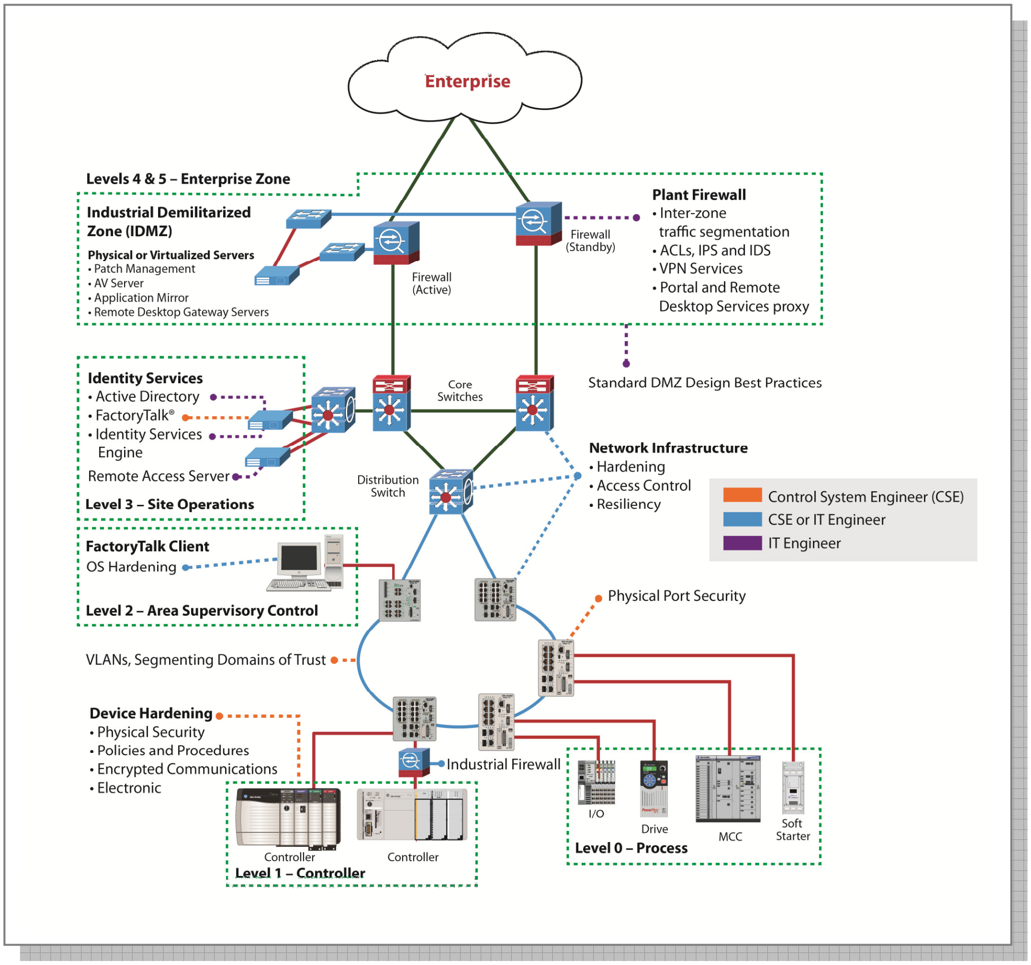
The OEM Guide to Networking

Key Network Technologies and Considerations when Designing and Deploying Industrial Ethernet Networks



Date: March 2016

Publication: ENET-RM001A-EN-P

Table of Contents

Introduction

Today's open networking technologies provide significant flexibility. With flexibility comes the responsibility to understand and deploy solutions that are based on sound engineering and design principles. This guide is intended to help OEMs understand key technologies, networking capabilities and other considerations that could impact them as they develop industrial Ethernet solutions for the machines or equipment they build. This not only includes the networks dedicated to the machines or equipment but also the networking integration requirements for the deployment of smart assets (i.e., machines or equipment) into an end user's plant-wide infrastructure.

This guide is structured to introduce key technologies, provide some high level best practices and guidelines to follow and ask some questions that could help identify where or when a capability is relevant within an OEM's solution. Many of the questions require an ongoing dialog between the OEM and the end user to answer. The content and questions should be used to help drive these discussions so the key capabilities can be identified. Once these capabilities are identified, solutions can be developed to meet the application requirements.

Since the guide is intended to be introductory, references for more in-depth content are provided within each section. These references should be used for more detailed information and further study.

Network Infrastructure for Industrial Operations

Introduction to the OSI Reference Model

The Open Systems Interconnection model (OSI Model) is a conceptual model for how applications can communicate over a network. The purpose of the OSI reference model is to guide vendors and developers so the digital communication products and software programs they create will interoperate. The model partitions a communication system into seven abstraction layers.

Table 1 - Layers of the OSI Model

Layer	Layer Name	Device	Function	Example Standards
Layer 7	Application	Software/ Firmware	Network Services to User Application	CIP IEC 61158
Layer 6	Presentation	Software/ Firmware	Provides formatting functions for application layer protocol conversion, compression, encryption, etc.	CIP IEC 61158
Layer 5	Session	Software/ Firmware	Establishes and manages communications between multiple applications	CIP IEC 61158
Layer 4	Transport	Software/ Firmware	Reliable end-to-end data delivery, provides error recognition and recovery	IETF TCP/UDP
Layer 3	Network	Routers 	Manages data packets, packet delivery, and end-to-end routing of packets	IETF IP
Layer 2	Data Link	Switches 	Creates frames for transmission and controls the shared access to the physical network. Includes error checking, error correction, etc.	IEEE 802.3/802.1
Layer 1	Physical	Cabling 	Electrical details of the transmission, pin-outs, voltages, cable type, etc.	TIA - 1005

Layer 1. Physical Layer

The Physical layer describes the electrical or optical signals used for communication. It includes the voltage of the electrical current used to transport the signal, the media type (Twisted Pair, Coaxial Cable, Optical Fiber, etc.), impedance characteristics, physical shape of the connector, synchronization, and other attributes.

Layer 2. Data Link Layer

The Data Link layer is responsible for providing end-to-end validity of the data being transmitted. The Data Link Layer is logically divided into two sublayers, The Media Access Control (MAC) Sublayer and the Logical Link Control (LLC) Sublayer.

The Media Access Control (MAC) Sublayer determines the physical addressing of the hosts for communicating with other devices on the network. MAC addresses are burned into the network nodes and constitute the low-level address used to determine the source and destination of network traffic. The Logical Link Control sublayer is responsible for synchronizing frames, error checking, and flow control.

Layer 3. Network Layer

The Network layer of the OSI model is responsible for managing logical addressing information in the packets and the delivery of those packets to the correct destination. The logical addresses (e.g., IP addresses) are used to uniquely identify a node on the network and identify the network on which the node resides. The logical address is used by network layer protocols to deliver the packets to the correct network and node on the network. Routers direct the data packet generated by the Network Layer using information stored in a table known as a routing table. The routing table is a list of available destinations that are stored in memory on the routers.

Layer 4. Transport Layer
The Transport layer controls the reliability of a given link through flow control, segmentation/de-segmentation, and error control. The transport layer creates packets out of the message received from the application layer. Packetizing is a process of dividing the long message into smaller messages. The transport layer can keep track of the packets and retransmit those that fail. The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred.

The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are commonly categorized as layer 4 protocols.

Layer 5. Session Layer
The Session layer is responsible for establishing, managing, and terminating connections between applications at each end of the communication. It provides for full-duplex, half-duplex, or simplex operation, and establishes check pointing, adjournment, termination, and restart procedures.

In the connection establishment phase, the service and the rules (e.g., who transmits and when, how much data can be sent at a time etc.) for communication between the two devices are proposed. The participating devices must agree on the rules. Once the rules are established, the data transfer phase begins. When the session is complete, the connection is terminated and communication ends gracefully.

Layer 6. Presentation Layer
The Presentation layer receives data from the application layer to be sent over the network and makes sure that the data is in the proper format. If it is not, the presentation layer converts the data to the proper format. On the other side of communication, when the presentation layer receives network data from the session layer, it makes sure that the data is in the proper format and once again converts it if it is not.

Formatting functions at the presentation layer may include compression, encryption, and ensuring that the character code set (e.g., ASCII, Unicode, EBCDIC (Extended Binary Coded Decimal Interchange Code, which is used in IBM servers), etc.) can be interpreted on the other side.

For example, if we select to compress the data from a network application that we are using, the Application layer will pass that request to the Presentation layer, but it will be the Presentation layer that does the compression.

Layer 7. Application Layer
The Application layer is the OSI layer closest to the end user, which means both the OSI Application layer and the user interact directly with the software application. This layer is not the application itself; it is the set of services an application should use when communication with another partner is needed.

Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network resources or the requested communication exists. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer. Some examples of Application layer implementations include web browsers, file transfer programs, and email systems. The Common Industrial Protocol (CIP) is an Application layer protocol.

Introduction to the Hierarchical Campus Model

The hierarchical model, refer to Figure 1 - Hierarchical Campus Model, can be helpful to design a modular topology using scalable "building blocks" that allow the network to meet evolving business needs. The modular design makes the network easy to scale, understand, and troubleshoot by promoting deterministic traffic patterns. The model uses a layered approach to network design. The building block components are the access layer, the distribution layer, and the core (backbone) layer. The principal advantages of this model are its hierarchical structure and its modularity.

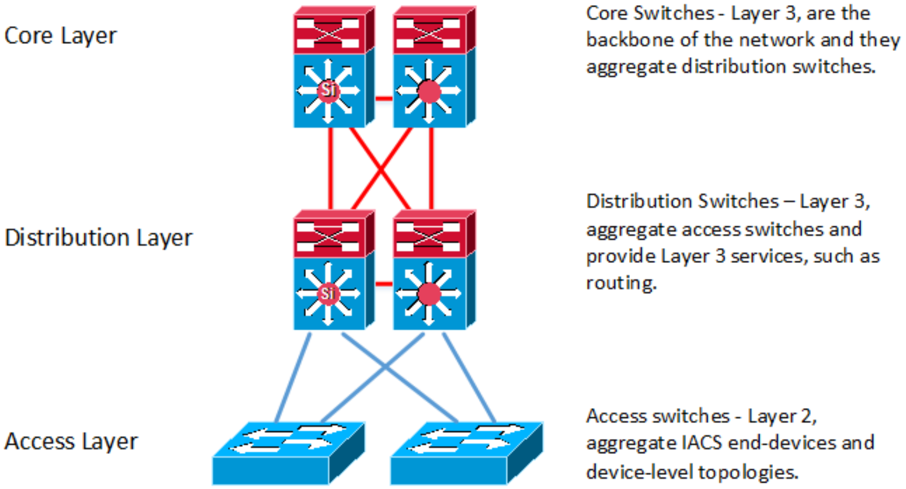

Core Layer
Distribution Layer
Access Layer
Core Switches - Layer 3, are the backbone of the network and they aggregate distribution switches.
Distribution Switches – Layer 3, aggregate access switches and provide Layer 3 services, such as routing.
Access switches - Layer 2, aggregate IACS end-devices and device-level topologies.

Figure 1 - Hierarchical Campus Model

Core Layer

In a typical hierarchical model, the individual building blocks are interconnected using a core layer. The core serves as the backbone for the network. The core needs to be fast and extremely resilient because every building block depends on it for connectivity.

Distribution Layer

The distribution layer aggregates nodes from the access layer. The distribution layer creates a fault boundary providing a logical isolation point in the event of a failure originating in the access layer. Typically, the distribution layer uses Layer 3 switching for its connectivity to the core of the network and Layer 2 services for its connectivity to the access layer.

Access Layer

The access layer is the first point of entry into the network for edge devices, end stations, IP phones, etc. The switches in the access layer are typically connected to two separate distribution layer switches for redundancy.

Introduction to the Converged Plant-wide Ethernet (CPwE) Logical Model

To understand the security and network architecture requirements of an industrial automation and control system (IACS), a logical model is used to describe the basic functions and composition of IACS applications. The logical model also segments the devices and equipment into hierarchical functions. Figure 2 - CPwE Logical Model is a representation of the Converged Plant-wide Ethernet (CPwE) logical model. It is based on several other models and standards - Purdue Model for Control Hierarchy and the International Society of Automation ISA-99 and ISA-95.

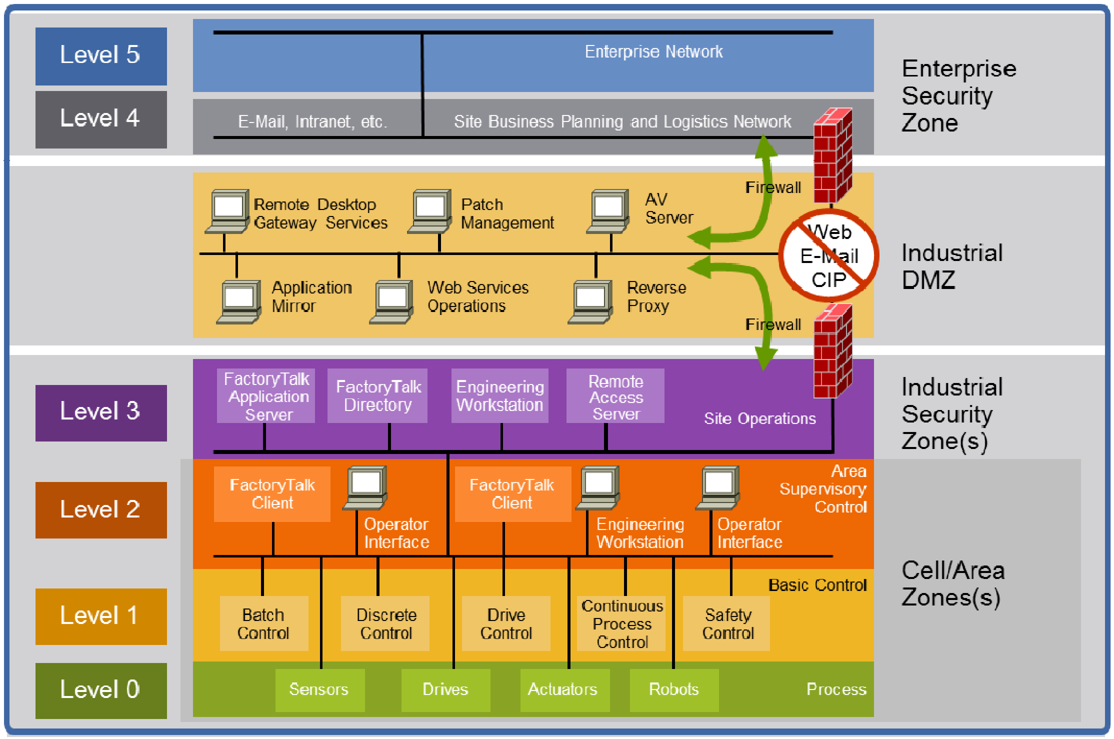


Figure 2 - CPwE Logical Model

For simplification of this document, we will look at networks that are placed into two categories:

1. Plant-wide networks (i.e., Levels 2 and 3 of the end user network), and
2. Machine or equipment networks (i.e., Levels 0 and 1 of the OEM network).

Plant-wide Networks

The plant-wide network (Industrial Zone) is comprised of Cell/Area Zone (Levels 0-2) networks and Level 3 Site Operations. It could contain multiple Cell/Area Zones. Refer to Figure 3 - CPwE Logical Framework. All the systems, devices, and controllers critical to monitoring and controlling the IACS application are in this zone. To preserve smooth plant operations and functioning of the systems and network, the plant-wide network (Industrial Zone) requires clear logical segmentation and protection from Levels 4 and 5 of enterprise operations.

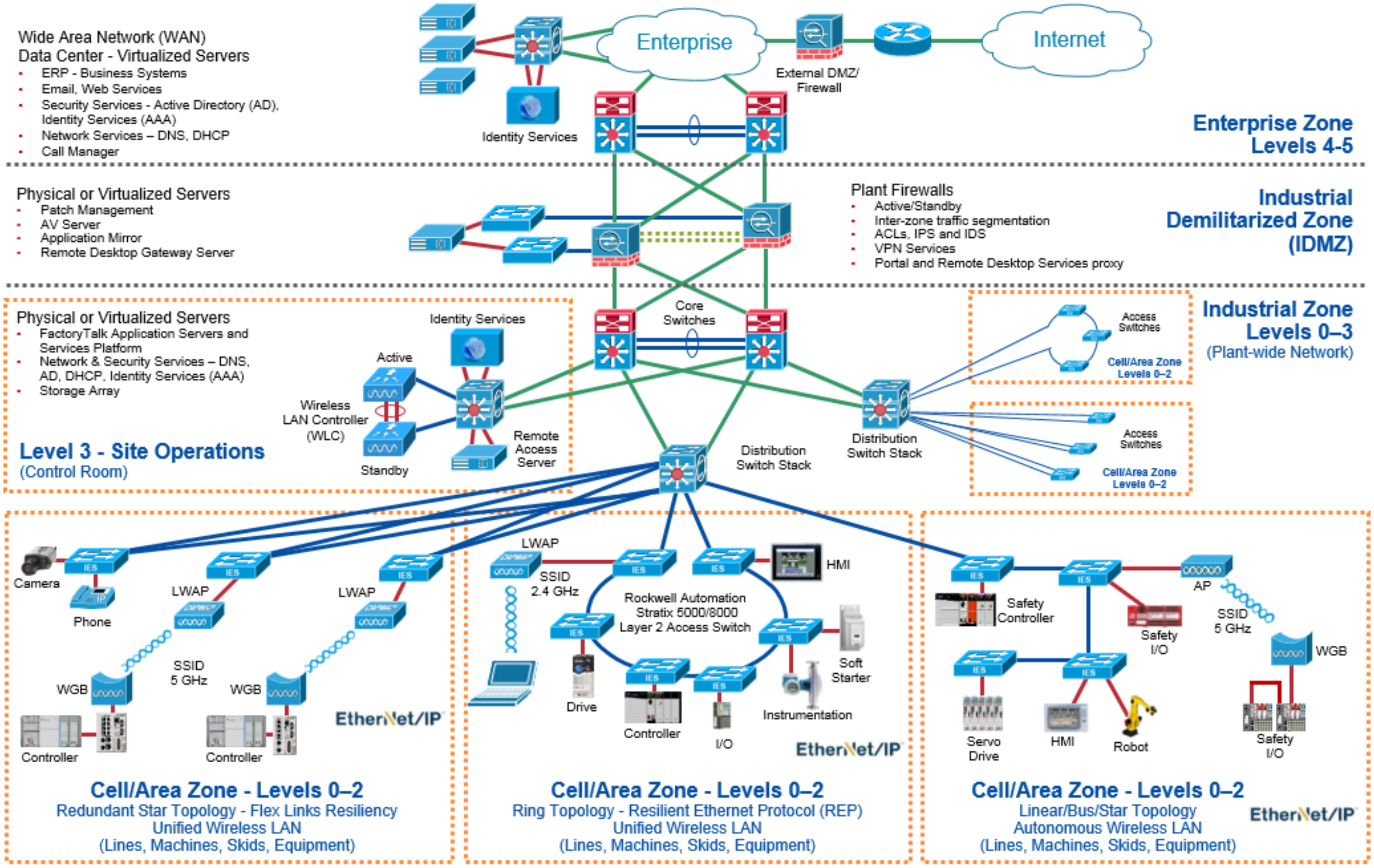

Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD), Identity Services (AAA)
Network Services – DNS, DHCP
Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Enterprise Zone
Levels 4-5
Physical or Virtualized Servers
Patch Management
AV Server
Application Mirror
Remote Desktop Gateway Server
Plant Firewalls
Active/Standby
Inter-zone traffic segmentation
ACLs, IPS and IDS
VPN Services
Portal and Remote Desktop Services proxy
Industrial
Demilitarized Zone
(IDMZ)
Physical or Virtualized Servers
FactoryTalk Application Servers and Services Platform
Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
Storage Array
Identity Services
Core Switches
Active
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Level 3 - Site Operations
(Control Room)
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone
Levels 0–3
(Plant-wide Network)
Camera
IES
Phone
LWAP
LWAP
SSID 5 GHz
WGB
WGB
Controller
Controller
EtherNet/IP
Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
LWAP
SSID 2.4 GHz
HMI
Rockwell Automation Stratix 5000/8000 Layer 2 Access Switch
Drive
Controller
I/O
Soft Starter
Instrumentation
EtherNet/IP
Cell/Area Zone - Levels 0–2
Ring Topology - Resilient Ethernet Protocol (REP)
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
Safety Controller
AP
Safety I/O
SSID 5 GHz
WGB
Servo Drive
HMI
Robot
Safety I/O
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP

Figure 3 - CPwE Logical Framework

The Cell/Area Zone is a functional area within a plant facility. Many plants have multiple Cell/Area Zones. In an automotive plant, it may be a body shop or a sub-assembly process. In a food and beverage facility, it may be the batch mixing area. In a logistics or distribution facility, it may be a sorting system. The Cell/Area Zone may be as small as a single controller and its associated devices on a process skid, or multiple controllers on an assembly line. Each plant facility defines the Cell/Area Zone demarcation differently and to varying degrees of granularity.

A Cell/Area Zone is a set of IACS devices, controllers, etc. that are involved in the real-time control of a functional aspect of the IACS application. To control the functional process, they are all in real-time communication with each other.

The end user may define a Cell/Area Zone per OEM machine/equipment or by a functional area that could include multiple machines or equipment provided by different OEMs.

From an OEM's perspective, there are a few key network design goals when their machine/equipment becomes part of a larger end user infrastructure:

1. seamless integration into the end users plant-wide network,
2. application performance (ensure outside traffic doesn't impact machine or equipment performance), and
3. Intellectual property protection.

Machine/Equipment Level Networks

The machine/equipment level networks illustrated here are intended to introduce high level options for OEMs that are providing stand-alone machines/equipment.

Device-level Linear/Ring Topology – EtherNet/IP 2-port embedded switch technology

Additional Resources

Resources	Description
EtherNet/IP Embedded Switch Technology Application Guide Publication ENET-AP005	This publication provides details about how to install, configure, and maintain linear and Device-level Ring (DLR) networks by using Rockwell Automation EtherNet/IP devices equipped with embedded switch technology.
Embedded Switch Technology Reference Architectures - Reference Manual Publication ENET-RM003	This publication provides design recommendations for connecting device-level topologies to larger, switch networks comprised of Layer 2 access switches.

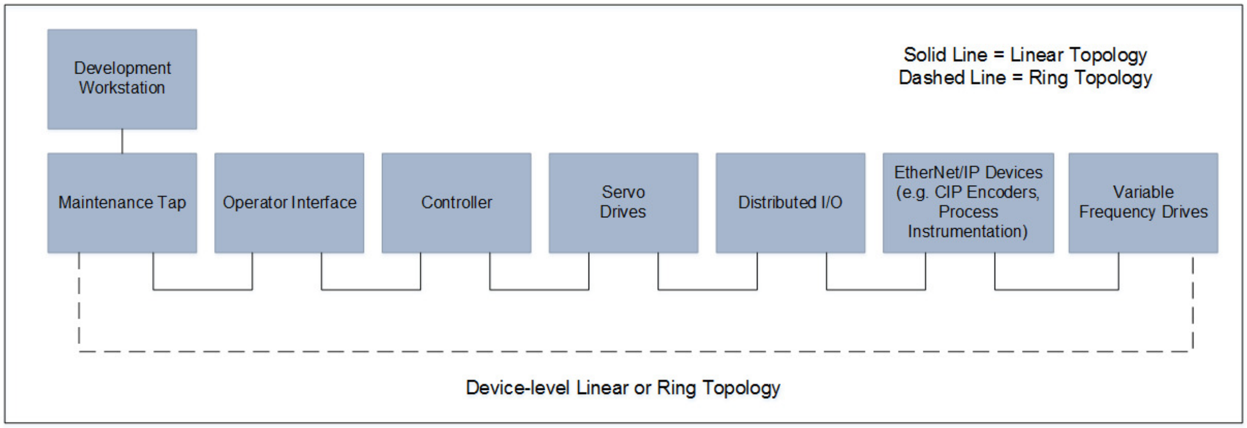

Development Workstation
Solid Line = Linear Topology
Dashed Line = Ring Topology
Maintenance Tap
Operator Interface
Controller
Servo Drives
Distributed I/O
EtherNet/IP Devices (e.g. CIP Encoders, Process Instrumentation)
Variable Frequency Drives
Device-level Linear or Ring Topology

Figure 4 - Device Level Topologies

A device-level linear topology is one where the devices with two external Ethernet ports (a two-port switch) are connected one to the other as shown with the solid line in Figure 4 - Device Level Topologies. A device-level ring (DLR) topology is one where the linear connection is closed by making an extra connection from the last device on the line to the first.

One of the nodes on a DLR is considered to be the active ring supervisor; all of the other nodes can be designated as a backup supervisor or a ring node. The backup supervisor becomes the active supervisor in the event the active supervisor is interrupted or lost. The active ring supervisor is charged with verifying the integrity (prevent loops) of the ring, and reconfigures (changes the topology) the ring to recover from a single fault condition.

The active DLR supervisor uses the beacon protocol frames to monitor the network to determine whether the ring is intact and operating normally, or the ring is broken and faulted. During normal operation, the active ring supervisor blocks one of its ports and forwards traffic out the other.

Following detection of a failure, the active ring supervisor begins forwarding network traffic through both of its ports by unblocking the previously blocked port. Recovery time for a DLR network is typically less than 3ms for a 50-node network. Note that a DLR can recover only from a single point of failure.

Linear Topology General Advantages/Disadvantages

Advantages of a linear topology include the following:

- Simplifies installation by eliminating long cable runs back to a central switch
- Extends the network over a longer distance because individual cable segments (cable between two devices) can be up to 100m
- Supports up to 50 devices per line

The primary disadvantage of a linear topology is that a lost connection or link failure disconnects all downstream devices. To counter this disadvantage, a ring topology can be employed.

Device Level Ring (DLR) Topology General Advantages/Disadvantages

Advantages of a ring topology include the linear topology advantages plus the following:

- Resilience to a single point of failure (cable break or device failure)
- Fast recovery time from a single point of failure

The primary disadvantages of a device-level ring topology are additional setup required (e.g., configuring the active ring supervisor) over a device-level linear or switch-level star network topology, and potential non-compatibility with switch-level resiliency protocols.

The DLR topology is implemented similarly to a linear topology. The primary difference between the two topologies is that, with a ring topology, an extra connection is made from the last device on the line to the first, closing the loop or ring.

A DLR or ring topology has a distinct advantage over a linear topology. The network is resilient to a single point of failure. That is, if a link is broken in the DLR, the ring can recover from a single fault and maintain communications. This failure point can occur anywhere on the ring and the DLR is still able to recover fast enough to avoid application disruption.

EtherNet/IP 2-port embedded switches offer the following capabilities that are critical to industrial control networks:

- Precision Time Protocol (PTP), end-to-end mode - IEEE 1588 transparent clock functionality for re-phasing of the clocks
- Prioritization/QoS – ODVA CIP Layer 2 and Layer 3 QoS definitions
- Beacon protocol - used to manage the traffic in a device-level ring topology
- Internet Group Management Protocol (IGMP) for multicast management

Managed Switch-level Star Topology

Additional Resources

Resources	**Description**
Ethernet Design Considerations Reference Manual Publication ENET-RM002	This publication provides an explanation of Ethernet concepts including network layout and components, network infrastructure devices and features, and network protocols.
Stratix Managed Switches User Manual Publication 1783-UM007	This publication describes the embedded software features and tools for configuring and managing Stratix™ managed switches.

A managed switch star topology is one in which point-to-point connections are made between the switch and the end devices. Refer to Figure 5 - Switch-level Star Topology for an example.

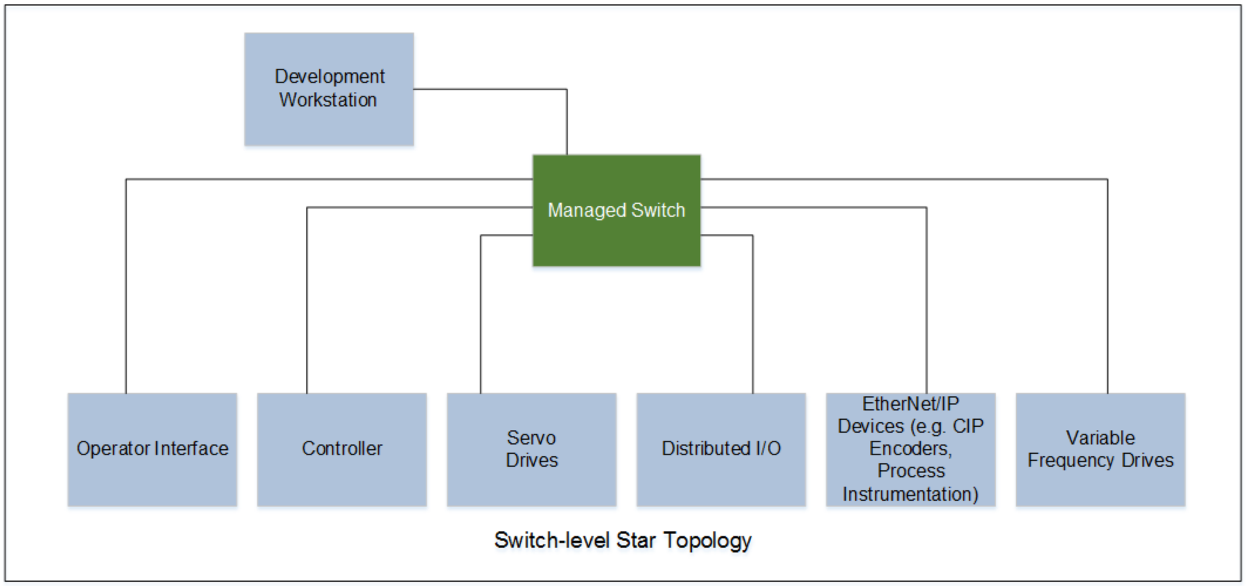

Development Workstation
Managed Switch
Operator Interface
Controller
Servo Drives
Distributed I/O
EtherNet/IP Devices (e.g. CIP Encoders, Process Instrumentation)
Variable Frequency Drives
Switch-level Star Topology

Figure 5 - Switch-level Star Topology

Managed Switch Star Topology General Advantages/Disadvantages

Advantages of a star topology include the following:

- Easy to design, configure, and implement
- Point to point connection – if a connection is lost, only that device is effected; the rest of the network remains intact
- Maintenance and troubleshooting is easier because all traffic is seen by the switch
- Lower mean time to repair (MTTR) – DHCP per port and automatic device configuration allow failed devices to be replaced without requiring full device and network reconfiguration

The disadvantage of a star topology is that all end devices must typically be connected back to a central location on the machine or equipment. This increases the amount of cable infrastructure and increases the number of available ports required by the central switch, leading to a higher cost-per-node solution.

Selecting a managed switch with the proper capabilities to meet the application needs is required. Not all managed switches offer the same capabilities. Examples of some of the key capabilities to consider include: Virtual Local Area Networks (VLANs), routed access, QoS, resiliency protocols and loop prevention, multicast management, Precision Time Protocol support, DHCP, NAT, and easily obtainable diagnostic information.

Other Topology Options

Many OEM solutions are addressed by utilizing one of the topologies described above. For some OEM equipment (i.e., larger device node count, multiple equipment sections, or physically larger footprints) the OEM solution may require expansion of these topologies. This could include utilizing a combination of a device-level and switch-level topology.

Network Design Considerations

There are many factors that impact the success or failure of a network design. The intent of this document is to focus on the concepts and factors that impact most network designs. This section will discuss the key features and capabilities that may be required for IACS applications. These features will help determine the type and capabilities of the networking infrastructure required. Although there is no priority of one feature over another, and in fact many features can and should coexist in an architecture, the features are presented in the following order to assist the reader in a logical progression of design considerations.

- Segmentation – Physical and Logical
  - Virtual Local Area Networks (VLANs)
  - Routed Access
- Security
  - Secure Remote Access
- Prioritization/Quality of Service (QoS)
- Multicast Management
- Time Synchronization – IEEE 1588 PTP, End to End Mode
  - CIP Sync
  - CIP Motion
- Availability
  - Resiliency Protocols and Loop Prevention
- Network Address Translation (NAT)
- Dynamic Host Configuration Protocol (DHCP)
  - DHCP Persistance (DHCP per port)

Segmentation – Physical and Logical

Additional Resources

Resources	**Description**
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide Publication ENET-TD001, Page 96 Bookmark = Logical Segmentation and VLANs	This publication describes the design and implementation guidelines of a Converged Plant-wide Ethernet Network for Industrial Ethernet Applications.
Segmentation Methods within the Cell/Area Zone – Application Guide Publication ENET-AT004	This publication describes the use of physical segmentation using the ControlLogix/CIP Bridge. It also reviews advantages and disadvantages of other segmentation methods that can be used within a Converged Plant-wide Ethernet architecture.

Segmentation is the process of outlining which IACS devices need to be in the same LAN, then segmenting that LAN from other LANs. Segmentation is a key consideration for a Cell/Area Zone network. Segmentation is important to help manage the real-time communication properties of the network, while also supporting seamless plant-wide connectivity requirements as defined by the network traffic flows. Security is also an important consideration in making segmentation decisions.

A security policy may call for limiting access of plant floor personnel (such as a vendor or contractor) to certain areas of the plant floor (such as a functional area). Segmenting these areas into distinct subnets and VLANs greatly assists in the application of these types of security considerations.

Subnets and VLANs are two concepts that go hand-in-hand. Subnets are a subset of IP addresses assigned to a set of devices. Subnets are a Layer 3 concept. VLANs are a Layer 2 concept. When a VLAN is defined, it creates a broadcast boundary (i.e., broadcast domain) where traffic is contained to devices that are members of the defined VLAN. Devices within a VLAN can communicate with each other without a Layer 3 switch or router. Devices in different VLANs that need to communicate will need a Layer 3 switch or router. Typically, devices in a VLAN are assigned IP addresses from the same subnet and a subnet has devices in a single VLAN. Using a one-to-one relationship between VLANs and subnets is a best practice.

Segmentation can be achieved via the following two key mechanisms in the Cell/Area Zone network:

- Physical—Use of bridges and gateways to break up Layer 2 networks and achieve segmentation
- Logical – Use of VLANs and routed access switches to break up Layer 2 networks and achieve segmentation; a routed access switch supports one or more routing types (static, connected, or dynamic)

Physical segmentation is a common approach in IACS Ethernet implementations. For example, one approach is to physically separate input/output (I/O) traffic from HMI traffic and not to connect the I/O traffic to the plant-wide network infrastructure. In these cases, a controller has separate network interface connections (NIC) to each network, and the only means to communicate between the two networks is over the backplane of the controller. The I/O network is, therefore, reachable only via the controller backplane that processes only CIP traffic. This is referred to as a ControlLogix Gateway/CIP Bridge. Refer to Figure 6 - Example of Physical Segmentation.

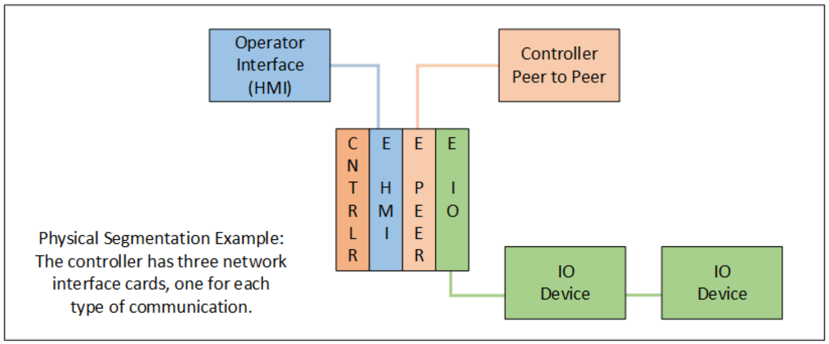

Operator Interface (HMI)
Controller Peer to Peer
CNTRLR
E HMI
E PEER
E IO
IO Device
IO Device
Physical Segmentation Example: The controller has three network interface cards, one for each type of communication.

Figure 6 - Example of Physical Segmentation

Logical segmentation is a second approach utilized and this segmentation method uses virtual LANs. A virtual LAN (VLAN) is a switched network segmented on a functional, application, or organizational basis, as opposed to a physical or geographical basis. Switches filter destination MAC addresses and forward VLAN frames only to ports that serve the VLAN to which the traffic belongs. A VLAN can consist of several IACS devices and network switches, all of which are members of a single logical broadcast domain. A VLAN does not have physical proximity constraints for the broadcast domain, since multiple VLANs can be implemented on the same physical infrastructure.

With VLANs, you can configure a switch to support multiple segmented networks without the traffic from one network burdening the other (e.g., IP multicast traffic from VLAN 10 will not reach VLAN 22). A VLAN helps to restrict broadcast traffic and helps to simplify management of security policies by creating smaller domains of trust. Refer to Figure 7 - Example of Logical Segmentation.

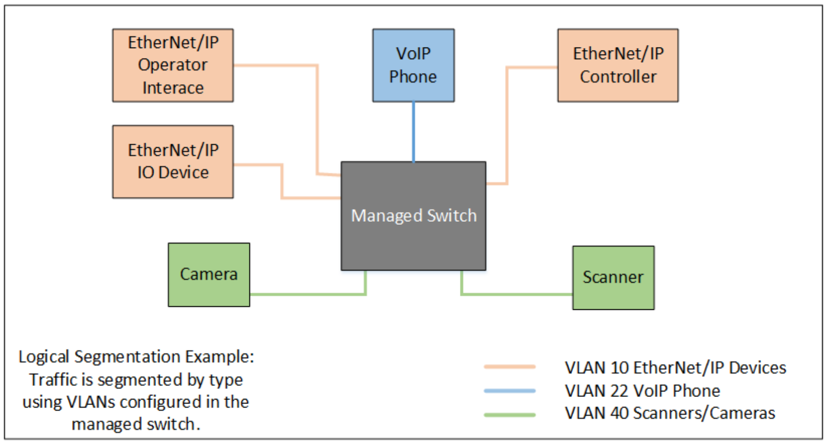

EtherNet/IP Operator Interace
VoIP Phone
EtherNet/IP Controller
EtherNet/IP IO Device
Managed Switch
Camera
Scanner
Logical Segmentation Example: Traffic is segmented by type using VLANs configured in the managed switch.
VLAN 10 EtherNet/IP Devices
VLAN 22 VoIP Phone
VLAN 40 Scanners/Cameras

Figure 7 - Example of Logical Segmentation

IEEE 802.1Q VLAN Trunking (Layer 2) – VLAN trunking is the ability to extend VLAN definitions across a set of managed switches. This allows devices configured in VLAN 10 on Switch#1 to communicate to devices configured in VLAN 10 on Switch #2. A trunk port configured on a switch can support more than one VLAN. Refer to Figure 8 - Example of VLAN Trunking.

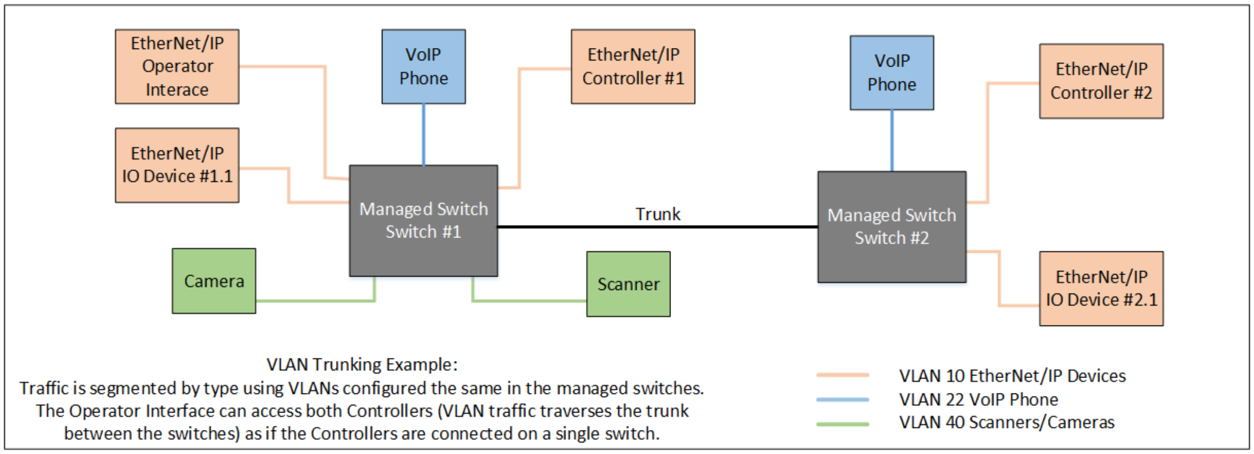

EtherNet/IP Operator Interace
VoIP Phone
EtherNet/IP Controller #1
VoIP Phone
EtherNet/IP Controller #2
EtherNet/IP IO Device #1.1
Managed Switch Switch #1
Trunk
Managed Switch Switch #2
Camera
Scanner
EtherNet/IP IO Device #2.1
VLAN Trunking Example:
Traffic is segmented by type using VLANs configured the same in the managed switches.
The Operator Interface can access both Controllers (VLAN traffic traverses the trunk
between the switches) as if the Controllers are connected on a single switch.
VLAN 10 EtherNet/IP Devices
VLAN 22 VoIP Phone
VLAN 40 Scanners/Cameras

Figure 8 - Example of VLAN Trunking

VLAN Summary

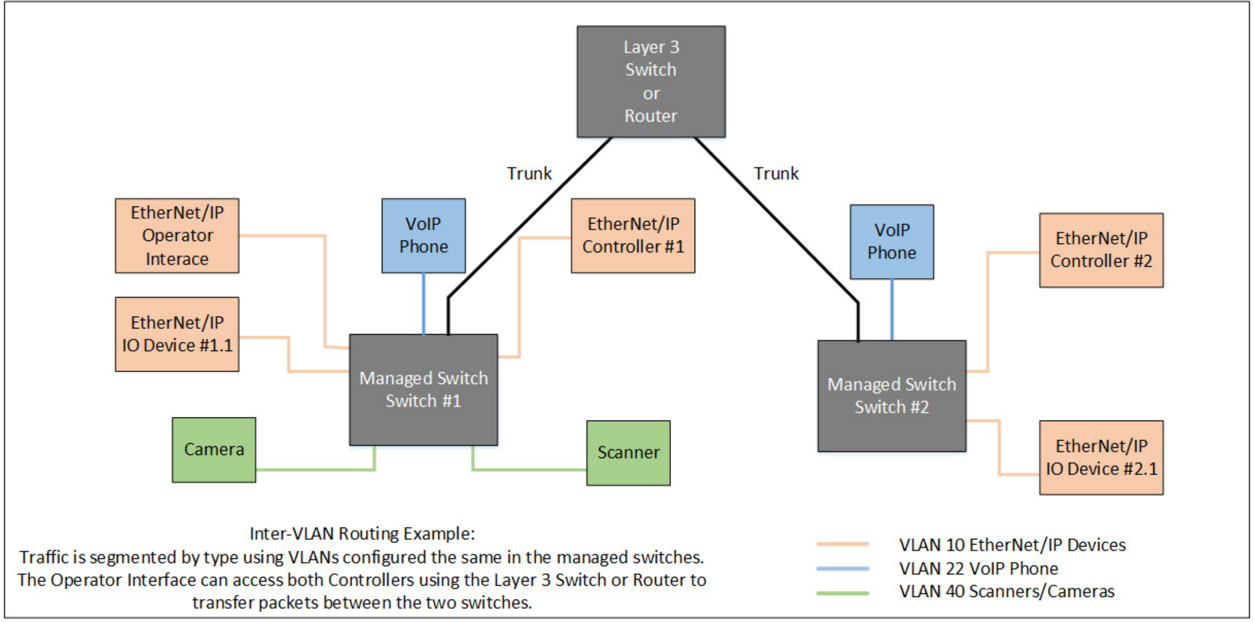
- VLANs segment a network logically without being restricted by physical connections
- A VLAN is established within or across switches
- Data is only forwarded to ports within the same VLAN
- Devices within each VLAN can only communicate with other devices on the same VLAN
- Segments traffic to restrict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

VLAN Trunking Summary

- 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
- Trunk or uplink ports are used to interconnect switches and carry traffic from multiple VLANs

Inter-VLAN Routing

In order to forward data between VLANs (i.e., inter-VLAN routing), a Layer 3 device (switch or router) is required. Use Layer 3 Inter-VLAN routing/switching between VLANs within the same Cell/Area Zone or between zones within the plant. Layer 3 switching can be accomplished with a routed access switch (within the machine/skid) or a plant-wide distribution switch. Routing types include connected, static or dynamic. Refer to Figure 9 - Example of Inter-VLAN Routing.


Layer 3 Switch or Router
Trunk
Trunk
EtherNet/IP Operator Interace
VoIP Phone
EtherNet/IP Controller #1
VoIP Phone
EtherNet/IP Controller #2
EtherNet/IP IO Device #1.1
Managed Switch Switch #1
Managed Switch Switch #2
Camera
Scanner
EtherNet/IP IO Device #2.1
VLAN 10 EtherNet/IP Devices
VLAN 22 VoIP Phone
VLAN 40 Scanners/Cameras

Inter-VLAN Routing Example:
Traffic is segmented by type using VLANs configured the same in the managed switches.
The Operator Interface can access both Controllers using the Layer 3 Switch or Router to transfer packets between the two switches.

Figure 9 - Example of Inter-VLAN Routing

Segmentation Guidelines and Best Practices

- Create smaller modular building blocks to help minimize network sprawl and build scalable, robust and future-ready network infrastructure.
  - Smaller broadcast domains
  - Smaller fault domains (e.g., Layer 2 loops)
  - Smaller domains of trust (security)
  - Avoid large Layer 2 networks to simplify network management.
- Configure separate VLANs for different work cells or areas of your plant. Since 80-90% of traffic is confined to a particular area or cell, configuring one VLAN for the traffic in that area or cell is optimal.
- All devices with multicast connections must be on the same VLAN. Within a VLAN, multicast and unicast traffic can be mixed depending on application requirements. The default communication type of unicast should be used for point-to-point communication to minimize device, network, and infrastructure loading.
- Cell/Area Zone definition
  - Design small cell or area zones, each with a dedicated VLAN and IP subnet.
  - Restrict data flow out of the cell or area zone unless plant-wide operations explicitly require it.
  - Segment traffic types (e.g., CIP, VoIP, HTTP) into VLANs and IP subnets to better manage the traffic and simplify security management.
  - Within the cell or area zone, use Layer 2 VLAN trunking between switches with similar traffic types. When trunking, use 802.1Q, VLAN Trunking Protocol (VTP) in transparent mode.
- Use Layer 3 routed access or distribution switches to route information between Cell/Area Zone VLANs and plant-wide operations in the Industrial Zone.
- Enable IP directed broadcast on Layer 3 switches that connect Cell/Area Zone VLANs with EtherNet/IP traffic for easy configuration and maintenance from control systems, such as RSLinx® software.
- Do not explicitly use VLAN 1; some security threats assume that VLAN 1 is the default VLAN for data and/or management traffic and may target VLAN 1 in their attacks.

- Assign different traffic types to a unique VLAN, other than VLAN 1

Segmentation Questions

- Will the machine or equipment utilize a controller platform that allows multiple network interface modules? If yes, then physical segmentation is possible.
- Will the machine or equipment be standalone? If yes, then physical and or logical segmentation is possible.
- Will the machine or equipment be integrated into an end user's plant-wide network? If yes, then refer to the plant-wide integration section of this guide for additional consideration questions.

Segmentation is important in all network designs and becomes more critical when an OEM machine/equipment is integrated into an end user's plant-wide network. In these cases, the OEM and end user must work together to design a solution. In almost all cases some logical segmentation should be implemented.

Applicability to Topologies

Topology	**Applicability**
Device-level Topologies using EtherNet/IP 2-port Embedded Switch Technology	Physical Segmentation Logical Segmentation only if integrated with a Managed Switch
Managed Switch-level Topologies	Physical and Logical Segmentation

Security

Additional Resources

Resources	**Description**
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide Publication ENET-TD001, Page 251 Bookmark = IACS Network Security and the Demilitarized Zone	This publication describes the design and implementation guidelines of a Converged Plant-wide Ethernet Network for Industrial Ethernet Applications.
Design Considerations for Securing Industrial Automation and Control System Networks - Whitepaper Publication ENET-WP031	This publication describes general considerations to design and deploy a holistic defense-in-depth industrial security policy to help secure networked IACS assets.
Deploying Identity Services within a Converged Plantwide Ethernet Architecture - Design and Implementation Guide Publication ENET-TD008	This publication outlines the key requirements and design considerations to help in the successful deployment of the Cisco® Identity Services Engine (Cisco ISE) within IACS plant-wide architectures. It is a CPwE-REP Cisco® Validated Design (CVD).
Securely Traversing IACS Data across the Industrial Demilitarized Zone – Design and Implementation Guide Publication ENET-TD009	This publication provides recommendations for segmenting business system networks from plant-wide networks by using an Industrial Demilitarized Zone (IDMZ) to separate the network level between the Industrial and Enterprise Zones. It is a CPwE-IDMZ Cisco® Validated Design (CVD).
Security Considerations in Converged Plantwide Ethernet Quick Reference Drawing Publication IASIMP-QR035	This publication provides a high level overview of various security layers that can be implemented within the Converged Plant-wide Ethernet Network.

A plant's security plan (policy and procedures) is defined by the end user and therefore it is paramount that OEMs that need to integrate their equipment at an end user's site understands the security plan. OEMs need to be aware of end user business practices, standards, policies and tolerance to risk. OEMs will need to understand how their equipment will be integrated to ensure tie-ins do not negatively impact their equipment performance or introduce security vulnerabilities into the end users plant-wide network infrastructure. It is also important for OEMs to think about a security plan for their equipment that may not be integrated. Some of the same concepts are applicable; the OEM may just put more emphasis in certain areas.

To maintain availability, integrity, and confidentiality of the plant, the IACS applications and the IACS network, key security concepts must be applied to any solution. These practices follow a defense-in-depth approach where a number of considerations, techniques and practices are applied within the overall system to protect the system and network.

Layers of Defense

- Policies, Procedures and Awareness – plan of action around procedures and education to protect company assets (risk management) and provide rules for controlling human interactions in IACS systems.
- Physical Security – limit the physical access to cells/areas, control panels, devices, cabling, and control room, etc. to authorized personnel by applying things like locks, gates, key cards, and biometrics. This may also include policies, procedures and technology to escort and track visitors.
- Network Security – This includes the network infrastructure; e.g., firewall policies, access control list (ACL) policies for switches and routers, authentication, authorization, and accounting (AAA), intrusion detection and prevention systems (IDS/IPS)
- Computer Hardening – This includes patch management, Anti-X (e.g., virus, spyware, malware) software, and removal of unused applications/protocols/services, closing unnecessary logical ports, and protecting physical ports.
- Application Security – This includes authentication, authorization and audit software. Implement change management and accounting as well as authentication and authorization to help keep track of both access and changes by users.
- Device Hardening – This includes change management, communication encryption, and restrictive access.

The industrial network security framework should utilize a defense-in-depth approach that is aligned to industrial security standards such as ISA/IEC-62443 (formerly ISA-99) IACS Security and NIST800-82 Industrial Control System (ICS) Security. Refer to Figure 10 - CPwE Architectural Security Framework.

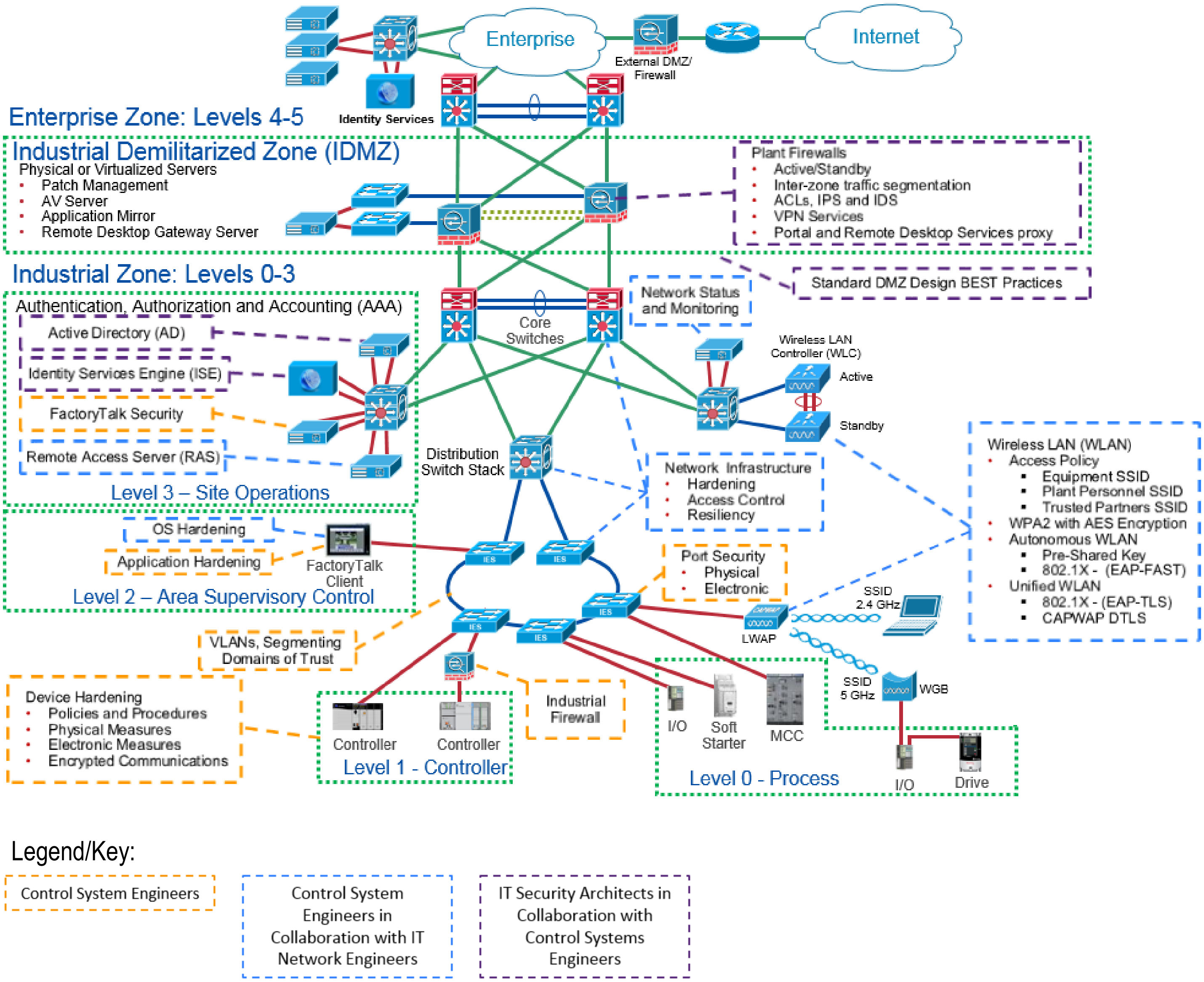


Figure 10 - CPwE Architectural Security Framework

The security design considerations for the Cell/Area Zone network include the following:

- Port configuration (including MAC address filtering, limited ACL configurations, QoS Trust)
- Physical – port block outs and cable lock-ins
- Infrastructure protection (hardening from a security perspective) of the network infrastructure to prevent unauthorized access
- Layer 2 security—Networking services can be disrupted through attacks on the protocols and standards to which they adhere. Layer 2 security protects the network services from attacks on the key protocols, including the following:
    - Quality of service (QoS)
    - Address Resolution Protocol (ARP)
    - Rapid Spanning Tree Protocol (RSTP)
    - Dynamic Host Configuration Protocol (DHCP)
    - MAC address flooding

- Monitoring of network infrastructure administration data (syslogs and SNMP)
- VLANs for segmentation, to create smaller domains of trust

Security Summary

- No single product, technology or methodology can fully secure IACS applications.
- Protecting IACS assets requires a defense-in-depth security approach, which addresses internal and external security threats.
- Utilize multiple layers of defense (physical, procedural and electronic) at separate IACS levels by applying policies and procedures that address different types of threats.
- Align with the end user's approach to security including business practices, standards, policies and current status of the networking infrastructure.
- Leverage Industrial Security Policies
    - Physical access, port security, access control lists, application security, remote access (avoidance of back doors)
    - Alignment with IACS security standards such as ISA/IEC-62443 (formerly ISA 99) and NIST 800-82

Security Guidelines and Best Practices

- Utilize a defense-in-depth security approach
- Deploy an Industrial Demilitarized Zone (IDMZ) between Industrial and Enterprise Zones
- Control access to your network using Access Control Lists and port blocking features
- Limit and manage network traffic by using Firewalls and Intrusion Detection/Prevention systems
- Protect PC assets by using anti-virus and application whitelisting
- Establish a system patching policy to keep software up to date
- Develop and follow security policies for managing and protecting passwords, managing removable media and the use of personal devices
- Utilize physical controls where possible to prevent unintentional human errors (e.g., key-switches, locked panels, switch port lock-in and block-out, etc.)
- Monitor what is going on in the application (e.g., change management software, controller diagnostics, switch diagnostics, etc.)
- Leverage license based source protection and content licensing to protect your intellectual property

Security Questions

- Will the end user allow remote access to the OEM's machine/equipment? If yes, does the end user have approved methods that must be followed?
- Will the OEM's machine/equipment be standalone? If yes, then the OEM has greater flexibility in the layers of security to implement and the overall security plan.

    These questions will help an OEM develop the security requirements specific to the machine/equipment.

    - What physical infrastructure features will you provide as part of your solution to help restrict access (e.g., lock and key control panels, cable lock-in on used ports and port block out devices on unused networking ports, etc.)?

    - What network infrastructure hardware and software will you provide and utilize to block communication paths and services that are not explicitly authorized (e.g., firewalls, managed switches, unified threat management appliances, etc.)?
    - If your solution leverages managed switches, how will you utilize the features in managed switches to restrict access (e.g., MAC address port security, VLAN segmentation, disabling unused ports, ACLs, etc.)?
    - How will you prevent unauthorized access to a controller or operator interface?
    - How will you detect changes made on the machine/equipment?
    - How will you protect your intellectual property?

- Will the OEM's machine/equipment be integrated into an end user's plant-wide network? If yes, then the OEM must understand the end user's security requirements and who is implementing the security plan. This could be the EU, SI/SP, OEM or a combination.

  The questions that follow are directed toward the end user and will help an OEM drive the discussion and understanding of the end user's security requirements.
    - Do you have an IT security policy? If yes, have the end user explain it.
    - Do you have an industrial security policy? If yes, have the end user explain it.
    - Do you have a remote access policy for employees? If yes, what remote access technology and products do you utilize?
    - Do you have a "partner" or "guest" remote access policy? If yes, what methodology is used to manage partner access? What method is approved for OEM access to their machine/equipment?
    - Do you have a policy for SI/SPs and OEMs to connect to IACS assets when they are performing work on-site? If yes, have the end user explain it.
    - Do you have a secure tunnel from your enterprise network to the IACS plant-wide network?
    - Is network segmentation used? If yes, have the end user explain how the network infrastructure is segmented into domains of trusts.
    - What methods are used to control access to devices (e.g., MAC address filtering, ACL configurations, VLAN segmentation, etc.)?
    - What level of port security is being implemented (e.g., switch level – locking out ports, turning off ports, etc.)?
    - Who is responsible for implementing the security requirements?
    - What infrastructure management tools will be deployed? Do they require a specific capability (e.g., SNMP)?

Applicability to Topologies

Topology	**Applicability**
Device-level Topologies using EtherNet/IP 2-port Embedded Switch Technology	Limited – some defense in depth layers can be leveraged but not all.
Managed Switch-level Topologies	Varied – the available methods will be dependent on the capabilities of the managed switch used.

Secure Remote Access

Additional Resources

Resources	Description
Scalable Secure Remote Access Solutions for OEMs Publication ENET-WP025	This publication provides guidance to help enable secure remote access to plant-based applications and data. It provides guidance for OEMs to collaborate with their customers when designing a secure remote access solution.
Achieving Secure, Remote Access to Plant-Floor Applications and Data Publication ENET-WP009	This publication provides guidelines for remotely accessing automation systems to share plant data, applications, and resources, regardless of physical location.

Secure remote access enables OEMs to respond faster to equipment malfunctions or prevent them by collecting and monitoring machine performance data. For example, information from the OEM's machine can be available through performance dashboards to display live machine health indicators to understand when preventative maintenance is needed. OEMs can receive notifications when important parameters reach a predefined threshold enabling them to be proactive rather than reactive for device faults and alarms, to enable a faster and more proactive response. Once a fault notification is received, the OEM can use historical machine information in conjunction with their locally hosted software tools to troubleshoot systems remotely, by having remote access to PLC application code to identify issues, make any required changes, and give guidance to on-site personnel. Ultimately, this enables OEM support personnel to be more responsive and efficient. It also benefits the end user to keep their operations downtime to a minimum.

The deployment of a secure remote access solution that allows an OEM to connect with their machine/equipment in an end user's facility requires early dialog between entities to understand the options for an acceptable solution. Choosing a solution and the technology for secure remote access is dependent upon many factors and the solution for one user may not be acceptable to another. The following factors are all critical to determining a possible solution: the end users' business practices, corporate/local standards, industrial security policies and procedures (avoidance of back doors), risk tolerance, application requirements, current status of network infrastructure (segmentation into domains of trust), and alignment with IACS security standards. Regardless, OEM's need to be cognizant of security risks and choose solutions that provide secure access to protect their machine and the end user from unauthorized access.

When deciding on a secure remote-access solution, OEMs have different options across a range of features and security strengths. At a minimum a secure remote access solution should only require an outbound port through the customer's firewall limiting the ability for inbound open communications into the customer's environment. Communications need to be secured through SSL (Secure Socket Layer) encryption and security certificates established between the on premise appliance and the host. Finally the solution should offer the end user the ability to control and audit remote access.

Typically, the solutions establish remote access by creating a dynamic VPN to the customer network. This can be an issue because access is not controlled to an individual machine / device or IP address. The preferred solution adds additional security capabilities that protect both the OEM and the end user through several additional security capabilities. More sophisticated remote-access solutions can also incorporate security "fingerprint" certificates which incorporate a combination of hardware MAC ID's to establish a secondary certificate that gets registered with the host server. In the event of hardware tampering the certificates no longer match and remote access is disabled. Remote access is limited by user account, site, machine and individual device. This limits individual's visibility and access to only the machine or device that they are authorized and qualified to gain access to, protecting the OEM's intellectual property and the end user's security.

Finally, it is important to identify and report on remote access activity. A secure remote access solution should give the end user complete control. This means that the end user has the ability to approve or reject a remote access session, and has full surveillance to the remote actions. Furthermore, to establish accountability, all remote sessions should be recorded, logged, and identified with the specific user/login. These additional security features protect the OEM by limiting access to their machines as well as the end user by limiting access to other assets on their network.

An end user's firewall can be configured to allow or deny access on any TCP port in either inbound or outbound connections. A secure remote access solution should only require TCP port 443 to be configured to allow outbound and acknowledgment packets. This means that an end user can set up their firewalls to block any inbound traffic to their network. A remote access server would continuously send outbound packets through Port 443 to an externally hosted Service Center that manages user credentials, data storage, dashboards, and reports. Using SSL encryption and various levels of certification, the external Service Center is the only destination for the outbound packets. The return acknowledgment packet is then used to send information back to the remote access server from the Service Center, creating a continuous connection in a secure environment that allows for secure remote access.

A high level depiction of this solution is shown in Figure 11 - Secure Remote Access Solution.

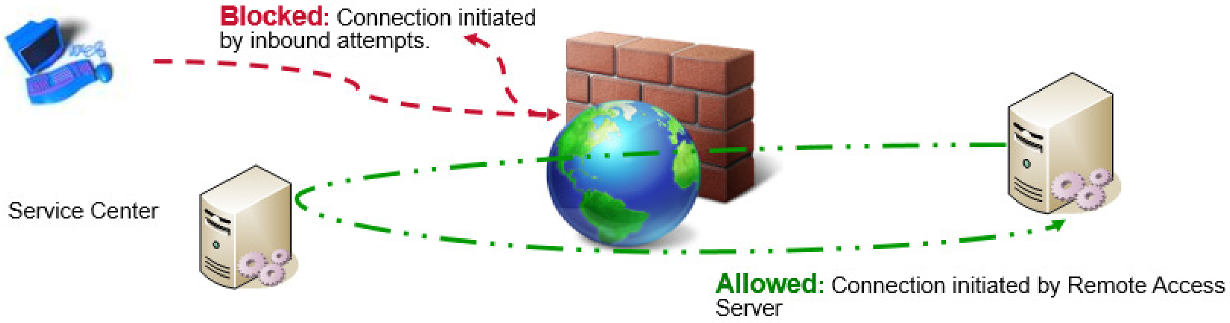

Blocked: Connection initiated by inbound attempts.
Service Center
Allowed: Connection initiated by Remote Access Server

Figure 11 - Secure Remote Access Solution

Secure Remote Access Summary

- Secure remote access allows end users to integrate their smart machines with their plant-wide networks and share information with their OEM partners, ultimately enabling OEMs to respond faster to equipment or help prevent them in the first place
- A remote access solution should provide the appropriate levels of security to meet the manufacturer's current and future needs, as well as align with established security standards
- Utilize multiple defense/security mechanisms by applying policies and procedures that address different types of threats
- Align with the end user's approach to security including business practices, standards, policies, and current status of the networking infrastructure

Secure Remote Access Guidelines and Best Practices

- Deploy an Industrial Demilitarized Zone (IDMZ) between Industrial and Enterprise Zones
- Control access to your network using Access Control Lists and port blocking features
- Limit and manage network traffic by using Firewalls and Intrusion Detection/Prevention systems
- Develop and follow security policies for managing and protecting remote access user logins and passwords
- Use only a Port 443 (HTTPS) outbound connection for an access point
- Conforming to a common end user remote access platform for multiple vendors minimizes the number of overall access points for the end user

Secure Remote Access Questions

Refer to the previous section, specifically the Security Questions directed at the end user to understand the security requirements and plan that could impact remote access.

- Do you have a remote access policy for employees? If yes, what remote access technology and products do you utilize (e.g., VPN)?
- Do you have a “partner” or “guest” remote access policy? If yes, what methodology is used to manage partner access?
- Will the end user allow remote access to the OEM’s machine/equipment? If yes, does the end user have approved methods that must be followed?
- Is cellular a communication method that the end user would find acceptable? If yes, does the end user have requirements for protecting sensitive information (e.g., recipes or other intellectual property)?

Prioritization/Quality of Service (QoS)

Additional Resources

Resources	**Description**
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide Publication ENET-TD001, Page 127 Bookmark = Quality-of-Service (QoS)	This publication describes the design and implementation guidelines of a Converged Plant-wide Ethernet Network for Industrial Ethernet Applications.

Quality of Service determines how packets are marked, classified, and treated based on traffic type.

Latency, (the average amount of time a message takes to be transmitted and processed from the originating node to the destination node), and jitter, (the amount of variance in the latency of a message), cause the most impact to network determinism and must be tightly controlled. To minimize application latency and jitter, control data must have priority within the cell or area zone.

QoS gives preferential treatment to some network traffic at the expense of others. Plant-wide networks must prioritize 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, and Motion) have different requirements for latency, packet loss and jitter.

The application of QoS shall be applied to the critical CIP-based implicit I/O as well as the explicit traffic generated by IACS applications. Quality of service (QoS) refers to control mechanisms that can provide various priorities to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from the application program. QoS guarantees are important if the network performance is critical, especially for real-time IACS applications.

Prioritization/QoS Summary

- QoS prioritizes traffic into different service levels; Allows for predictable service for different applications and traffic types
- QoS helps mitigate delays caused by latency or jitter
- QoS helps reduce packet loss
- QoS does not increase bandwidth
- ODVA has specified QoS markings for CIP and PTP traffic
    - EtherNet/IP 2-port Embedded Switch Technology incorporates these Layer 2 and Layer 3 QoS definitions
    - Stratix Managed Switches load an initial switch configuration that sets up the policing, queuing and scheduling

Prioritization/QoS Guidelines and Best Practices

- Leverage ODVA specification for QoS traffic
    - EtherNet/IP 2-port Embedded Switch Technology utilizes ODVA QoS definitions – no configuration required
    - Stratix Managed Switches utilize ODVA QoS definitions – enabled by default

  Note: Other switches (especially enterprise switches) may have a different prioritization
- The Stratix Managed Switch portfolio recognizes or "trusts" QoS capable devices and prioritizes CIP traffic as it exits the switch
- Deploy QoS consistently throughout the EtherNet/IP IACS Network
- The more IACS devices that implement QoS, the better the network infrastructure devices (switches, routers) can take advantage of QoS features

Prioritization/QoS Questions

- Does your application include integrated motion? If yes, then the ODVA defined prioritization QoS standards are required.
- Does your application utilize EtherNet/IP networks for I/O control? If yes, then the ODVA defined prioritization QoS standards are required.

Applicability to Topologies

Topology	Applicability
Device-level Topologies using EtherNet/IP 2-port Embedded Switch Technology	EtherNet/IP 2-port Embedded Switch Technology utilizes ODVA QoS definitions – no configuration required.
Managed Switch-level Topologies	Stratix Managed Switches utilize ODVA QoS definitions – enabled by default

Multicast Management

Additional Resources

Resources	Description

Converged Plantwide Ethernet (CPwE) Design and Implementation Guide Publication ENET-TD001, Page 118 Bookmark = Multicast Management	This publication describes the design and implementation guidelines of a Converged Plant-wide Ethernet Network for Industrial Ethernet Applications.

Multicast traffic can be an important consideration of a Cell/Area Zone network because it is used by some of the key IACS communication protocols. Unmanaged multicast traffic is treated by the network infrastructure as a Layer 2 broadcast; every IACS device on the network receives the message. The impact increases exponentially as more multicast producing endpoints are added to the LAN.

Internet Group Management Protocol (IGMP) is a communication protocol used to manage the membership of IP multicast groups. Without IGMP, switches treat multicast packets the same as broadcast packets. Multicast packets are re-transmitted (flooded) to all ports within the same VLAN. IGMP enables the network infrastructure to understand which endpoints are interested in which multicast data, and thus to forward the messages only to those endpoints that want them. This reduces the amount of traffic the network and endpoints must handle.

When IGMP snooping is enabled, the switch listens to IGMP traffic and develops a table that lists the multicast groups and the end devices. Thus, when a multicast packet is received, the switch forwards it only to end devices that want it.

If multicast packets mix with enterprise or IT traffic, there is the distinct potential of redundant use of multicast group addresses that would lead to disruptions in both the IACS and the relevant IT application. For this and many other reasons, it is recommended that an IDMZ between the Industrial and Enterprise zone be deployed to ensure that IACS multicast traffic and IT-driven multicast traffic remain separate.

Multicast Management Summary

- IGMP Querier functionality manages a table that lists the devices that are participating in multicast groups
- IGMP Snooping functionality inspects packets from devices and forwards multicast data only to devices that request the data
- IGMP snooping constrains the flooding of multicast traffic by dynamically configuring switch ports so that multicast traffic is forwarded to ports associated with only a particular IP multicast group

Multicast Management Guidelines and Best Practices

- Configure the network infrastructure switches to leverage IGMP Querier and IGMP Snooping functions
- Enable the IGMP Querier function on the highest Layer switch with the lowest IP Address within the defined VLAN
- Enable IGMP snooping on all of the switches
- Stratix Managed Switches and end devices all support IGMP Version 2; the application should be configured to operate using IGMP Version 2 to avoid any compatibility issues

Multicast Management Questions

- Does your application utilize controller redundancy (controller redundancy requires the use of multicast I/O)? If yes, then IGMP multicast management capabilities are required.
- Does your application require time synchronization (CIP Sync requires the use of multicast packets)? If yes, then IGMP multicast management capabilities are required.

- Does your application utilize multicast packets (e.g., shared I/O, Produce/Consume tags, etc.)? If yes, then IGMP multicast management capabilities are required.

Applicability to Topologies

Topology	Applicability
Device-level Topologies using EtherNet/IP 2-port Embedded Switch Technology	EtherNet/IP 2-port Embedded Switch Technology leverages IGMP capabilities. IGMP Snooping is enabled by default on devices that support it. IGMP Querier is disabled by default on devices that support it.
Managed Switch-level Topologies	Stratix Managed Switches are IGMP capable but IGMP Querier and IGMP Snooping must be configured on the switches that require it.

Time Synchronization – IEEE 1588 PTP, End-to-End mode

Motion control is one of many applications that require time synchronization in the control system. In addition to motion control, there are sequence-of-events applications where time stamping is required to determine the order in which certain events occurred. There are data logging applications that use time to associate when data was collected from the system, as well as scheduled-output applications, in which an output can be triggered based on time.

Each of these applications requires different levels of time accuracy. Most data logging applications need little more than one-tenth of a second to a second of accuracy when logging data. Motion control, on the other hand, usually requires a much higher degree of synchronization; normally in microseconds (µs) of accuracy.

CIP Sync is the name given to the CIP (Common Industrial Protocol) implementation of time synchronization using the IEEE 1588-2008 Precision Time Protocol, end-to-end mode.

From the IEEE 1588 specification:

> *"The IEEE 1588 standard specifies a protocol to synchronize independent clocks running on separate nodes of a distributed measurement and control system to a high degree of accuracy and precision. The clocks communicate with each other over a communication network. In its basic form, the protocol is intended to be administration free. The protocol generates a master slave relationship among the clocks in the system. Within a given subnet of a network there will be a single master clock. All clocks ultimately derive their time from a clock known as the grandmaster clock. The communication path between any clock and its grandmaster clock is part of a minimum spanning tree."*

Precision Time Protocol Questions

- Does your application require CIP Sync capabilities (see CIP Sync section questions)? If yes, then Precision Time Protocol capabilities are required.
- Does your application require CIP Motion capabilities (see CIP Motion section questions)? If yes, then Precision Time Protocol capabilities are required.

CIP Sync

Additional Resources

Resources	Description
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide Publication ENET-TD001, Page 375 Bookmark = CIP Sync Sequence of Events	This publication describes the design and implementation guidelines of a Converged Plant-wide Ethernet Network for Industrial Ethernet Applications.
Integrated Architecture and CIP Sync Configuration Publication IA-AT003	This publication explains the CIP Sync technology and how you can synchronize clocks within the Rockwell Automation Integrated Architecture.

CIP Sync is the name given to time synchronization services for the Common Industrial Protocol (CIP). These services allow accurate real-time synchronization of devices and controllers connected over networks that require time-stamping, sequence of events recording, distributed motion control, and other highly distributed applications that need increased control coordination.

CIP Sync uses the IEEE 1588 "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", referred to as Precision Time Protocol (PTP), to synchronize devices to a very high degree of accuracy. CIP Sync provides very high accuracy beyond those attainable with the Network Time Protocol (NTP). CIP Sync is based on the IEEE 1588 standard, PTP, end-to-end mode. PTP provides a standard mechanism to synchronize clocks across a network of distributed devices.

The PTP uses various types of clocks which are summarized below.
Grandmaster clock - The Grandmaster clock provides a Master time reference for the Slave clocks, responds to requests from Slave clocks to measure network latency, provides information describing the clock quality of the Grandmaster, provides additional management and identification data to Slave clocks, and releases Mastership if a better quality clock comes into the system.

Slave clock – A slave clock synchronizes the local clock to the Master time reference, synchronizes the local clock frequency to match the Master reference frequency, occasionally generates requests to measure network latency, monitors information describing the clock quality of new Master clocks that may appear, and switches to a new Master when a Master clock appears that is better than the current Master.

Boundary clock - Boundary clocks function as a "boundary" or interface between PTP synchronization segments, intercepting upstream PTP messages and then generating new PTP messages. A boundary clock uses its own separate but synchronized clock. These devices synchronize their internal clock to a higher quality Grandmaster clock. Time synchronization packets sent are timestamped by using their own internal time reference. Standard or non-PTP messages are allowed to pass uninterrupted through the switch. Boundary clocks are multi-port clocks where one port is typically a slave to an upstream master, while the remaining ports become masters to the downstream devices.

Transparent clock - A transparent clock is a switch (or router) that has more than one port and compensates for delays within the device. It improves time synchronization accuracy by compensating for the delay. Transparent clocks measure the residence time (or the time to propagate through the switch) of the PTP messages as they pass between ports. The measured residence times are used to update the correction fields of the PTP timing messages. The residence time varies packet-to-packet based on network traffic. There are two types of transparent clocks but only one (end-to-end) supports CIP Sync. End-to-end transparent clocks compensate for the residence time as the PTP messages pass between ports. The residence time is then added to the correction field of the PTP packet. This correction field ensures that the downstream clocks will be able to properly compensate for switch latency.

The CIP Sync packets, used for IEEE 1588 time synchronization, are exchanged between the grandmaster clock and all CIP Sync slave devices (for example, the Kinetix 6500, CIP Sync I/O) once every second. These time-critical components are equipped with transparent clocks to handle the re-phasing of time as the time sync messages pass through each device.

Switches that do not have 1588 time-synchronization capabilities (transparent or boundary clock capabilities) are not capable of re-phasing time or regulating against the grandmaster in any way. Any time-synchronized packet passing through the switch experiences delays passing; and these delays vary from instance to instance, depending on such factors as traffic loading. Because there is no time awareness in these switches, the delays are not included in the time adjustment calculation and therefore time synchronization becomes unpredictable.

CIP Sync Summary

- The master-slave PTP port assignment is determined by the Best Master Clock algorithm, as each of the ports interrogates adjacent clocks to compare credentials. The port that is connected to the "best" clock becomes the slave PTP port.
- Only end-to-end transparent clocks are supported by CIP Sync. Peer-to-peer transparent clocks are not supported.
- It is important to position the devices properly when using a linear topology. Devices requiring time synchronization should be neighbors (e.g., controller next to servo drive). Switches that don't support the 1588 time synchronization capabilities will introduce delays manifesting as time variations. The time variations could cause unacceptable disturbances in the motion system.
- Transparent clocks are effective in long linear topologies (up to 50 or more links). The inherent nature of a transparent clock allows cascaded connections to properly compensate for end-to-end propagation delay caused by variable switch latency.

CIP Sync Guidelines and Best Practices

- If you have a large system, and there are only a few devices that you want to avoid using as a Grandmaster, you can set the priority values for those few devices greater than 128 and let the remaining devices (including new, out-of-box devices you add later) negotiate normally.
- If you have only a few devices from which you want to choose a Grandmaster, set the priority values to less than 128 for those few; this will block modules with default settings from becoming Grandmaster.
- Transparent clocks provide the highest level of performance for most small-to-medium sized CIP Sync architectures.
- Boundary clocks do a good job of coordinating time and are less susceptible to architectural depth and system traffic than switches with no level of implementation. Boundary clocks are generally sufficient for general time stamping of data (alarm data).

CIP Sync Questions

- Does your application utilize sequence of event (SOE) modules or require SOE first fault reporting? If yes, then CIP Sync is required.
- Do you need Cell/Area Zone synchronization of time with devices on the network? If yes, then CIP Sync is required.
- Does your application require accurate time stamp data (i.e., alarm and event data)? If yes, then CIP Sync is required.
- Does your application include integrated motion on EtherNet/IP networks? If yes, then CIP Sync is required.

CIP Motion

Additional Resources

Resources	Description
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide Publication ENET-TD001, Page 309 Bookmark = CIP Motion	This publication describes the design and implementation guidelines of a Converged Plant-wide Ethernet Network for Industrial Ethernet Applications.
Design and Implementation Guide for Using Integrated Motion on EtherNet/IP Publication ENET-WP035	This publication provides a brief overview of the guidelines for using Integrated Motion on EtherNet/IP.

EtherNet/IP uses CIP Motion and CIP Sync to achieve real-time motion control. CIP Sync uses the IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, commonly referred to as the Precision Time Protocol (PTP), to synchronize devices to a very high degree of accuracy. CIP Sync incorporates the IEEE 1588 services that measure network transmission latencies and corrects for infrastructure delays. The result is the ability to synchronize clocks in distributed devices and switches to within hundreds of nanoseconds of accuracy.

When all the devices in a control system share a synchronized, common understanding of system time, very precise control can be accomplished by including time as a part of the motion information. Unlike approaches to motion control that rely on scheduling, the CIP Motion solution does not schedule the network to create determinism. Instead, CIP Motion delivers the data and the timestamp for execution as a part of the packet on the network. This allows motion devices to follow positioning path information according to a pre-determined execution plan. Because the motion controller and the drives share a common understanding of time, the motion controller can tell the drive where to go and what time to be there.

CIP Motion Summary

- Applications that require high accuracy and performance, (for example, high performance motion control) should use devices and switches that support time synchronization and that implement transparent clock or boundary clock mechanisms.
- Application (CIP) types can be mixed on the same subnet/VLAN as long as those devices that require high precision have a clear view of the system time master by using devices that maintain time accuracy through the use of transparent or boundary clocks.
- The use of transparent and boundary clocks, as well as QoS, makes the system extremely robust to variations in network loading.
- Grandmaster clock changes are very disruptive to plant-wide time for 5-15 minutes following the event. You could experience jitter storms where average jitter exceeds several milliseconds and 100µs registration misalignments between motion axes.
- Changing the wallclock of the Grandmaster is very disruptive and will impact motion applications.

CIP Motion Guidelines and Best Practices

- The preferred network location of the Grandmaster clock is where it will not be interrupted if a portion of the machine/equipment is taken offline for service.
- For systems that cannot tolerate high jitter spikes and registration misalignments, use a dedicated Grandmaster clock.
- Writing to the wallclock of a controller configured as the Grandmaster should be avoided during active motion.

- Don’t apply a boundary clock to more than one or two hops because multiple hops can reduce the accuracy of the clocks needed for a motion control system. If more than one hop is needed, use a transparent clock for downstream devices.

CIP Motion Questions

- Does your application include integrated motion on EtherNet/IP networks? If yes, then CIP Motion is required.

Applicability to Topologies

Topology	Applicability
Device-level Topologies using EtherNet/IP 2-port Embedded Switch Technology	Transparent Clock
Managed Switch-level Topologies	Transparent or Boundary clock options

Network Availability

Additional Resources

Resources	Description
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide Publication ENET-TD001, Page 105 Bookmark = Availability and Network Resiliency	This publication describes the design and implementation guidelines of a Converged Plant-wide Ethernet Network for Industrial Ethernet Applications.
Deploying the Resilient Ethernet Protocol (REP) in a Converged Plantwide Ethernet (CPwE) Architecture – Design and Implementation Guide Publication ENET-TD005	This publication describes the design and implementation guidelines for deploying the Resilient Ethernet Protocol (REP). The CPwE-REP Cisco® Validated Design (CVD) describes the implementation of Resilient Ethernet Protocol (REP) for a switch ring topology in the CPwE system.

Availability of the network is critical in IACS applications. If the OEM machine or equipment will be connected to the plant-wide network, then it is important for the OEM to have some knowledge of how the infrastructure will be implemented to support availability and resiliency and the requirements for connection to that infrastructure. Therefore, a brief overview is provided on the various resiliency protocols that could be used. Note: On larger machines/equipment that utilize multiple managed switches, these protocols can still be applied.

Resiliency Protocols and Loop Prevention

A resiliency protocol maintains parallel links for redundancy while avoiding Layer 2 loops. Layer 2 loops occur when there is more than one path between two endpoints (e.g., multiple connections between two network switches or two ports on the same switch connected to each other). Network convergence time is a measure of how long it takes to detect a fault, find an alternate path, and recover from the fault. During the network convergence time, some portion of the traffic is dropped by the network because interconnectivity does not exist. Communication connections drop if the convergence time is longer than the connection timeout.

Redundant paths can create a switching (bridging) loop. Redundant paths occur in ring and redundant star topologies. A resiliency protocol is required to eliminate loops in the network. 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. A Layer 2 resiliency protocol maintains redundant paths while avoiding switching (bridging) loops.

Resiliency Protocols

- Spanning Tree Protocol (STP), Rapid STP (RSTP), Multiple Instance STP (MSTP); IEEE standards
- Resilient Ethernet Protocol (REP); Cisco Technology
- EtherChannel Link Aggregation Control Protocol (LACP); IEEE standard
- Flex Links; Cisco Technology
- Device Level Ring (DLR) Protocol; ODVA

Spanning Tree Protocol (STP), Rapid STP (RSTP), Multiple Instance STP (MSTP)

Spanning Tree Protocol (STP) is designed to run on bridges and switches. Its main purpose is to ensure that loops are avoided when there are redundant paths by deterministically blocking appropriate interfaces. If a link failure occurs in such a network, the STP is responsible for establishing a new path for data traffic.

Spanning Tree is arguably the only standard network protocol commonly available from a wide-range of vendors and across any type of topology. Spanning Tree is an IEEE standard. This IEEE standard has gone through several revisions since its conception which are summarized as follows:

- Original Spanning Tree incorporated into IEEE 802.1D. STP will recover from a topology change in less than 60 seconds. Generally speaking, STP is too slow to use in IACS networks.
- Rapid Spanning Tree known as IEEE 802.1w now incorporated into IEEE 802.1D- 2004, which significantly reduced the convergence time.
- Multiple Spanning Tree known as IEEE 802.1s now incorporated into IEEE 802.1Q-2003 extends the RSTP to work with multiple VLANs. MSTP is the default for the Stratix Managed Switches.

Note: Unmanaged switches do not support STP or RSTP, or any other resiliency protocol.

Resilient Ethernet Protocol (REP)

REP is a Cisco protocol that provides an alternative to STP to control network loops and handle link failures, and to improve convergence time significantly. It is the only ring switch-level resiliency protocol applicable to both Industrial Automation and IT applications. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment.

A REP segment is a chain of switch ports connected to each other and configured with the same segment ID. Each end of a segment terminates on what is called the “edge port” of an edge switch. With REP, in order to prevent a loop in the network, one switch port (the alternate port) is always blocked in any given segment. The blocked port helps ensure that the traffic within the segment is loop-free by requiring traffic flow to exit only one of the edge ports. Therefore, when a failure occurs in the segment, REP opens the alternate port so traffic can reach the edge of the segment. Refer to Figure 12 - Example REP Segment.

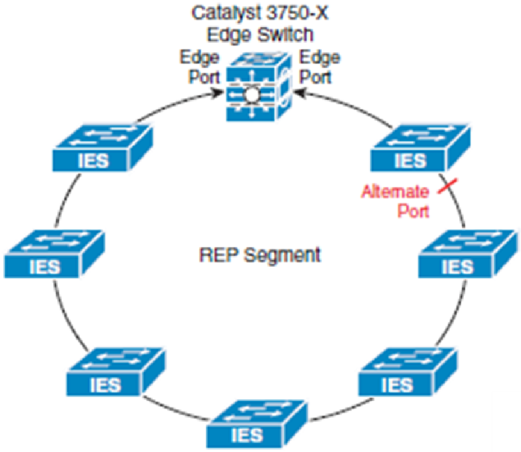


Figure 12 - Example REP Segment

When determining where and how to deploy REP segments in an IACS architecture, consideration must be given to the number of devices and/or switches attached to the REP segment, the number of VLANs configured within the REP segment, and the number of MAC addresses that will be utilized in the REP segment. The combination of these factors affect the recovery time of a REP segment during failover.

Another important factor to consider when designing a REP ring is latency. Since latency is a cumulative process based on the number of switches and/or other devices between the start and end points of a packet, limiting the size of the ring also becomes extremely important if latency is a determining factor in the design. Every device that the packet must pass through, such as a switch, adds latency to the data path.

REP is suitable for IACS applications that can tolerate up to a 100ms network convergence recovery time on fiber interfaces. Some example applications include; Controller to Human Machine Interface (HMI), Controller to Controller, Controller to I/O, Controller to variable frequency drives (VFDs), and Controller to Motor Control Centers (MCCs). Applications with integrated safety, motion or large amounts of multicast traffic are not suitable for REP.

In many MCC-based applications, device and I/O RPI settings as fast as the default 20ms are not required. For applications that can perform appropriately with device and I/O RPI settings of 100ms or greater, a Fast Ethernet (100 Mbps) copper switch-to-switch connection can provide sufficient convergence in a REP topology.

EtherChannel Link Aggregation Control Protocol (LACP)

EtherChannel and Link Aggregation Control Protocol (LACP) are designed to provide additional bandwidth between two devices by aggregating multiple Ethernet connections into a higher bandwidth virtual connection. However, these protocols need to quickly recover from the loss of one or more channel members. This fast recovery from a failure of an individual channel member can be used to provide link redundancy between two devices.

EtherChannel bundles multiple Ethernet links between two switches into a single logical link. EtherChannel balances the traffic load across the various physical links. When a physical link is lost, the EtherChannel load balancing algorithm stops using the lost link and uses the available links. When the link is restored, EtherChannel resumes balancing the load across the available link. In this way, EtherChannel can be used as a resiliency protocol when multiple links exist between two switches. To be used as a resiliency protocol, the switches must have redundant links between each other, such as in the redundant star topology. EtherChannel cannot be used in a ring topology as a resiliency protocol where the switches have one physical link between each switch.

Flex Links

Flex Links is a Cisco-proprietary resiliency protocol that is an alternative to STP and EtherChannel in redundant star networks. Flex Links are a pair of switch ports or port channels where one interface is configured to act as a backup to the other. With Flex Links, you define an active uplink interface (primary) and a backup uplink interface (standby). When the primary interface is active, it begins forwarding the traffic (sending and receiving frames just like any other port). The backup interface is in a standby state and does not send or receive any packets. When a failure is detected on the forwarding link, the MAC address and multicast entries are transferred to the standby link. When the failed interface is restored, it becomes the standby link.

Flex Links contains features to improve the recovery of multicast traffic (i.e., CIP I/O traffic). The Flex Links features converge the multicast traffic resulting in little to no outage to the EtherNet/IP connections. Flex Links is the preferred CPwE resiliency protocol for a switch-level redundant star topology. Flex Links does not function in a ring topology.

EtherNet/IP 2-port Embedded Switch Technology – Device Level Ring (DLR) Protocol

The DLR protocol is a Layer 2 protocol that provides link-level, physical redundancy. It provides network convergence in the 1…3ms range for simple IACS device-level networks. DLR provides resiliency directly to an end device (such as an I/O module, drive, or controller). The ring is a single fault tolerant network.

Some control applications, such as safety and motion, require network convergence times faster than what switch-level resiliency protocols can provide. In these cases, using the EtherNet/IP 2-port Embedded Switch and the DLR protocol is the only alternative.

Network Availability Summary

- Network convergence (healing, recovery, etc.) must complete before the IACS application is impacted
- Network convergence must occur quickly enough to avoid a controller connection timeout
- 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 and jitter

Network Availability Guidelines and Best Practices

- Utilize a single STP implementation across the entire IACS network to avoid any incompatibility between the variants
- Use fiber media and SFPs for all inter-switch links ring and redundant star switch-level topologies

- Use MSTP for multi-vendor switch deployment, redundant star or ring switch-level topologies, with CIP explicit messaging such as HMI, or unicast CIP implicit I/O applications with an RPI of greater than or equal to 100ms
- Use EtherChannel & LACP for increased bandwidth or to balance traffic across switch ports in a redundant star switch-level topology, with CIP explicit messaging such as HMI
- Use Flex Links for Stratix Managed Switch deployments – redundant star switch-level topology, with unicast or multicast CIP implicit I/O applications
- Use REP for Stratix Managed Switch deployments - ring switch-level topology, with unicast CIP implicit I/O applications
- Use DLR for ring device-level topology, and for applications such as CIP Safety, ControlLogix Redundancy, multicast CIP I/O applications, and CIP Motion

The IACS application requirements will dictate the topology and protocols needed. It is important to note that there is a difference between network convergence and application recovery. It is possible that an application can be impacted even though network convergence times are acceptable (e.g., controller connection to I/O closes before network recovers).

Failures scenarios of an application should be considered to help determine acceptable risk and potential application impacts. What is the impact to the application when a single failure event occurs (e.g., module failure, end device failure, cable break, network storm/traffic flooding event, etc.)? Does the application need to handle more than one failure?

Network Availability Questions

- What network topology, ring or redundant star, is being used? Refer to Table 2 - Resiliency Protocols for a comparison chart for options to consider.
- What network convergence time can the IACS application tolerate? Refer to Table 2 - Resiliency Protocols for a comparison chart for resiliency options to consider.
- Does the IACS application utilize compatible infrastructure components? If yes, then leverage the more capable resiliency protocols (i.e., Flex Links, EtherChannel, REP, etc.)

Table 2 - Resiliency Protocols

Resiliency Protocol	Mixed Vendor	Ring	Redundant Star	Network Convergence > 250ms	Network Convergence 60 - 100ms	Network Convergence 1 - 3ms
STP (802.1D)	X	X	X			
RSTP (802.1w)	X	X	X	X		
MSTP (802.1s)	X	X	X	X		
rPVST+		X	X	X		
REP		X			X	
EtherChannel (LACP 802.3ad)	X		X		X	
Flex Links			X		X	
DLR (IEC and ODVA)	X	X				X

Applicability to Topologies

Topology	Applicability
Device-level Topologies using EtherNet/IP 2-port Embedded Switch Technology	Applies to Device-level Ring only.
Managed Switch-level Topologies	Options vary based on the topology and Managed Switch chosen

Network Address Translation (NAT)

Additional Resources

Resources	Description
Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture-Design and Implementation Guide Publication ENET-TD007	This publication describes the design and implementation guidelines for deploying Network Address Translation (NAT). The CPwE-NAT Cisco® Validated Design (CVD) outlines the key requirements and design considerations to help in the successful design and deployment of NAT within plant-wide architectures.
Stratix/Infrastructure Product Family NAT/VLAN Reference Drawings Publication IASIMP-QR030	This publication is a collection of drawings that provide use cases for the Network Address Translation (NAT) and VLAN capabilities in the Stratix/Infrastructure Product Family. It also compares and contrasts the different segmentation options available with NAT and VLANs.

Network Address Translation (NAT) enables the reuse of IP addressing without introducing a duplicate IP address error into your IACS application architecture.

Technology and business aspects drive the decision to use NAT. From a business perspective, OEMs use NAT to enable the replication of skids and machines, including IP addressing. NAT can help reduce development and commissioning costs. From a technology perspective, end users use NAT when the IP address space within the plant-wide network infrastructure is limited and not every device requires communication outside the skid or machine-level network.

NAT is a networking technology that enables control system engineers to build IACS applications using duplicate IP addresses, while allowing those IACS applications to integrate into the larger plant-wide architecture. When the applications are integrated the devices will need to utilize unique IP addressing. NAT can be configured to translate only specific IP addresses from inside the IACS application to the outside plant-wide architecture. Doing so provides an added benefit of effectively hiding the inside IP addressing schema of the IACS application.

NAT translations have two forms: one-to-one (1:1) and one-to-many (1:n). Stratix Managed Switches use one-to-one NAT, implemented in a Layer 2 access switch. A Layer 2 NAT device has two translation tables where inside-to-outside and outside-to-inside subnet translations can be defined. This unique implementation provides wire speed performance and supports multiple VLANs through the NAT boundary for enhanced network segmentation.

A Layer 3 NAT device has only one translation table for inside-to-outside translations and does not translate outside IP addresses back to inside IP addresses. Devices on the inside (machine/equipment) network use a gateway address to communicate with the outside (plant-wide) network. A Layer 3 NAT device is typically a software-based implementation resulting with performance based on the CPU processing power and current loading.

NAT Summary

- NAT enables the reuse of IP addressing without introducing a duplicate IP address error into your IACS application architecture.
- NAT allows OEMs to develop standard machines and eliminate the need for unique IP addressing and code modifications.

- NAT helps reduce development and commissioning costs when machines/equipment are replicated.
- NAT allows end users to more easily integrate machines/equipment into their larger plant-wide network without extensive coordination with their OEMs.
- NAT can save limited IP address space within the plant-wide network infrastructure by only exposing the devices that need to communicate outside the machine/equipment.
- NAT can add complexity to the plant-wide network design if not implemented correctly or implemented without real need.
- Some types of traffic (e.g., HTTP, DCOM, multicast traffic, etc.) are not supported across the NAT boundary.
- Asset management of the end nodes (inside) is dependent on whether the end node is contained in the NAT table and made available (outside).
- Three types of translation can be implemented; single, range, and subnet.

NAT Guidelines and Best Practices

- Restrict the NAT translations to only the IP addresses that are required outside (i.e., don't translate all inside devices to outside addresses).
- NAT is not always the correct solution (e.g., expecting to save plant-wide IP addresses but then translating the addresses of all devices on OEM machine/equipment).
- Use proper segmentation methods as outlined previously and limit the total number of translated addresses in the Layer 2 network to avoid issues such as excessive broadcast traffic.
- Select the proper NAT device based on the application requirements (e.g., total number of translations, performance of NAT device, etc.).
- Keep documentation up-to-date otherwise the maintenance of NAT tables can become cumbersome.
- HMI client/server communication may not operate correctly across a NAT boundary because it relies on OPC and DNS therefore do not use a distributed HMI network application with NAT between servers and clients. It is acceptable for the controller to reside on the inside with the HMI data server on the outside of the NAT boundary.

NAT Questions

- Do you need to replicate machines/equipment without having to reprogram logic each time to satisfy end user IP addressing requests? If yes, then NAT can be a potential solution.
- Do you want to protect (hide) end devices within your machine/equipment level network from potential end user traffic? If yes, then NAT can be a potential solution.
- Does the machine/equipment you produce have significant variations in layout, design, and control programs? If yes, then NAT is probably not a good solution.
- If the machine/equipment is being integrated into a plant-wide network, do all the machine/equipment nodes need to be exposed to the plant-wide network? If yes, then NAT is probably not a good solution.
- Does the end user typically use an architecture with multiple networks (and network cards) segmented based on function and the machine/equipment controller you are furnishing does not have this capability? If yes, then NAT can be a good solution.

Applicability to Topologies

Topology	Applicability
Device-level Topologies using EtherNet/IP 2-port Embedded Switch Technology	Applicable but requires additional networking infrastructure.
Managed Switch-level Topologies	Applicable but not on all Managed Switches

Dynamic Host Configuration Protocol (DHCP)

Additional Resources

Resources	Description
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide Publication ENET-TD001, Page 447 Bookmark = DHCP Persistence in the Cell/Area Zone	This publication describes the design and implementation guidelines of a Converged Plant-wide Ethernet Network for Industrial Ethernet Applications.

DHCP is an auto-configuration protocol used in IP networks. DHCP allows the IP address, subnet mask, and default gateway of any node to be configured automatically from a switch, router or central server. The primary reason for using DHCP on an IACS network is to allow server (switch) management of addressing. Because a server manages IP address allocation, it is unnecessary to statically configure some IACS device addresses. This can save significant configuration time during maintenance.

DHCP Persistence enables IACS implementers to reserve and pre-assign an IP address to a specific switch port. This enables an IACS device connected to that switch port, configured for dynamic IP allocation, to always receive a consistent IP address regardless of its MAC address. This capability helps to reduce the amount of time required to provision or replace IACS devices, such as drives and I/O. This also helps to reduce the required level of skilled resources to provision or replace an IACS device.

Because DHCP Persistence allows only a single device to be connected per port, do not use DHCP

Persistence with two-port Ethernet modules. If you attempt to use DHCP Persistence with these modules, only the first module in a line or ring is assigned an IP address. The remaining modules downstream are not assigned IP addresses.

DHCP Snooping is a feature applied to ensure the security of an existing DHCP infrastructure. DHCP Snooping prevents unauthorized DHCP servers from assigning addresses to clients. When DHCP Snooping is enabled on a switch, the switch can a) track the physical location of hosts, b) ensure that hosts use only the IP addresses assigned to them, and c) ensure that only responses from authorized DHCP servers are communicated to the end device. This feature helps ensure the deterministic nature similar to static IP addressing by ensuring only the appropriate server (in this case the switch to which the end device is connected) assigns the IP address.

DHCP Guidelines and Best Practices

- Plan IP addressing, VLAN scheme and designated switch port; then configure switch ports to assign specific IP Addresses based on the assigned end device.
- Set up the industrial Ethernet switch with DHCP Persistence with planned IP addresses.
- Ensure devices being connected to a network switch port utilizing DHCP Persistence is configured to get an IP address assignment via DHCP (the factory default setting for a new device is BOOTP/DHCP).
- Do not mix dynamic assignments and reservations on the same VLAN (i.e., one switch configured as a DHCP Server and one switch configured as a DHCP Server with DHCP persistence).
- Enable DHCP Snooping on the switch to prevent rogue DHCP servers from assigning IP addresses to the end nodes.
- Do not use DHCP Persistence on EtherNet/IP 2-port Embedded Switch Technology devices unless you do not intend to connect anything downstream of the device (i.e., on the second port).

DHCP Questions

- Are you using EtherNet/IP 2-port Embedded Switch Technology for a line or ring of devices? If yes, then DHCP cannot be used.
- Are you trying to simplify procedures when a device is replaced on a network? If yes, then DHCP could be a good solution.
- Are you trying to simplify procedures when a new device (planned) is added on a network? If yes, then DHCP could be a good solution.
- Do you intend to leverage the Automatic Device Configuration feature available in some Rockwell Automation products? If yes, then DHCP is required.

Applicability to Topologies

Topology	Applicability
Device-level Topologies using EtherNet/IP 2-port Embedded Switch Technology	Not Applicable, unless you do not intend to connect anything downstream of the device (i.e., on the second port).
Managed Switch-level Topologies	Applicable on all Stratix Managed Switches

Physical Layer Infrastructure

Wired Infrastructure

Additional Resources

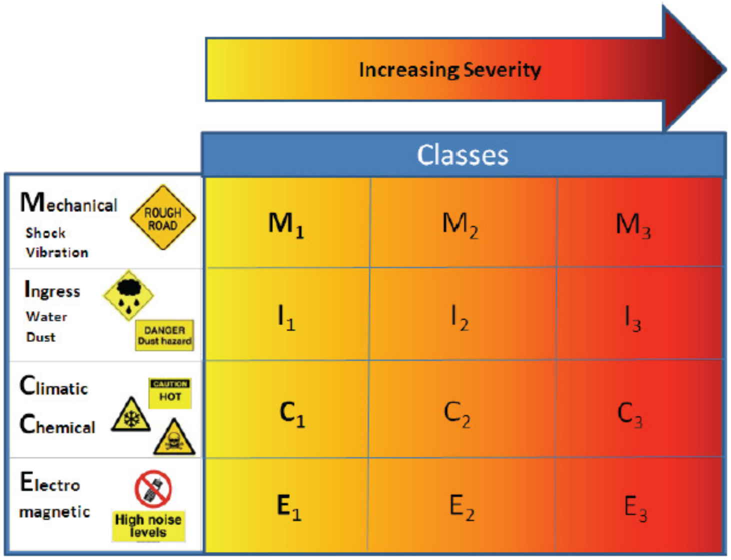
Resources	Description
Guidance for Selecting Cables for EtherNet/IP Networks Publication ENET-WP007	This publication provides guidance to the user on selecting cabling based on the application, environmental conditions, and mechanical requirements.
EtherNet/IP Media Planning and Installation Manual Publication PUB00148RO	This publication by the ODVA describes the required media components and how to plan for, verify, troubleshoot and certify EtherNet/IP networks.
Fiber Optic Infrastructure Application Guide Publication ENET-TD003	This publication details methods for deploying a fiber optic physical infrastructure to support the Converged Plant-wide Ethernet Network.
Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide Publication PANDUIT / Physical Infrastructure Reference Architecture Guide	This publication provides guidance for designing, deploying and managing the physical infrastructure for an Industrial Ethernet network following the Converged Plant-wide Ethernet Network.

Industrial network data requires an efficient and unified physical infrastructure to travel seamlessly throughout the plant -- and across the enterprise. The backbone of a unified network is a well-designed and reliable physical layer. The network's physical layer encompasses everything needed to achieve connectivity and for host applications to turn data into information and decision making– from conduit and cable, wireless access points to the network switches and the critical compute and data storage resources.

To ensure that your network investment delivers full value and maximum output, it's important to take a structured, engineered approach to the physical layer. That means identifying and evaluating everything from data throughput and the environment, to wiring distances and availability.

To aid in understanding the environment, a classification system called MICE (Mechanical, Ingress, Climatic/Chemical and Electromagnetic) is used. Cabling attributes and performance can be defined for the industrial areas based on the environments and conditions as defined by MICE severity levels called classifications.

Table 3 - MICE Classification Table


ROUGH ROAD
DANGER Dust hazard
CAUTION HOT
High noise levels

Increasing Severity

	Classes		
Mechanical Shock Vibration	M_1	M_2	M_3
Ingress Water Dust	I_1	I_2	I_3
Climatic Chemical	C_1	C_2	C_3
Electro magnetic	E_1	E_2	E_3

This system provides a method of categorizing the environmental classes for decision-making on the level of hardening required the network media, connectors, pathways and enclosures. A higher MICE level means that your physical infrastructure may need to be ruggedized for vibration, sealed for wash down, fabricated with materials that can withstand extreme temperatures, or shielded for rejecting EMI noise.

Cables can be shielded or unshielded. There are a number of factors in determining if shielded cabling or unshielded should be used. Some geographical areas mandate that shielded twisted pair (STP) cabling be used. Some companies have policies regarding the use of STP or unshielded twisted pair (UTP) cabling.

Fiber Optic cabling can be single mode or multimode. The selection to use fiber often comes down to two main factors, distance and noise immunity. The choice of single mode or multimode is usually driven by distance or end device support.

Table 4 - Cable Comparison

UTP versus STP	Unshielded Twisted Pair (UTP)	Shielded Twisted Pair (STP)
	Costs less Installs faster Smaller diameter, more flexible	Excellent immunity from EMI and RFI noise Can located cable close to sources of noise Well suited for more rigorous environments
Cat5E versus Cat 6	Cat5E	Cat6
	Costs less Suitable for speeds less than a gigabit	Higher signal to noise ratio, performance margins Designed to deliver gigabit performance
Copper versus Fiber Cabling	Copper	Fiber
	Termination and installation is faster Less fragile Distances of less than 100m	Cost of fiber transceivers is higher Use when excessive EMI noise is present Use when distance is a factor (over 100m)
Single mode versus Multimode Fiber	Multimode	Single Mode
	For distances of up to 550m @ 1G and 2km @ 100M Lower cost transceivers, connectors and installation Higher fiber cost, but lower total system cost	Longer distances (up to 40km) Higher bandwidth capabilities Lower fiber cost, but higher total system cost

Structured cabling solutions are available for the Control Room, Cell/Area Zones, Control Panels and On-Machine deployments.

For OEM solutions, the use of Zone Enclosures and the Zone Cabling approach can provide some benefits including cost savings, flexibility for machine moves/changes, and improved availability. The basic idea is to move infrastructure such as switches and patch panels that might be housed in racks or enclosures in a control room out to the manufacturing cell/area, closer to the machine/equipment.

Wireless Infrastructure

Additional Resources

Resources	**Description**
Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture – Design and Implementation Guide Publication ENET-TD006	This publication describes the design and implementation guidelines for using 802.11 Wireless LAN networking capabilities with emphasis on equipment connectivity. The CPwE-WLAN Cisco® Validated Design (CVD) provides design considerations for fixed position, nomadic and mobile equipment use cases, with scalability from small autonomous WLAN architectures to large plant-wide Unified WLAN architectures.
Wi-Fi for Industrial Applications Publication IASIMP-QR033	This publication is a high level reference drawing showing various components used in the deployment of a Wireless LAN solution.

Two wireless architectures are predominantly used in IACS environments: Autonomous WLAN and Unified WLAN.

The Autonomous WLAN architecture consists of stand-alone access points (APs) that implement all of the WLAN functions: management, control, data transport and client access. An example of an autonomous access point is the Stratix 5100 AP or any Cisco AP running the autonomous Cisco IOS software.

Each autonomous AP is configured and managed individually. Limited coordination of operation exists between autonomous APs, as well as limited capability to implement scalable solutions for configuration and firmware management, client mobility, WLAN security and resilience.

The Unified WLAN architecture has the ability to address large-scale plant-wide 802.11 wireless needs. The Unified Access architecture allows for centralized management and control of the wireless access points distributed throughout the plant.

By utilizing a Wireless LAN Controller (WLC) and Lightweight Access Points (LWAP), a centralized management model is created, thus introducing security and self-healing mechanisms to the wireless architecture. The Unified WLAN architecture also introduces foundational services, including intrusion prevention and wireless guest access, for better control over devices seeking to connect to the WLAN.

The main goal when designing wireless coverage for an IACS application is to provide adequate signal strength for wireless clients throughout the Cell/Area Zone and to be able to support the required data rate. In addition, wireless cell size should be controlled to achieve the desired number of clients per AP, and to minimize co-channel interference between cells.

It is critical to perform a professional site survey to determine the number and locations of the APs that can cover the area with the required level of redundancy. The site survey should also determine the appropriate antenna types and verify link performance and supported data rates. The survey needs to be executed where the machine/equipment will be installed and should be repeated as changes are made within the installed environment to ensure communication performance is adequately maintained.

Plant-wide Integration

Additional Resources

Resources	Description
Stratix/Infrastructure Product Family NAT/VLAN Reference Drawings Publication IASIMP-QR030	This publication is a collection of drawings that provide use cases for the Network Address Translation (NAT) and VLAN capabilities in the Stratix/Infrastructure Product Family. It also compares and contrasts the different segmentation options available with NAT and VLANs.
Segmentation Methods within the Cell/Area Zone – Application Guide Publication ENET-AT004	This publication describes the use of physical segmentation using the ControlLogix/CIP Bridge. It also reviews advantages and disadvantages of other segmentation methods that can be used within a Converged Plant-wide Ethernet architecture.

When OEM machines/equipment need to be integrated into a line or plant-wide network infrastructure, the OEM and end user or the end user's representative need to collaborate. It is critical for all parties to understand the integration plan and the expectations to meet the end user's requirements for resiliency, segmentation, security, and network management.

The high level architectures depicted in this section add to the standalone machine/equipment architecture shown previously. The green boxes shown offer some options for integration methods. The selection of the specific network components used will be determined based on the end user and application requirements.

Device-level Linear/Ring Topology – EtherNet/IP 2-port embedded switch technology

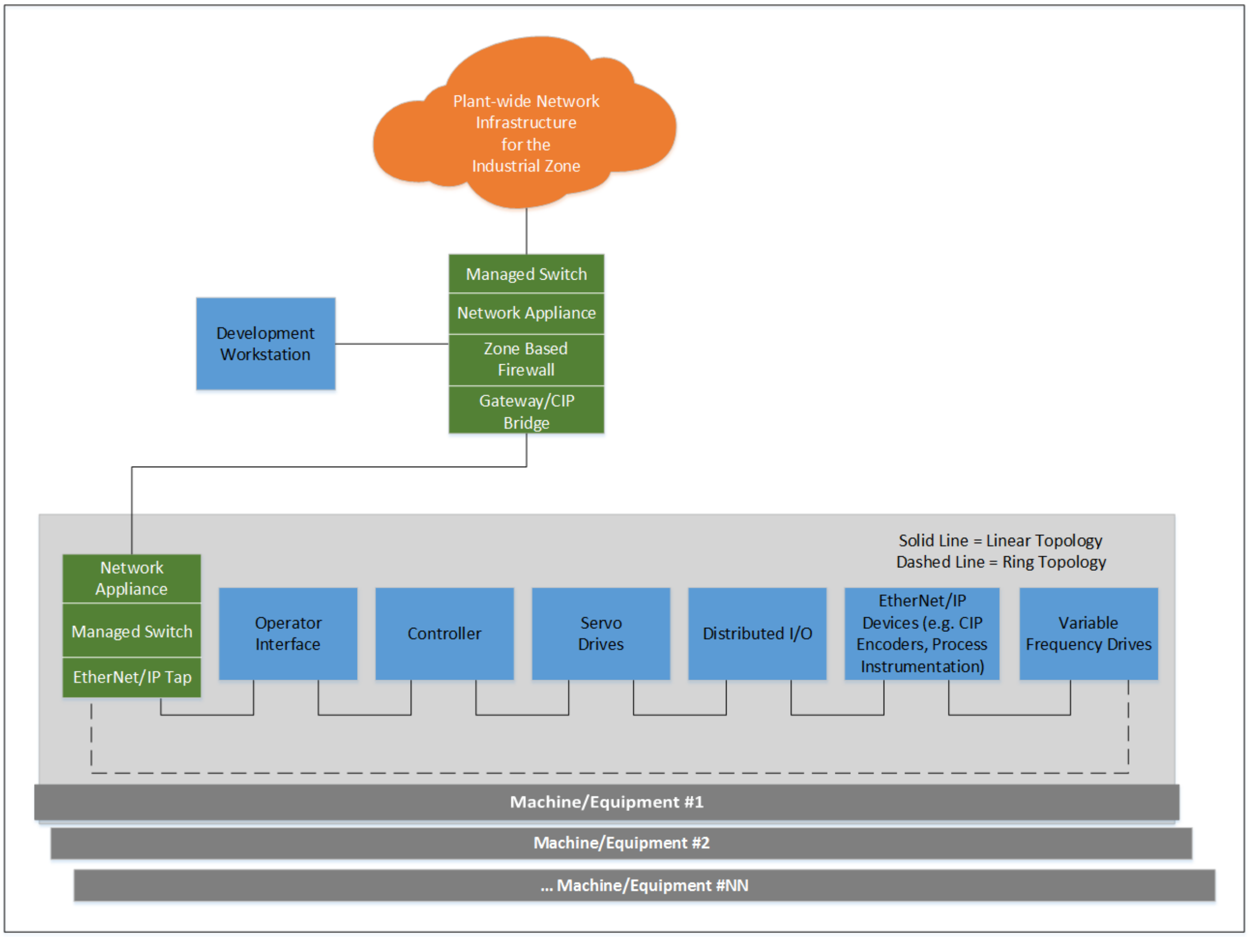


Figure 13 - Device-level Topologies Integrated to Plant-wide Networks

Managed Switch-level Topology

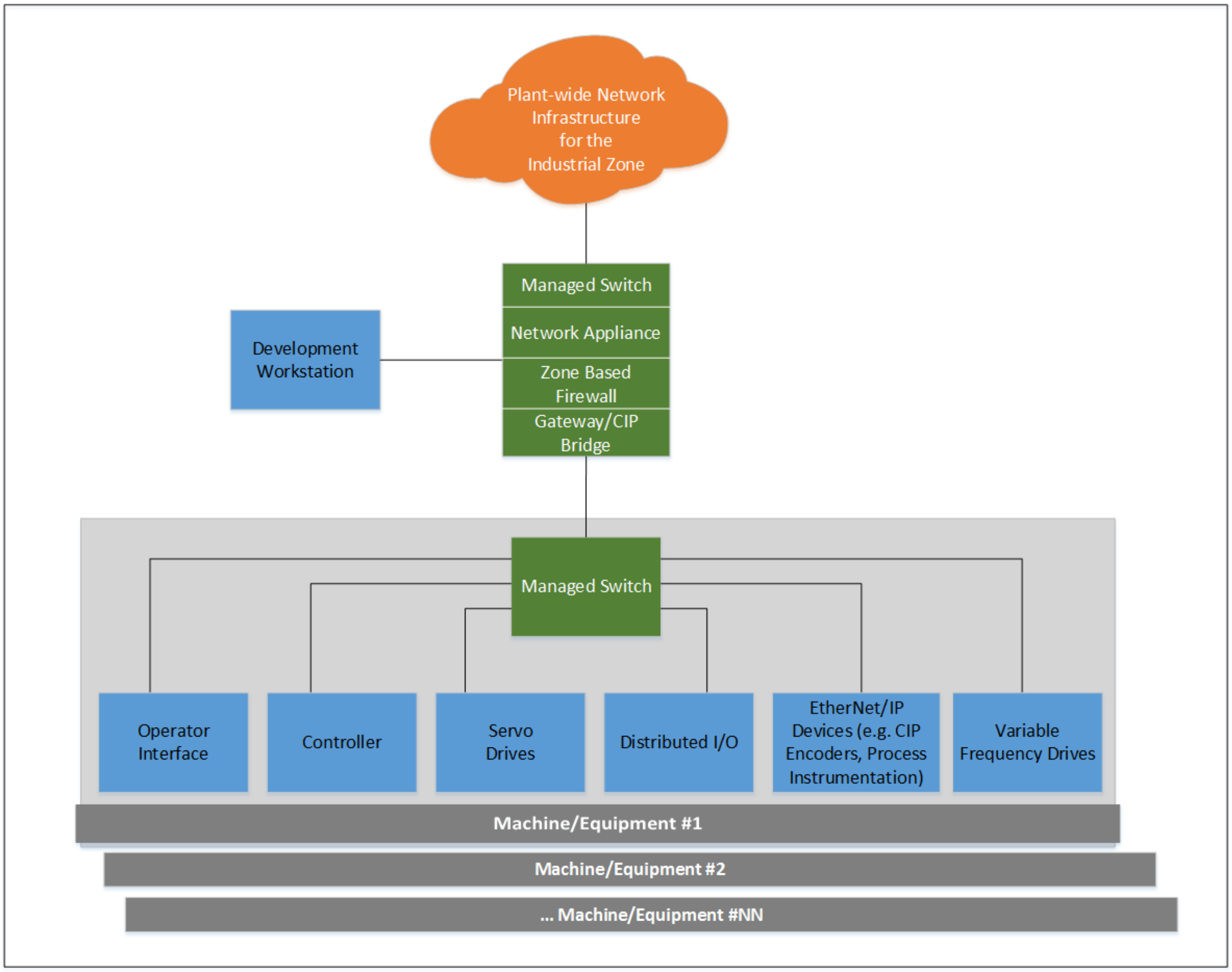


Figure 14 - Switch-level Topology Integrated to Plant-wide Networks

To determine the best component(s) to utilize within the green boxes shown in the high level architectures and who will supply these components requires all parties involved in the design to collaborate.

One of the first things to understand is who will be responsible for defining, managing and maintaining the addressing schema (IP Address, subnets, VLANs, etc.) used within the plant or within a Cell/Area Zone. This could be the end user's IT department, the end user's operations department (OT), an end user's designee (SI/SP, General Contractor, EPC firm, etc.), OEM or some combination.

The next question is how the party responsible for the addressing schema will disperse the addresses. Will an address range be provided (address range class, subnet, and gateway) or will assignments be made down to the end node? If an address range is given, are there any rules that need to be followed when assigning an IP address to a node from within the range provided?

It will also be necessary to understand the implementation conventions. For example, will addresses be manually set (static IP) or dynamically set (BOOTP/DHCP)? Will addresses be set via hardware for end nodes that provide this capability or will addresses always be set via software? Can a device that supports NAT be utilized? If yes, are there rules to follow when deploying these devices (e.g., specific devices must be translated)? Will DNS be used? If yes, who manages and maintains the DNS server?

Answers to many of the questions outlined in the network design considerations section (segmentation, security, availability, NAT, DHCP) will help are narrow in on acceptable solutions.

Finally, you must agree on who is responsible to provide the device used for integration. An OEM will need to account for the device and location of the device in their scope of supply.

Integration Options

- Managed Switches
  - Utilizing unique IP subnets/VLAN definitions
  - Utilizing NAT to allow reuse of IP subnets
- Network Appliance utilizing NAT
- Zone Based Firewall
- Gateway/CIP Bridge – Multiple network interface modules

Managed switches utilizing unique IP subnets/VLAN definitions – all nodes within the Industrial Zone must have unique IP addresses. Each Cell/Area Zone is segmented with a unique VLAN. Thus a Layer 3 device (switch or router) is required when communication must occur between Cell/Area Zones. OEMs must adhere to the plant-wide addressing schema. {Example architecture contained in Stratix/Infrastructure Product Family NAT/VLAN Quick Reference Drawings}

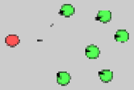
Managed switches utilizing NAT – IP addresses can be reused across Cell/Area Zones allowing OEMs to define their own IP addressing schema. The switch is configured to translate the OEM inside IP addresses to the plant-wide outside IP addresses for each device that needs to communicate to the plant-wide network. Resiliency options available. {Example architecture contained in Stratix/Infrastructure Product Family NAT/VLAN Quick Reference Drawings}

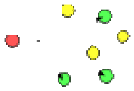
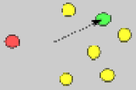
Network Appliance utilizing NAT - IP addresses can be reused across Cell/Area Zones allowing OEMs to define their own IP addressing schema. The network appliance must be configured to translate the OEM IP addresses to the plant-wide IP addresses for each device that needs to communicate to the plant-wide network. No redundant path topology options are available. {Example architecture contained in Stratix/Infrastructure Product Family NAT/VLAN Quick Reference Drawings}

Zone Based Firewall – This device offers security features, routing capabilities and NAT. The Security features include VPN support, Firewall, Encryption Services, and ACLs. Encrypted tunnels can be established between sites over a VPN connection. A Zone-Based Policy Firewall (ZFW) can be implemented within the Cell/Area Zone or OEM application (machine or equipment). It allows OEMs to define the flow of information and access to their machine/equipment from the plant-wide network while making use of features such as Network Address Translation (NAT). {Example architecture contained in Stratix/Infrastructure Product Family NAT/VLAN Quick Reference Drawings}

Gateway/CIP Bridge – - IP addresses can be reused across Cell/Area Zones allowing OEMs to define their own IP addressing schema. Only CIP traffic can traverse the CIP Bridge. Unwanted plant-wide traffic is blocked. This solution is easy to deploy but has limited scalability and requires EtherNet/IP modules be installed in the ControlLogix chassis. The Operations team can easily manage this solution.

Appendix 1: Key Terms/Acronyms and Definitions

Term/Acronym	Description/Definition
AAA	Authentication, Authorization and Accounting - AAA is a system for tracking user activities on an IP-based network and controlling their access to network resources. AAA is often implemented on a dedicated server.
ACL	Access Control List - An ACL is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation.
AP	Wireless Access Point – A wireless access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi.
Application Whitelisting	Application whitelisting is a computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.
ARP	The Address Resolution Protocol (ARP) is a telecommunication protocol used for resolution of network layer addresses into link layer addresses. ARP is used for converting a network address (e.g., an IPv4 address) to a physical address like an Ethernet address (e.g., MAC address).
BOOTP	Bootstrap Protocol – BOOTP is a computing protocol used to automatically assign an IP address to network devices.
Broadcast Packet	 A broadcast is an Ethernet packet that is transmitted to all nodes on the network. One to all.
Broadcast Domain	A broadcast domain is a logical division of a network, in which all nodes can reach each other by broadcast at the data link layer.
CIP	Common Industrial Protocol - The Common Industrial Protocol (CIP™) encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications – control, safety, synchronization, motion, configuration and information.
CPwE	Converged Plantwide Ethernet – The CPwE solution is designed for industrial Ethernet applications. It is built on guidelines from the Cisco Ethernet-to-the-Factory (EttF) solution and the Rockwell Automation Integrated Architecture.
DHCP	Dynamic Host Configuration Protocol - DHCP is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, devices request IP addresses and networking parameters automatically from a DHCP server.
DLR	Device Level Ring, EtherNet/IP 2-port embedded switch technology – DLR is a ring topology created at the end devices that utilize two network ports. A DLR network is a single-fault tolerant network.
DNS	Domain Name System – The DNS is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. Primarily, it translates domain names to numerical IP addresses.
EtherNet/IP 2-port embedded switches	The term "EtherNet/IP 2-port embedded switches" as used within this document refers to 2-port embedded switch technology products that comply with the ODVA EtherNet/IP standards.
EU	End User – the client or user of the product (machine/equipment) or service.
HMI	Human Machine Interface
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zone – The IDMZ is sometimes referred to as a perimeter network that exposes a trusted network to an untrusted network. The purpose of the IDMZ is to add an additional buffer layer of security. This buffer zone provides a barrier between the Industrial and Enterprise Zones, but allows for data and services to be shared securely.
IEC	International Electrotechnical Commission – The IEC is the world's leading organization for the preparation and publication of International Standards for all electrical, electronic and related technologies.
IEEE **802.3**	Institute of Electrical and Electronics Engineers IEEE 802.3 is a standard specification for Ethernet, a method of physical communication in a local area network (LAN). In general, 802.3 specifies the physical media and the working characteristics of Ethernet.
IETF	Internet Engineering Task Force – the IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
IGMP	Internet Group Management Protocol - IGMP is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. Without IGMP, switches treat multicast packets the same as broadcast packets.
IP	Internet Protocol - IP is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries
ISA	International Society of Automation – The ISA is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure.
Jitter	The amount of variance in the latency.
LACP	Link Aggregation Control Protocol – LACP applies to methods of combining (aggregating) multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail.
LAN	Local Area Network - A LAN is a computer network that interconnects computers within a limited area.
Latency	The average amount of time a message takes to be transmitted and processed from the originating node to the destination node.
MAC Address	A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment.

Term/Acronym	Description/Definition
Managed Switch	The term “managed switch” as used within this document refers to a switch that can support IACS applications and leverages Rockwell Automation and/or Cisco technology. Managed switches provide the ability to configure, manage, and monitor a LAN.
MCC	Motor Control Center – An MCC is an assembly of one or more enclosed sections having a common power bus and principally containing motor control units.
MSTP	Multiple Instance Spanning Tree Protocol – MSTP defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.
Multicast Packet	A multicast packet is an Ethernet packet that is transmitted from one sender to multiple destinations simultaneously. One-to-many. 
NAT	Network Address Translation - NAT is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
NTP	Network Time Protocol - NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
ODVA	The organization that supports the network technologies built upon the Common Industrial Protocol or “CIP” – EtherNet/IP, DeviceNet, CompoNet and ControlNet
OEM	Original Equipment Manufacturer – a company that manufactures machines or equipment and sells to clients (end users).
PTP	Precision Time Protocol – IEEE 1588-2008 Precision Time Protocol The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.
QoS	Quality of Service - QoS prioritizes traffic into different service levels and provides preferential forwarding treatment to some data traffic at the expense of lower-priority traffic.
RSTP	Rapid Spanning Tree Protocol - Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) is an evolution of the 802.1D standard. Cisco enhanced the original Spanning Tree Protocol 802.1D specification with features to speed up the convergence time of a bridged network.
REP	Resilient Ethernet Protocol - REP is a Cisco protocol that provides an alternative to STP to control network loops and handle link failures, and to improve convergence time significantly. It applies to switch-level ring topology.
SI/SP	Systems Integrator/Solution Provider – an engineering company that designs, develops, and delivers automation solutions.
SNMP	Simple Network Management Protocol - SNMP is an Internet-standard protocol for managing devices on IP networks. SNMP is widely used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
SOE	Sequence of Events
STP	Shielded Twisted Pair – when discussing media
STP	Spanning Tree Protocol – when discussing loop avoidance STP is an older network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them.
TIA **TIA-1005**	Telecommunications Infrastructure Standard Structured cabling in an industrial environment (e.g, (such as manufacturing facilities, laboratories, refineries, etc.) may be subject to more hostile environmental conditions that commercial building cabling plants.
Unicast Packet	A unicast packet is an Ethernet packet transmitted between two nodes on a network. Point-to-point. 
UTP	Unshielded Twisted Pair – when discussing media
VFD	Variable Frequency Drive
VLAN	Virtual LAN - A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.
VPN	Virtual Private Network – A VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.
VTP	VLAN Trunking Protocol - VTP is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network.
WLAN	Wireless Local Area Network - A WLAN is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, manufacturing operation, or office building.
ZFW	Zone Based Firewall – A ZFW is a stateful firewall that utilizes zones to control traffic. Interfaces will be assigned to zones and security policies will be assigned to traffic between zones.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846