Intelligent Motor Control
Industrial Networks Designs and Considerations

David C. Mazur, P.Eng., Ph.D. & Gregory S. Wilcox

Speakers

David C. Mazur, P.Eng., Ph.D.
Global Technical Consultant
David received his B.S. EE degree summa cum laude and first in his class from Virginia Polytechnic Institute and State University, Blacksburg, VA in 2011. David graduated with his M.S. EE degree in 2012 for his work based on rotor angle measurement of synchronous machines from Virginia Polytechnic Institute and State University. He graduated with his Ph.D. in Mining Engineering in September 2013 for his work with the IEC 61850 standard. He is an active member of the IEEE IAS and serves as working group chair for the Communication-Based Protection of Industrial Applications Working Group. He also serves as a member of the Mining Industry Committee (MIC) as well as the Industrial and Commercial Power Systems Committee (I&CP). David is also an active voting member of the IEEE Standards Association (SA).

Gregory Wilcox
Development Manager for Reference Architectures
Gregory leads a multi-company effort to establish tested and validated design guidelines that helps to reduce risk, simplify design and speed deployment of large-scale industrial automation network infrastructures. As a major contributor to the Cisco and Rockwell Automation Alliance, Gregory has advanced the adoption of convergence between industrial automation technology (IAT) and information technology (IT). Gregory has been designing and implementing industrial automation network solutions for the past 28 years, with 24 of those years at Rockwell Automation, holding roles of increasing responsibility such as Application Engineer and Solution Architect, resulting in extensive experience in developing control and information solutions for industrial applications. Prior to joining Rockwell Automation, Gregory worked in the defense industry developing industrial automation and control system solutions for both discrete and process applications.
Industrial Networks Trends

- Open networks are in demand
  - Broad availability of products, applications and vendor support for Industrial Automation and Control System (IACS)
  - Network standards for coexistence and interoperability of industrial automation devices
- Convergence of network technologies
  - Reduce the number of disparate networks in an operation and create seamless information sharing throughout the plant-wide / site-wide architecture
  - Use of common network design, deployment and troubleshooting tools across the plant-wide / site-wide architecture; avoid special tools for each application

Industrial Networks Trends

- Better asset utilization to support lean initiatives
  - Common network infrastructure assets, while accounting for environmental requirements
  - Reduce training, support, and inventory for different networking technologies
- Future-ready – maximizing investments and minimizing risks
  - Support new technologies and features without a network forklift upgrade
Industrial Applications Convergence

Multi-discipline Industrial Network Convergence

Dispersion Technology

Single Industrial Network Technology

Industrial Network Technology should service...

- **System Integrator**
  - Enable seamless plant-wide / site-wide information sharing
  - Converge industrial and non-industrial traffic

- **Equipment Builder**
  - Enable convergence-ready solutions
  - Use a single multi-discipline control and information platform

- **IT Network Engineer**
  - Use standard Ethernet and TCP/IP
  - Utilize common network infrastructure assets & tools

- **Control System Engineer**
  - Enable future-ready, high performance
  - Use an established, widely accepted network technology supported by leading industry vendors
Network Technology Convergence

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 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

MANAGE / MONITOR

AUDIT

DESIGN/PLAN

Enabling OEM
Convergence-Ready
Solutions

Because Network Infrastructure Matters

IEEE
Cabling Benefits

- UL / cUL listed for use with high voltage power cables
  - 600V cable designed to support high voltage applications
  - UL rated for use in Power Limited Trays
- Provides reliable network connection in harsh conditions
  - Protected from noise, chemicals, thermal and mechanical issues for the harshest possible industrial environments (M3I3C3E3 rated)
  - Foil and braided shield for maximum noise immunity
  - Wide thermal operational range (-20°C ... 80°C)
- Cat 5e cable enables high speed data rate
  - More data can be transferred in a shorter period of time
- Copper cabling standard but fiber can be used for longer runs

Embedded Systems – Rugged Industrial Design

Lightning Strike
- +/- 2KV, 40A surge repeatedly applied to the network cable
- IEC 61000-4-5

Industrial Noise
- +/- 1KV high voltage burst applied to the network cable
- IEC 61000-4-4

Radio Frequency Interference
- 150kHz ... 80MHz interference applied to the network cable
- IEC 61000-4-6

Static Discharge
- +/- 8KV ESD event at 12 locations on the MCC and network cable
- IEC 61000-4-2

No Communication Failures!
No Dropped Packets!
Less Down Time!
Network Design Considerations

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

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation
- Resiliency Protocols and Redundant Topologies
- Time Synchronization
- Prioritization - Quality of Service (QoS)
- Multicast Management
- Convergence-Ready Solutions
- Security - Defense-in-Depth
- Scalable Secure Remote Access

Integrated Architecture

Plant-wide Optimization  Machine Builder Performance
Ethernet/IP: The Industrial Protocol

- ODVA
  - Supported by global industry leaders such as Cisco Systems®, Omron®, Schneider Electric®, Bosch Rexroth AG®, Endress+Hauser and Rockwell Automation
  - Conformance & Performance Testing

- Standard
  - IEEE 802.3 - standard Ethernet
  - Precision Time Protocol (IEEE-1588)
  - IETF - Internet Engineering Task Force, standard Internet Protocol (IP)
  - ODVA - Common Industrial Protocol (CIP)
  - IEC - International Electrotechnical Commission

- Multi-discipline control and information platform
- Established - products, applications and vendors

What’s the difference?

OSI 7-Layer Reference Model

<table>
<thead>
<tr>
<th>Open Systems Interconnection</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>Open Systems Interconnection Protocol (CIP) IEC 61158 ISO 8805</td>
</tr>
<tr>
<td>Presentation</td>
<td>Layer 6</td>
<td>Encryption/Other processing</td>
<td>IETF TCP/UDP TCP/UDP, IP, ICMP, IGMP, UDP, TCP</td>
</tr>
<tr>
<td>Session</td>
<td>Layer 5</td>
<td>Manage Multiple Applications</td>
<td>IETF IP IP, ICMP, IGMP, UDP, TCP</td>
</tr>
<tr>
<td>Transport</td>
<td>Layer 4</td>
<td>Reliable End-to-End Delivery Error Correction</td>
<td>IETF TCP/UDP TCP/UDP, IP, ICMP, IGMP, UDP, TCP</td>
</tr>
<tr>
<td>Network</td>
<td>Layer 3</td>
<td>Packet Delivery, Routing</td>
<td>IETF IP IP, ICMP, IGMP, UDP, TCP</td>
</tr>
<tr>
<td>Data Link</td>
<td>Layer 2</td>
<td>Framing of Data, Error Checking</td>
<td>IEEE 802.3/802.1 Ethernet Frame Format</td>
</tr>
<tr>
<td>Physical</td>
<td>Layer 1</td>
<td>Signal type to transmit bits, pin-outs, cable type</td>
<td>TIA - 1005 TIA-1005 wiring, RJ-45 connector</td>
</tr>
</tbody>
</table>

What makes EtherNet/IP industrial?

5-Layer TCP/IP Model
OSI Reference Model

<table>
<thead>
<tr>
<th>Layer No.</th>
<th>Layer Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 7</td>
<td>Application</td>
<td>CIP</td>
</tr>
<tr>
<td>Layer 6</td>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td>Layer 5</td>
<td>Session</td>
<td></td>
</tr>
<tr>
<td>Layer 4</td>
<td>Transport</td>
<td>IETF TCP/UDP</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Network</td>
<td>IETF IP</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Data Link</td>
<td>IEEE 802.3/802.1</td>
</tr>
<tr>
<td>Layer 1</td>
<td>Physical</td>
<td>TIA - 1005</td>
</tr>
</tbody>
</table>

Protocol Stack

<table>
<thead>
<tr>
<th>Layer No.</th>
<th>Layer Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 7</td>
<td>Application</td>
<td>CIP</td>
</tr>
<tr>
<td>Layer 6</td>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td>Layer 5</td>
<td>Session</td>
<td></td>
</tr>
<tr>
<td>Layer 4</td>
<td>Transport</td>
<td>IETF TCP/UDP</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Network</td>
<td>IETF IP</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Data Link</td>
<td>IEEE 802.3/802.1</td>
</tr>
<tr>
<td>Layer 1</td>
<td>Physical</td>
<td>TIA - 1005</td>
</tr>
</tbody>
</table>

Encapsulation Decapsulation
Encapsulation Example

- The Ethernet message structure is a concatenation of protocols
- EtherNet/IP defines an Encapsulation protocol that sets up the TCP resources

OSI Model: Physical Layer Independent

<table>
<thead>
<tr>
<th>Layer No.</th>
<th>Layer Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 7</td>
<td>Application</td>
<td>CIP</td>
</tr>
<tr>
<td>Layer 6</td>
<td>Presentation</td>
<td>IETF TCP/UDP</td>
</tr>
<tr>
<td>Layer 5</td>
<td>Session</td>
<td>IETF IP</td>
</tr>
<tr>
<td>Layer 4</td>
<td>Transport</td>
<td>IEEE 802.3/802.1</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Network</td>
<td>Copper</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Data Link</td>
<td></td>
</tr>
<tr>
<td>Layer 1</td>
<td>Physical</td>
<td></td>
</tr>
</tbody>
</table>
OSI Model: Data Link Layer

Independent

<table>
<thead>
<tr>
<th>Layer No.</th>
<th>Layer Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 1</td>
<td>Physical</td>
<td>IEEE 802.11 Wi-Fi</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Data Link</td>
<td>IEEE 802.11</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Network</td>
<td>IETF IP</td>
</tr>
<tr>
<td>Layer 4</td>
<td>Transport</td>
<td>IETF TCP/UDP</td>
</tr>
<tr>
<td>Layer 5</td>
<td>Session</td>
<td></td>
</tr>
<tr>
<td>Layer 6</td>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td>Layer 7</td>
<td>Application</td>
<td>CIP</td>
</tr>
</tbody>
</table>

OSI Reference Model: Network

Independent
Network Architectures

- Isolated Network with Single Controller (ODVA)
  - Equipment Builder Solution (Machine or Process Skid)

Linear

Ring

Network Architectures

- Isolated Network with Multiple Controllers (ODVA)
  - Examples
    - Integrated Equipment Builder Solutions
    - Single Cell/Area Zone, Multiple Machines/Lines or Skids/Areas

Linear

Ring
Network Architectures

- Connected and Integrated Control System (ODVA)
- Examples
  - Integrated Equipment Builder Solutions or End User Plant-wide / Site-wide Network
  - Single Cell/Area Zone, Multiple Machines/Lines, Multiple Skids/Areas

Connected and Integrated Control System (ODVA)

Examples
- Integrated Equipment Builder Solutions or End User Plant-wide / Site-wide Network
- Single Cell/Area Zone, Multiple Machines/Lines, Multiple Skids/Areas

Convergence-Ready

Topology Layouts
Network Architectures

Network Architectures: Site-to-Site Connection

- Broad geographic area
  - WAN Examples:
    - Point-to-Point Link – PSTN Leased Lines – T1, E1
    - Circuit Switching - ISDN
    - Packet Switching - Frame Relay, Broadband DSL, Broadband Cable
  - Higher Latency
    - Use case examples – HMI and Data Collection
Benefits of Ethernet/IP

- Single industrial network technology for:
  - Multi-discipline Network Convergence - Discrete, Continuous Process, Batch, Drive, Safety, Motion, Power, Time Synchronization, Supervisory Information, Asset Configuration/Diagnostics, and Energy Management
- Established - 375+ vendors, over 7,500,000 nodes
  - Risk reduction - broad availability of products, applications and vendor support
  - ODVA: Cisco Systems, Endress+Hauser, Rockwell Automation are principal members
  - Supported - Defined QoS priority values for EtherNet/IP devices

Benefits of EtherNet/IP

- Standard - IEEE 802.3 Ethernet and IETF TCP/IP Protocol Suite
  - Enables convergence of IAT and IT - voice, video and data - common toolsets (assets for design, deployment and troubleshooting) and skills/training (human assets)
  - Topology and media independence - flexibility and choice
  - Device-level and switch-level topologies; copper - fiber - wireless
- Portability and routability - seamless plant-wide / site-wide information sharing
  - No data mapping - simplifies design, speeds deployment and reduces risk
- Common industrial application layer protocol
  - DeviceNet, ControlNet and EtherNet/IP - seamless bridging throughout CIP networks
Automatic Device Configuration

Saves the End-User time / money by reducing down-time

Intelligent Motor Control
Real Time Network Design and Segmentation

David C. Mazur, P.Eng., Ph.D. & Gregory S. Wilcox
Application Requirements

- What is real-time?
  - Application dependent ... only you can define what this means for your application.

<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>Communication Technology</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>Period</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>Industries</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>Applications</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

Network Technology Convergence

- Theoretical Ethernet @ 100 Mbps
  - Short frame with 64 bytes (1 bit – 10ns)
    ≈ 148,000 frames/second
  - Long frames with 1518 bytes
    ≈ 8,000 frames/second
- Theoretical EtherNet/IP @ 100 Mbps
  - Typical I/O frame size (64 byte + 36 byte I/O data) ≈ 104,000 frames/second
  - Maximum I/O frame size (64 byte + 511 byte I/O data) ≈ 21,000 frames/second
    - Normal CIP Forward_Open
- I/O Scanner exchanges 36 bytes of I/O data with 10 I/O adapters every 1 ms
  - The I/O Scanner must be able to:
    - Consume 10,000 frames/second
    - Product 10,000 frames/second

Design considerations you should consider

- Performance of Scanner
  - Maximum # of Adapters (CIP Connections)
  - Minimum RPI (how fast)
  - Maximum I/O Data Size per RPI
- Performance of Adapters
  - Minimum RPI (how fast)
  - Maximum I/O Data Size per RPI
- Network Infrastructure Latency and Jitter
- Speed / Duplex
- Physical Environment – e.g., EMI Interference

This represents about 10% of the total network bandwidth
Segmentation

- 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
**Structure and Hierarchy**

The Cell/Area zone is a Layer 2 network for a functional area (plant-wide or site-wide).

Key network considerations include:

- Structure and hierarchy using smaller Layer 2 building blocks
- Logical segmentation for traffic management and policy enforcement (e.g., QoS, Security) to accommodate time-sensitive applications
### Islands of Automation with Isolated Networks

- **Islands of Automation**

  ![Sneakernet](image)

- **Benefits**
  - Clear network ownership demarcation line

- **Challenges**
  - Limited visibility to control network devices for asset management
  - Limited future-ready capability

### Segmentation – Multiple Network Interface Cards

- **Isolated networks – two NICs for physical network segmentation**

  ![Diagram of isolated networks](image)

  - **Benefits**
    - Plant-wide information sharing for data collection and asset management
    - Future-ready
  - **Challenges**
    - Blurred network ownership demarcation line

- **Converged networks – logical segmentation**

  ![Diagram of converged networks](image)

  - **Benefits**
    - Plant-wide information sharing for data collection and asset management
    - Future-ready
  - **Challenges**
    - Blurred network ownership demarcation line
Segmentation

- Isolated networks - two NICs for physical network segmentation
  - **Benefits**
    - Clear network ownership demarcation line
  - **Challenges**
    - Limited visibility to control network devices for asset management
    - Limited future-ready capability
    - Smaller PACs may not support

- Converged networks - logical segmentation - two NICs for scalability, performance, capacity and flexibility
  - **Benefits**
    - Plant-wide information sharing for data collection and asset management
  - **Challenges**
    - Blurred network ownership demarcation line
    - Converged networks - logical segmentation - two NICs for scalability, performance, capacity and flexibility

Network Address Translations (NAT) Appliance

- Segmented Networks - Layer 2 (e.g. VLAN) and Layer 3 (e.g. subnet)
- Smaller Layer 2 building blocks
Virtual Local Area Networks (VLANs)

- Layer 2 network service, VLANs segment a network logically without being restricted by physical connections
  - VLAN established within or across switches
- Data is only forwarded to ports within the same VLAN
  - Devices within each VLAN can only communicate with other devices on the same VLAN
- Segments traffic to restrict unwanted broadcast and multicast traffic
- Software configurable using managed switches

Benefits
- Ease network changes – minimize network cabling
- Simplifies network security management - domains of trust
- Increase efficiency

VLANs

- Layer 2 VLAN Trunking
  - Independent of physical switch location
  - Logically group assets by type, role, logical area, physical area or a hybrid of these
  - Devices communicate as if they are on the same physical segment – no re-cabling required
- Software configurable using managed switches

- A Layer 3 device (Router or Layer 3 switch) is required to forward traffic between different VLANs
  - Inter-VLAN routing
**VLANs**

- **Multi-Layer Switch**
  - Layer 2 VLAN Trunking
  - Layer 3 Inter-VLAN routing

![Diagram of VLANs]

**VLAN Trunking**

- **VLAN Trunking Protocol (VTP)**
  - Provides centralized VLAN management, runs only on trunks
  - Three modes:
    - Server: updates clients and servers
    - Client: receive updates - cannot make changes
    - Transparent: allow updates to pass through

- Use VTP transparent mode to decrease potential for operational error
  - Configured by default on Stratix 5700/8000/8300
  - Define VLANs at each switch, no centralized management
**VLAN Example**

- Smaller Layer 2 building blocks
- Isolated Network with Multiple Controllers (ODVA)
  - Examples:
    - Single Cell/Area Zone, Single Line, Multiple Machines (vendors)

**No Segmentation (Not Recommended)**

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

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

NAT Segmentation

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

<table>
<thead>
<tr>
<th>Segmentation Techniques</th>
<th>Positive Design Considerations</th>
<th>Negative Design Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Segmentation (Not Recommended)</td>
<td>• Initially, may appear to be simpler to design and deploy</td>
<td>• Same Layer 2 broadcast and fault domain, not a scalable or future-ready solution</td>
</tr>
<tr>
<td></td>
<td>• Link Resiliency (redundant path topologies)</td>
<td>• Every node requires a unique IP address</td>
</tr>
<tr>
<td>Multiple NIC Segmentation</td>
<td>• Simple to design and deploy</td>
<td>• Not scalable or future-ready, only CIP traffic can traverse a CIP bridge, limited quantity of bridge modules</td>
</tr>
<tr>
<td></td>
<td>• Smaller Layer 2 domains (broadcast and fault)</td>
<td>• Smaller PACs do not support a dual NIC</td>
</tr>
<tr>
<td></td>
<td>• Reusable IP addresses / subnets</td>
<td>• No Link Resiliency (redundant path topologies)</td>
</tr>
<tr>
<td></td>
<td>• Clear demarcation line of network ownership</td>
<td></td>
</tr>
<tr>
<td>NAT Appliance Segmentation (9300-ENA)</td>
<td>• Smaller Layer 2 domains (broadcast and fault)</td>
<td>• More difficult to design, deploy and manage - manual entry and management of IP address translations</td>
</tr>
<tr>
<td></td>
<td>• Reusable IP addresses / subnets</td>
<td>• No Link Resiliency (redundant path topologies)</td>
</tr>
<tr>
<td></td>
<td>• Clear demarcation line of network ownership</td>
<td></td>
</tr>
<tr>
<td>Unified Threat Management Security Appliance (Stratix 5900)</td>
<td>• Smaller Layer 2 domains (broadcast and fault)</td>
<td>• More difficult to design, deploy and manage - manual entry and management of IP address translations</td>
</tr>
<tr>
<td></td>
<td>• Reusable IP addresses / subnets</td>
<td>• No Link Resiliency (redundant path topologies)</td>
</tr>
<tr>
<td></td>
<td>• Clear demarcation line of network ownership</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enhanced security features</td>
</tr>
<tr>
<td>VLANs Only Segmentation (Stratix 5700)</td>
<td>• Scalable and future-ready</td>
<td>• Layer 3 switch or router is required to forward (route) information between VLANs</td>
</tr>
<tr>
<td></td>
<td>• Smaller Layer 2 domains (broadcast and fault)</td>
<td>• Every node requires a unique IP address</td>
</tr>
<tr>
<td></td>
<td>• Smaller domains of trust (management of security policies)</td>
<td>• Blurred demarcation line of network ownership</td>
</tr>
<tr>
<td></td>
<td>• Link Resiliency (redundant path topologies)</td>
<td></td>
</tr>
<tr>
<td>VLAN Segmentation with NAT (Stratix 5700)</td>
<td>• Scalable and future-ready</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Smaller Layer 2 domains (broadcast and fault)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Smaller domains of trust (management of security policies)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reusable IP addresses / subnets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link Resiliency (redundant path topologies)</td>
<td></td>
</tr>
</tbody>
</table>

Industrial Traffic 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Random Drop Sensitivity</th>
<th>High</th>
<th>Low</th>
<th>High</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<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.
Quality of Service (QoS)

- QoS helps mitigate the following network issues:
  - End-to-end delay
    - Fixed delay – latency
    - Variable delay – jitter
  - Bandwidth capacity issues
  - 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

Quality of Service (QoS)

- QoS classification based on Layer attributes:
  - Layer 2 Destination MAC Address
  - Layer 2 EtherType
  - Layer 3 Source / Destination IP Address
  - Layer 4 TCP / UDP Source or Destination Port Number

- ODVA EtherNet/IP QoS Specification
  - Layer 2 ... Class of Service (CoS) ... 802.1Q/p
  - Layer 3 ... type of service (ToS) ... DiffServ Code Point (DSCP)
### QoS ODVA and DSCP and CoS Priority values

<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></td>
<td>Scheduled (2)</td>
<td>47</td>
<td>5</td>
<td>Safety I/O</td>
</tr>
<tr>
<td></td>
<td>High (1)</td>
<td>43</td>
<td>5</td>
<td>I/O</td>
</tr>
<tr>
<td></td>
<td>Low (0)</td>
<td>31</td>
<td>3</td>
<td>No recommendations at present</td>
</tr>
<tr>
<td>CIP UCMM</td>
<td>All</td>
<td>27</td>
<td>3</td>
<td>CIP messaging</td>
</tr>
</tbody>
</table>

### Prioritization

**Typical Enterprise QoS**
- Priority Queue, Queue 1: Voice, Video, Call Signaling, Network Control, Critical Data, Best Effort
- Output Queue 2: Video, Call Signaling, Network Control, Critical Data, Best Effort
- Output Queue 3: Best Effort, Bulk Data, Scavenger
- Output Queue 4: Bulk Data, Scavenger

**Cell/Area Zone QoS**
- PTP-Event: Voice, CIP Motion
- CIP Explicit Messaging, Call Signaling
- PTP Management, Safety I/O & I/O
- Network Control
- Output Queue 1: Voice, CIP Motion
- Output Queue 2: Voice, CIP Motion
- Output Queue 3: Video, Critical Data, Bulk Data, Best Effort, Scavenger
- Output Queue 4: Critical Data, Bulk Data, Best Effort, Scavenger

Note: Due to queue characteristics of the Stratix 5700/8000/8300, the queue order of priority is different than general enterprise switch.
QoS Design 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

QoS Concluding Thoughts

- 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
Intelligent Motor Control

Designing Resilient, Fault Tolerant Industrial Networks

David C. Mazur, P.Eng., Ph.D. & Gregory S. Wilcox

Layer 2 Loop Avoidance Resiliency Schemes

Switch-level Topologies

Device-level Topologies
Layer 2 Loop Avoidance Resiliency Schemes

![Diagram showing Layer 2 Loop Avoidance Resiliency Schemes]

<table>
<thead>
<tr>
<th>Schemes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Loop Avoidance Resiliency</td>
</tr>
<tr>
<td>Flex Links</td>
</tr>
<tr>
<td>Star</td>
</tr>
<tr>
<td>Redundant</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implementation Costs</th>
<th>Redundant Star</th>
<th>Ring</th>
<th>Linear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Redundant Star</td>
<td>Ring</td>
<td>Linear</td>
</tr>
<tr>
<td>Redundancy and Convergence</td>
<td>Redundant Star</td>
<td>Ring</td>
<td>Linear</td>
</tr>
<tr>
<td>Disruption During Network Upgrade</td>
<td>Redundant Star</td>
<td>Ring</td>
<td>Linear</td>
</tr>
<tr>
<td>Readiness for Network Convergence</td>
<td>Redundant Star</td>
<td>Ring</td>
<td>Linear</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overall in Network TCO and Performance</th>
<th>Best</th>
<th>OK</th>
<th>Worst</th>
</tr>
</thead>
</table>

Layer 2– Loop Avoidance

- **Rockwell Automation**
  - Stratix 5700/8000
  - Managed Industrial Layer 2 Access Switch
- **Rockwell Automation**
  - ControlLogix Programmable Automation Controller

**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
Layer 2 Loop Avoidance

- A Layer 2 resiliency protocol maintains redundant paths while avoiding switching (bridging) loop.

Layer 2 Loop Avoidance

- Network convergence (healing, recovery, etc.) must occur before the Industrial Automation and Control System (IACS) application is impacted.
Network Convergence

- Network convergence (healing, recovery, etc.) time – is a measure of how long it takes to detect a fault, find an alternate path, then start forwarding network traffic across that alternate path.
  - MAC tables must be relearned
  - Multicast on uplinks must be relearned
- During the network convergence time, some portion of the traffic is dropped by the network because interconnectivity does not exist.
- If the convergence time is longer than the Logix controller connection timeout, the IACS EtherNet/IP devices on the affected portion of the network may stop operating and may affect the industrial automation application.

Example 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
    - KB #18945 - ControlLogix MSG instruction timeout values
  - 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
Layer 2 Loop Avoidance

Don’t forget about potential loops on the switch itself

Switching Options

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

<table>
<thead>
<tr>
<th>Managed Switches</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
|                  | • Loop prevention  
|                  | • Security services  
|                  | • Diagnostic information  
|                  | • Segmentation services (VLANs)  
|                  | • Prioritization services (QoS)  
|                  | • Network resiliency  
|                  | • Multicast management services  | • More expensive  
|                  |                                           | • Requires some level of support and configuration to start up |

<table>
<thead>
<tr>
<th>Unmanaged Switches</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
|                    | • Inexpensive  
|                    | • Simple to set up  | • No loop prevention  
|                    |                                           | • No security services |
|                    |                                           | • No diagnostic information |
|                    |                                           | • No segmentation or prioritization services |
|                    |                                           | • Difficult to troubleshoot |
|                    |                                           | • No network resiliency support |

<table>
<thead>
<tr>
<th>ODVA Embedded Switch Technology</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
|                                | • Cable simplification with reduced cost  
|                                | • Ring loop prevention & Network resiliency  
|                                | • Prioritization services (QoS)  
|                                | • Time Sync Services (IEEE 1588 PTP Transparent Clock)  
|                                | • Diagnostic information  
|                                | • Multicast management services  | • Limited management capabilities  
|                                |                                           | • May require minimal configuration |
Network Resiliency Protocols

- **Device-level Topology**
  - Ring
    - Embedded switch technology EtherNet/IP IACS devices
    - Device Level Ring (DLR) Protocol – IEC & ODVA

- **Switch-level Topology**
  - Ring or Redundant Star
    - Spanning Tree Protocol (STP), Rapid STP (RSTP), Multiple instance STP (MSTP) – IEEE
      - Stratix 5700/8000/8300 – MSTP - default
      - Rapid Per VLAN Spanning Tree Plus (rPVST+) - Cisco Technology
  - Ring Only
    - Resilient Ethernet Protocol (REP) – Cisco Technology
  - Redundant Star Only
    - EtherChannel
      - Link Aggregation Control Protocol (LACP) - IEEE
    - Flex Links – Cisco Technology

Distribution switches typically provide first hop (default gateway) redundancy
- StackWise (3750X), stack management
- Hot Standby Router Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)
- Gateway Load Balancing Protocol (GLBP)
## Network Resiliency Protocols

<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></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></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></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PVST+</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EtherChannel (LACP 802.3ad)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flex Links</td>
<td>X</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>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>StackWise</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HSRP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GLBP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRRP (IETF RFC 3768)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Resilient Ethernet Protocol (REP)

REP segments apply to various Layer 2 Topologies

[Diagram of network topology showing REP segments and forwarding vs. blocking]