Reference Architectures for Industrial Automation and Control systems

Paul Didier, Cisco Systems

Technical Track
Isolated Single Controller
• Single Controller
• 10s of devices
• Potentially multiple switches
• Limited non-CIP traffic
• Sharing data via sneaker net or transferable device

Isolated Multiple Controller
• Multiple Controllers
• Up to 100s of devices
• 10s of switches, maybe a router
• A few networks
• Potentially multiple switches
• Controllers sharing data
• Some non-CIP traffic (e.g. HTTP, file sharing, etc.)

Enterprise Connected
• Many Controllers
• Up to 1000s of devices
• Lots of switches and routers and other network infrastructure
• Many “networks”
• Sharing data, applications and services between Enterprise and Plant networks
• Could have lots of non-CIP traffic (e.g. Voice, Video, etc.)
Agenda

Benefits of Reference Architecture

Overview

Topology and Resilience

Multicast Management and IGMP

Prioritization and QoS

Routing & Layer 3

Security
**Manufacturing 2.0: Plant Operations Transformation**

<table>
<thead>
<tr>
<th>Integrated Business and Plant Data …Multi-Site</th>
<th>Real-Time Asset Tracking, Monitoring, and Notification</th>
<th>Collaborative Tools and Processes</th>
<th>Enhanced Security and Personnel Tracking</th>
<th>IT and Control System Flexibility</th>
<th>Mobile and Remote Workers</th>
<th>Sensor Enabled Manufacturing</th>
</tr>
</thead>
</table>

- **Traditional Plant**
  - Restricted and Isolated Static Environment
  - "Solid State"

- **Plant of the Future**
  - Dynamic, Integrated Mobile, Real-Time Connected Environment
  - "Liquid State"

Source: AMR, Industry Week, Cisco Analysis
Manufacturing and IT Convergence
Creating Challenges and Opportunities

- Technology Convergence
- Network Convergence
- Organizational Convergence
- Cultural Convergence

Business Model Innovation
- Business Agility
- Competitive Advantage
### Challenges with Manufacturing Convergence

#### Organizational Issues
- Misaligned objectives
- Support requirements
- Different models and language

#### Industrial Applications
- Industrial protocols and traffic patterns
- Hardened products
- Determinism, latency, etc.
- Motion control

#### Security
- Increased risk with COTS technology
- Patching issues
- Implications of issues
- Impact on performance & ease of use

#### MFG and IT Skill Alignment
- Ease of use
- Multiple management tools
- Understanding of industrial applications

---

**Challenges**

- Misaligned objectives
- Support requirements
- Different models and language
- Industrial protocols and traffic patterns
- Hardened products
- Determinism, latency, etc.
- Motion control
- Increased risk with COTS technology
- Patching issues
- Implications of issues
- Impact on performance & ease of use
- Ease of use
- Multiple management tools
- Understanding of industrial applications
## Logical Architecture

**Built on Industry Standards**

<table>
<thead>
<tr>
<th>Zone</th>
<th>Network/Operations</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enterprise Zone</strong></td>
<td>Enterprise Network</td>
<td>Level 5</td>
</tr>
<tr>
<td></td>
<td>Site Business Planning and Logistics Network</td>
<td>Level 4</td>
</tr>
<tr>
<td><strong>DMZ</strong></td>
<td>Demilitarized Zone—Shared Access</td>
<td></td>
</tr>
<tr>
<td><strong>Manufacturing Zone</strong></td>
<td>Site Manufacturing Operations and Control</td>
<td>Level 3</td>
</tr>
<tr>
<td><strong>Cell/Area Zone</strong></td>
<td>Area Control</td>
<td>Level 2</td>
</tr>
<tr>
<td></td>
<td>Basic Control</td>
<td>Level 1</td>
</tr>
<tr>
<td></td>
<td>Process</td>
<td>Level 0</td>
</tr>
</tbody>
</table>
Converged Plantwide Ethernet Architecture

Enterprise Network Levels 4–5
Enterprise/IT Integration
Collaboration
Wireless
Application Optimization

Demilitarized Zone (DMZ) Firewalls
Application and Data share
Access Control
Threat Protection

Manufacturing Zone Level 3 Distribution and Core
Site Operations and Control
Multi-Service Networks
Network and Security Management
Routing

Cell/Area Zone Levels 0–2 Layer 2 Access
EtherNet/IP (Industrial Protocols)
Real–Time Control
Fast Convergence
Traffic Segmentation and Management
Ease of Use
The Cell/Area Zone is a Layer 2 network for a functional area of a production facility. Key network considerations include:

- Environmental constraints
- Range of device intelligence
- Time-sensitive applications
Networking Best Practices – Cell/Area Zone

Best Practices For Reducing Latency and Jitter, and to Increase Data Availability, Integrity and Security

IP Multicast Control
- IGMP Management

Segmentation
- Virtual LANs (VLANs)

Prioritization
- Quality of Service (QoS)

Apply Resiliency Protocols and multi-path topologies
- Use Fiber-media uplinks for fast convergence

Defense-in-Depth Security
Cell/Area Traffic Flows

- Cell/area traffic is predominately (>80%) local, cyclical I/O (a.k.a. Implicit) traffic
  - Producers generated UDP multi-cast messages
  - Consumer generated UDP uni-cast messages
  - Packets are small: 100-200 Bytes, but communicated very frequently (every 0.5 to 10’s of ms).
  - Typically un-routable (TTL=1 by application)

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

<table>
<thead>
<tr>
<th>Requirement Class</th>
<th>Target Cycle Time</th>
<th>Target RPI</th>
<th>Target Network Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information/Process (e.g. HMI)</td>
<td>&lt; 1 s</td>
<td>100 - 250 ms</td>
<td>&lt; 1 sec</td>
</tr>
<tr>
<td>Time critical processes (e.g. I/O)</td>
<td>30 - 50 ms</td>
<td>20 ms</td>
<td>&lt; 40 ms</td>
</tr>
<tr>
<td>Safety</td>
<td>10 - 30 ms</td>
<td>10 ms</td>
<td>&lt; 15 ms</td>
</tr>
<tr>
<td>Motion</td>
<td>500 µs - 5ms</td>
<td>50 µs - 1 ms</td>
<td>&lt; 1ms</td>
</tr>
</tbody>
</table>
Resiliency for Industrial Applications
Supporting Multiple Topologies

Ring Convergence
- Resilient Ethernet Protocol (REP)
- Achieves ~50 ms convergence in large, complex networks

Redundant Star Convergence
- Multiple protocol options
- Convergence times of <100ms for Flexlinks and Etherchannel

Tested with Rockwell applications and multicast traffic
Fast convergence avoids application reset and improves uptime
Critical for industrial applications
Reliability, Availability and Network Segmentation Cell/Area Zone Topology Options

<table>
<thead>
<tr>
<th>Cabling Requirements</th>
<th>Redundant Star</th>
<th>Ring</th>
<th>Linear</th>
</tr>
</thead>
<tbody>
<tr>
<td>East of Configuration</td>
<td>Red</td>
<td>Red</td>
<td>Green</td>
</tr>
<tr>
<td>Implementation Costs</td>
<td>Red</td>
<td>Red</td>
<td>Green</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
</tr>
<tr>
<td>Redundancy and Convergence</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
</tr>
<tr>
<td>Disruption During Network Upgrade</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
</tr>
<tr>
<td>Readiness for Network Convergence</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
</tr>
<tr>
<td>Overall in Network TCO and Performance</td>
<td>Best</td>
<td>OK</td>
<td>Worst</td>
</tr>
</tbody>
</table>
Spanning Tree Protocol (STP)

Most common standard protocol for network resiliency—IEEE 802.1D

Supports Redundant Star and Ring Topology

Provides alternate path in case of failures, avoiding loops

Unmanaged switches don’t support STP

Versions: STP, RSTP, MSTP and RPVST+ - there are differences

Coordinate with IT before implementing
Layer 2 Hardening
Spanning Tree Should Behave the Way You Expect

- Place the root where you want it—
  Distribution Switch
- Root primary/secondary macro
- The root bridge should stay where you put it
  - RootGuard
  - LoopGuard
  - UplinkFast
  - UDLD
- Only end-station traffic should be seen on an edge port
  - BPDU Guard
  - RootGuard
  - PortFast
  - Port-security
- Standard setup applies the above
EtherChannel

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

Cell/Area Zone Topology Options

- Use Fiber over Copper for uplinks
- Spanning Tree (MSTP) recovery in Ring topology for CIP Explicit Messaging such as HMI
- LACP in Redundant Star for CIP Implicit I/O applications
- Device Level Ring for device connectivity
Multicast Protocols

- IGMP—Internet Group Management Protocol
- IGMP snooping is used to prevent multicast from flooding all ports on a VLAN. It monitors the IGMP packets from end devices
  - IGMP snooping becomes operational as soon as a Querier is detected
  - A Layer 2 access switch can act as an IGMP querier
  - Recommendation to select the distribution switch as acting querier by giving it the lowest IP on the VLAN
- Make sure IT is aware of multicast requirements
- IE switch enables IGMP in standard setup
  - IGMP v2, Querier and Snooping
  - Standard setup applies the above
IP Multicast Group Concept

- The device must join a group in order to receive its data
- All members of a group receive the same data
- A device can send to a group without being a member of that group
IGMP Snooping Summary

- In a Consumer-Producer Model traffic grows exponentially with the number of hosts unless multicasts are constrained.
- IGMP Snooping provides scalability for Consumer-Producer Data Models by limiting the amount of multicast traffic.
- Performance benefits of the Consumer-Producer model are maintained (all consumers have equal access to data).
VLANs in an Industrial Ethernet System

Assign VLANs to devices when traffic patterns are known

Limit the flow of produce of required devices (e.g.: one VLAN per cell or zone)

Use L3 switch such as IE 3000 to exchange data between VLANs (i.e. PLC interlock layer)

Learn Your Traffic Patterns: Safemap.Sourceforge.Net
VLAN Considerations for Cell/Area zone

Design small Cell/Area zones, segment traffic types into VLANs and IP Subnets to better manage the traffic

Requires Layer-3 switch or router to communicate between VLANs

Use Layer 2 VLAN trunking between switches

► When trunking, use 802.1Q, VTP in transparent mode
► Set native VLAN to something other than 1

Use switchport mode host command to assign VLAN to end device

► Do not use VLAN 1 for EtherNet/IP Control & Information Traffic

Enable IP directed Broadcast on Cell/Area VLANs with EtherNet/IP traffic for easy configuration and maintenance from IACS applications

Prune unused VLANs for security

► Use VLAN 1 for data is viewed as a security risk

Create a Network Management VLAN, don’t use VLAN 1
Not All Traffic Is Created Equal
Prioritization Is Required

Control Networks Must Prioritize Control Traffic over Other Traffic Types to Ensure Deterministic Data Flows with Low Latency and Low Jitter

<table>
<thead>
<tr>
<th></th>
<th>Control (e.g., CIP)</th>
<th>Video</th>
<th>Data (Best Effort)</th>
<th>Voice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bandwidth</strong></td>
<td>Low to Moderate</td>
<td>Moderate to High</td>
<td>Moderate to High</td>
<td>Low to Moderate</td>
</tr>
<tr>
<td><strong>Random Drop Sensitivity</strong></td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Latency Sensitivity</strong></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td><strong>Jitter Sensitivity</strong></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>
Quality of Service Operations

Classification and Marking  Queuing and (Selective) Dropping  Post-Queuing Operations
Cell/Area Zone QoS Priorities

Output Queue traffic prioritization

Typical Enterprise QoS

Priority Queue 1
- Voice
- Video

Priority Queue 2
- Call Signaling
- Network Control

Priority Queue 3
- Critical Data
- Best Effort

Priority Queue 4
- Bulk Data
- Scavenger

Cell/Area Zone QoS

Priority Queue 1
- PTP-Event

Output Queue 3
- CIP Motion
- PTP Management, Safety I/O and I/O

Output Queue 4
- Network Control
- Voice
- CIP Explicit Messaging

Output Queue 2
- Call Signaling
- Video
- Critical Data
- Bulk Data
- Best Effort
- Scavenger

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

- Priority for latency and jitter sensitive CIP I/O traffic
  Guaranteed delivery for CIP sync, CIP motion
  Minimize impacts by DDoS attacks
- QoS deployed throughout industrial network
- QoS trust boundary moves from switch access ports to QoS-capable CIP devices
- For existing CIP devices, marking at the access port is based on port number
  CIP I/O UDP 2222
  CIP Explicit TCP 44818
## IP Addressing Management

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>All devices hard coded with an IP Address</td>
<td>▪ Simple to commission and replace</td>
<td>▪ In large environments, can be burdensome to maintain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Limited ranged of IP addresses and subnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Not all devices support</td>
</tr>
<tr>
<td>Static via BOOTP Configuration</td>
<td>Server assigns devices IP addresses Precursor to DHCP</td>
<td>▪ Supported by every device</td>
<td>▪ Requires technician to configure IP address/Mac address when a device is replaced</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Adds complexity and point of failure</td>
</tr>
<tr>
<td>DHCP</td>
<td>Server assigns IP addresses from a pool</td>
<td>▪ Efficient use of IP address range</td>
<td>▪ More complex to implement and adds a point of failure</td>
</tr>
<tr>
<td></td>
<td>(NOT RECOMMENDED for Cell/Area devices)</td>
<td>▪ Can reduce administration work load</td>
<td>▪ Devices get different IP addresses when they reboot</td>
</tr>
<tr>
<td>DHCP Option 82</td>
<td>Server assigns consistent IP addresses from a pool</td>
<td>▪ Efficient use of IP Address range</td>
<td>▪ More complex to implement and adds a point of failure</td>
</tr>
<tr>
<td></td>
<td>(NOT RECOMMENDED)</td>
<td>▪ Can reduce administration work load</td>
<td>▪ Mixed environments may not work</td>
</tr>
</tbody>
</table>
Manufacturing Zone Overview

- Highly available Layer 3, routing services for the Plant network
  - Provides inter Cell/Area zone connectivity
  - Interconnectivity to the DMZ
  - Network and Security management

- Level 3 Plantwide applications including the Factory Talk suite
  - Key network-based services such as Access and Authentication (e.g. Active Directory), DHCP, DNS, etc.
  - Remote Access Server
Distribution Layer
Policy, Convergence, QoS, and High Availability

- Availability, load balancing, QoS and provisioning are the important considerations at this layer
- Aggregates Cell/Area zones (access layer) and uplinks to core
- Protects core from high density peering and problems in access layer
- Route summarization, fast convergence, redundant path load sharing
- HSRP or GLBP to provide first hop redundancy
Core Layer
Scalability, High Availability, and Fast Convergence

- Backbone for the network—connects network building blocks
- Performance and stability vs. complexity—less is more in the core
- Aggregation point for distribution layer
- Separate core layer helps in scalability during future growth
- Keep the design technology-independent
Manufacturing Zone Scalability

**Small**
- Collapsed Core/Distribution
- 30-50 Access switches

**Medium**
- Collapsed Core/Distribution
- <200 Access Switches

**Large**
- Distinct Core/Distribution
- >200 Access Switches
Routing Design
Core and Distribution Routing Design

- Good routing design forms the foundation of the HA campus design
- Needed to quickly re-route around failed node/links while providing load balancing over redundant paths
- Build triangles not squares for deterministic convergence
- Only peer on links that you intend to use as transit
- Insure redundant L3 paths to avoid black holes
- Map the protocol design to the physical design
The greatest advantages of EIGRP are gained when the network has a structured addressing plan that allows for use of summarization and stub routers.

EIGRP provides the ability to implement multiple tiers of summarization and route filtering.

Relatively painless to migrate to a L3 access with EIGRP if network addressing scheme permits.

Able to maintain a deterministic convergence time in very large L3 topology.
The basic EIGRP design rules apply irregardless if the access is L2 or L3

- Minimize the number and time for query response to speed up convergence
- Summarize distribution block routes upstream to the core
- Summarize at every major network tier

```
interface TenGigabitEthernet 4/1
  ip summary-address eigrp 100 10.120.0.0 255.255.0.0 5
router eigrp 100
network 10.0.0.0
  passive interface <access-layer interface>
```
Design Principles—Plant Routing

Manage Your Routing Protocol

- Manage your routing protocol don’t let it manage you
- It is easy to just turn it on and forget because it works
- Optimize your configuration to ease management and improve convergence
- Manage:
  - Router peering
  - Route summarization
  - Route propagation
  - Failure notifications (LSA and queries)
  - Protocol timers

E.G. Prevent Peering Through the Access:

```bash
Router(config)#router eigrp 1
Router(config-router)#passive-interface Vlan 99
```

```bash
Router(config)#router eigrp 1
Router(config-router)#passive-interface default
Router(config-router)#no passive-interface Vlan 99
```
Logical Framework

**Strong Segmentation**

<table>
<thead>
<tr>
<th>Level 5</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail, Intranet, etc.</td>
<td>Site Business Planning and Logistics Network</td>
</tr>
</tbody>
</table>

**Level 3**
- Application Server
- Factory Directory
- Engineering Workstation
- Domain Controller
- Site Manufacturing Operations and Control

**Level 2**
- Factory Client
- Operator Interface
- Engineering Workstation
- Operator Interface
- Basic Control

**Level 1**
- Batch Control
- Discrete Control
- Drive Control
- Continuous Process Control
- Safety Control

**Level 0**
- Sensors
- Drives
- Actuators
- Robots
- Process

**Enterprise Zone**
- Web E-Mail CIP
- DMZ

**Enterprise Network**
- Purdue Reference Model, ISA-95
- ISA-99
DMZ Deployment
Components and Traffic Flow

Legend:
- Layer 3 link – no switchport, IP address assigned
- Layer 2 interswitch uplink – VLAN Trunk, Layer 2 resiliency
- Layer 2 access link – VLAN assigned to port
- Allowed Firewall traffic flows

DMZ Servers and Applications

Plant Firewall:
- Inter-zone traffic segmentation
- ACLs
- IPS & IDS
- VPN Services
- Portal and Terminal Server proxy

Enterprise Zone

DMZ Switches

Core Routers 6500 / 4500

Remote Access Server

Authentication, Security Management

Patch Management
Terminal Services
Application Mirror
AV Server

Manufacturing zone
DMZ and Secure Remote Access

Guiding Principals

Use IT-Approved Access and Authentication
- VPN for secure remote access
- Enterprise Access and Authentication servers (e.g., Active Directory, Radius, etc.)

IACS Protocols Stay home
Control the Application
- Remote Access Server
- Application level security

No direct traffic
No common protocols
Only one path in and out of manufacturing zone—the firewalls
Secure Remote Access

- Remote engineer or partner establishes VPN to corporate network; access is restricted to IP address of plant DMZ firewall
- Portal on plant firewall enables access to IACS data, files and applications
  - Intrusion protection system (IPS) on plant firewall detects and protects against attacks from remote host
- Firewall proxies a client session to remote access server
- Access to applications on remote access server is restricted to specified plant floor IACS resources through IACS application security