr>
<td>▪ Diagnostic information</td>
<td></td>
</tr>
<tr>
<td>▪ Multicast management services</td>
<td></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>Network Convergence &gt; 250 ms</th>
<th>Network Convergence 60 - 100 ms</th>
<th>Network Convergence 1 - 3 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>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>rPVST+</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>REP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</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>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Flex Links</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></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>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>HSRP</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>GLBP</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VRRP (IETF RFC 3768)</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>
Resiliency Protocols and Redundant Topologies

Device-level Ring Topology with Device Level Ring Protocol
- Supervisor blocks traffic on one port
- Sends Beacon frames on both ports to detect break in the ring
- Once ring is restored, supervisor hears beacon on both ports, and transitions to normal ring mode, blocking one port
Resiliency Protocols and Redundant Topologies

- ODVA - open standard enabling suppliers to develop compatible products
- Support for ring and linear topologies, fiber and copper implementations
- Network traffic is managed to ensure timely delivery of critical data (Quality of Service, IEEE-1588 Precision Time Protocol, Multicast Management)
- Ring is a single fault tolerant network
- Designed for 1-3 ms convergence for simple EtherNet/IP device networks
Resiliency Protocols and Redundant Topologies

- REP segment is a chain of switch ports connected to each other and configured with the same REP segment ID.
- Redundant path ring switch-level topology can be built with REP segments, ring is a single fault tolerant network.
- REP is suitable for IACS applications that can tolerate up to a 100 ms network convergence recovery time (on fiber interfaces).
- Only ring switch-level resiliency protocol applicable to both Industrial Automation and IT applications.
- Cisco innovation, included with Cisco Catalyst 3750-X switch stack, Stratix 5700, 8000 and Stratix 8300.
REP Design Considerations

• REP provides faster convergence (recovery from a failure) than RPVST+ or MSTP for a switch ring topology.
• REP is suitable for IACS applications that can tolerate up to a 100 ms network convergence recovery time (on fiber interfaces).
  – HMI connections
  – I/O and Produce/Consume connections with slow RPIs
  – Not bumpless for fast RPIs
• For IACS applications that require a faster network convergence recovery time, Cisco and Rockwell Automation recommend either a redundant star switch topology with the Flex Links resiliency protocol, or a device-level ring topology utilizing the ODVA DLR resiliency protocol.
• Use fiber media and SFPs for all inter-switch links – ring and redundant star switch-level topologies.
Redundant Path Topology and Resiliency Protocol Design Considerations

• Choice of Redundant Path Topology and Resiliency Protocol is application dependent
  – Switch-level vs. Device-level topologies
  – Ring vs. Redundant Star Topology
  – Mixed switch vendor environment - Legacy Migration
  – Geographic dispersion of EtherNet/IP IACS devices
  – Location within the hierarchal architecture - Layer 2 vs. Layer 3
• Performance
  • Tolerance to: Network Convergence time, Packet loss, Latency & Jitter
Networking Design Considerations

Recommendations and guidance to help reduce network **Latency** and **Jitter**, to help increase the **Availability**, **Integrity** and **Confidentiality** of data, and to help design and deploy a **Scalable, Robust, Secure** and **Future-Ready** EtherNet/IP network infrastructure:

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation / Structure
- Prioritization - Quality of Service (QoS)
- Redundant Path Topologies with Resiliency Protocols
- Time Synchronization – PTP, CIP Sync, CIP Motion
- Multicast Management
- **Convergence-ready Solutions**
- Security – Holistic Defense-in-Depth
- Scalable Secure Remote Access
- Wireless – Wi-Fi
Design and deployment considerations that a trusted partner (e.g. OEM, SI, Contractor) has to take into account to achieve seamless integration of their solution (e.g. machine, skid) into their customers’ plant-wide/site-wide network infrastructure.

Early, open and two-way dialogue is critical!
Convergence-Ready Network Solutions
Design and Implementation Considerations

• Use of a single industrial network technology that fully utilizes standard Ethernet and IP networking technology as the multi-discipline industrial network infrastructure.
  – Common network infrastructure devices – asset utilization
  – Future-ready - sustainability
• IP addressing schema
  – Class - address range, subnet, default gateway (routability)
  – Implementation conventions – static/dynamic, hardware/software configurable, NAT/DNS (who manages?)
• Use of Network Services
  – Managed switches, switch-level and device-level topologies
  – Segmentation, data prioritization
  – Availability – loop prevention, redundant path topologies with resiliency protocols
  – Time Synchronization Services
    • IEEE 1588 Precision Time Protocol (PTP w/E2E)
    • CIP Sync applications – first fault, SOE, CIP Motion
• Security stance
  – Physical access, port security, access control lists, application security (e.g. FactoryTalk Security)
  – Alignment with industrial automation and control system (IACS) security standards such as ISA/IEC-62443 (formerly ISA 99) and NIST 800-82
Convergence-Ready Network Solutions
Design and Implementation Considerations

Enterprise-wide Business Systems

Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ
Industrial Zone

Plant-wide Operation Systems

Physical or Virtualized Servers
- FactoryTalk Application Servers & Services Platform
- Network Services – e.g. DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

Level 3 - Site Operations

Cell/Area Zones
Levels 0-2

EtherNet/IP™

Integrated Services Router

NAT Appliance

Machine/Skid #1

Machine/Skid #2

Machine/Skid #3

VLANs w/ NAT

Copyright © 2014 Rockwell Automation, Inc. All Rights Reserved
Websites
– Reference Architectures

Design Guides
– Converged Plant-wide Ethernet (CPwE)
– CPwE Resilient Ethernet Protocol (REP)

Application Guides
– Fiber Optic Infrastructure Application Guide
– Wireless Design Considerations for Industrial Applications

Whitepapers
– Top 10 Recommendations for Plant-wide EtherNet/IP Deployments
– Securing Manufacturing Computer and Controller Assets
– Production Software within Manufacturing Reference Architectures
– Achieving Secure Remote Access to plant-floor Applications and Data
– Design Considerations for Securing Industrial Automation and Control System Networks
Additional Material

- A ‘go-to’ resource for educational, technical and thought leadership information about industrial network communication
- Standard Internet Protocol (IP) for Industrial Applications
- Coalition of like-minded companies
- Receive monthly e-newsletters with the latest articles and video
- Networks Mythbusters
- eLearning courses will be available at the end of 2014

www.industrial-ip.org
Top 10 Recommendations for Plantwide EtherNet/IP Deployments
1. Understand a networked device’s application and functional requirements. These include data requirements such as communication patterns and traffic types (industrial and nonindustrial).
2. Enable a future-ready network design. Use industry and technology standards, reference models and reference architectures, such as the Cisco and Rockwell Automation Converged Plantwide Ethernet (CPwE) Architectures.
Summary: Top 10 Recommendations for Plantwide EtherNet/IP Deployments

3. Create structure within the plantwide EtherNet/IP network. Develop a logical topology that uses both a multi-tier switch hierarchy. Define zones and segmentation, then place industrial automation and control system devices, servers or other communicating end-devices within the logical topology based on their location, function, availability and performance requirements.
4. Segment the logical topology into modular building blocks.

Create smaller Layer 2 networks to minimize broadcast domains. Use virtual local area networks (VLANs) within a zone to segment different traffic types, such as industrial and nonindustrial. Minimize the number of devices to less than 200 within a zone and VLAN. Use firewalls to strongly segment the manufacturing and enterprise zones, creating a demilitarized zone (DMZ) that enables secure sharing of applications and data between the zones.
5. Use managed industrial switches. These provide key network services such as loop prevention, resiliency, segmentation, prioritization, time synchronization, multicast management, security and diagnostics.
Summary: Top 10 Recommendations for Plantwide EtherNet/IP Deployments

6. Design and implement a robust physical layer reflecting availability and resiliency requirements:
   - Overlay the logical topology over the plant physical layout to create the physical topology.
   - Use 1 gigabit-per-second fiber uplinks and redundant paths between switches for optimal network resiliency.
   - Ensure the end devices and network infrastructure devices communicate at the best possible speed and duplex.
   - Deploy physical cabling corresponding to plant conditions and requirements.
   - Deploy a defense-in-depth approach to help prevent noise coupling through techniques such as bonding, EMI segregation, shield barriers and filtering.

- The M.I.C.E. system is an effective tool that provides necessary information to the design process.

- M.I.C.E. diagramming allows the design to balance component costs with mitigation costs in order to build a robust yet cost-effective system.
7. Determine application and network security requirements. Establish early dialogue with IT, considering applicable IT requirements. Implement a defense-in-depth security approach at multiple application layers such as physical, device, network and application, using an industrial security policy that’s unique from and in addition to the enterprise security policy.
8. Reduce network latency and jitter by using standard network protocols. Protocols include time synchronization using IEEE 1588 precision time protocol (PTP), quality of service (QoS) for control data prioritization and Internet Group Management Protocol for multicast management.
9. Increase control and information data availability. Implement a redundant path network topology such as a ring or redundant star. In addition, use a resiliency protocol to avoid Layer 2 loops while helping to ensure fast network convergence time. These considerations affect how quickly the network will recover from a disruption, which may result in application timeouts and system shutdowns.
10. Deploy a hierarchical network model using Layer 3 switches. Layer 3 switches support inter-VLAN routing between cell/area (Layer 2 network) zones and plantwide applications and servers. Layer 3 switch capabilities enable design recommendation 4. If the application requires industrialized Layer 3 switches, consider products such as the Allen-Bradley® Stratix 8300™ Layer 3 switch.
Top 10 Recommendations for Plantwide EtherNet/IP Deployments
Where can I learn more?

• Sessions
  • NI11 – IT and Plant Floor – Breaking Down the Barriers
  • NI13 – The Connected Enterprise
  • NI03 - Testing the Physical Layer for Ethernet/IP
  • NI04 - When is a good time to have MICE on your plant floor? Structured Cabling Best Practices (Industrial Ethernet)
  • NI18 – Remote Access

• Tradeshow
  • Solution Area 3 – Process & Connected Enterprise
  • Werner DataComm Booths
Questions?