Reference Architectures for Industrial Automation and Control Systems

Paul Didier
Solution Architect
Cisco

Presented at the ODVA
2012 ODVA Industry Conference & 15th Annual Meeting
October 16-18, 2012
Stone Mountain, Georgia, USA

Abstract

Rockwell Automation and Cisco have developed a set of Reference Architectures for Industrial Automation and Control Systems that promote use of standard Ethernet network functions in a hierarchical model. These architectures are designed to provide necessary levels of resiliency, scalability, security (including secure remote access) and high availability. The Reference Architecture has been adopted by numerous customers across a range of industries.

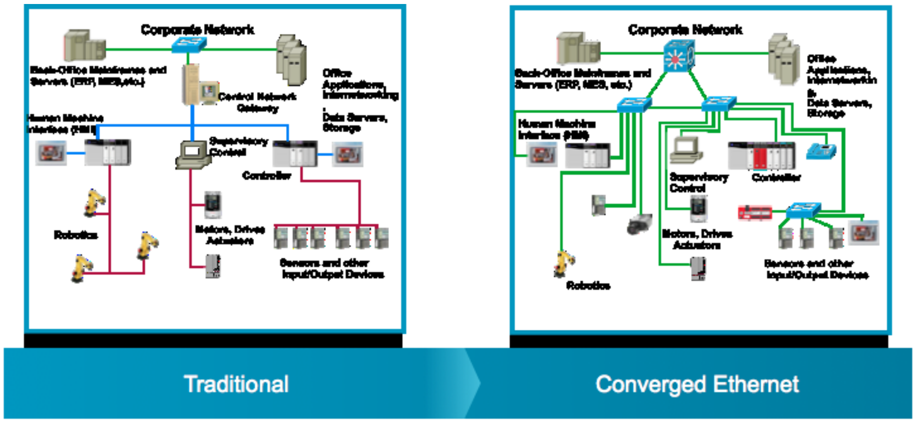
1. Segmentation, for example Virtual LANs (VLANs) for layer 2 and De-Militarized Zones with firewalls
2. Multicast management;
3. Prioritization with QoS
4. Resiliency on a range of network topologies
5. Scalability.

This paper will present the key functions and tenets of these Reference Architectures.

Overview

Industrial Automation and Control Systems, and manufacturing in particular, are going through a technology shift, adopting standard networks for plant and production environments. These standardized network environments are known as *industrial Ethernet* networks. They are shifting away from the numerous industrial-optimized networks typically not connected to the rest of the organization, called *IACS networks*. For the ODVA, this would represent a shift from ControlNet or DeviceNet to EtherNet/IP. This shift is depicted in Figure 1.

Figure 1 Traditional and converged industrial Ethernet environments


Corporate Network
Back-Office Mainframes and Servers (ERP, MES,etc.)
Control Network Gateway
Office Applications, Internetworking, Data Servers, Storage
Human Machine Interface (HMI)
Supervisory Control
Controller
Robotics
Motors, Drives Actuators
Sensors and other Input/Output Devices
Traditional
Corporate Network
Back-Office Mainframes and Servers (ERP, MES, etc.)
Office Applications, Internetworking, Data Servers, Storage
Human Machine Interface (HMI)
Supervisory Control
Controller
Motors, Drives Actuators
Sensors and other Input/Output Devices
Robotics
Converged Ethernet

The key reasons industrial organizations are shifting to converged industrial Ethernet solutions include:

- Ability to globalize operations through integration with Industrial Automation and Control Systems (IACSs) and the enterprise network, thus driving strategic business decisions and providing the ability to use global resources in order to build, maintain, and operate production facilities.

- Lower implementation costs and Total Cost of Ownership (TCO) through the use of standard vs. proprietary networking technologies.

- Improved operational costs and efficiency through ease-of-use features and capabilities of common tools that improve productivity for plant maintenance and engineering personnel.

- Visibility into the IACSs in order to optimize supply-chain management and drive efficient utilization of key production assets.

- Reduced mean-time to repair (MTTR) and increased overall equipment effectiveness (OEE) of production facilities through secure remote access for employees and partners.

- Shortened lead times of deploying new products as communication and collaboration between business decision makers and plant personnel become richer and easier through converged networks.

- Realized productivity improvements as ready-to-deploy collaboration technology (voice-over-IP phones and IP security cameras) become more common in industrial Ethernet networks.

To drive this shift to EtherNet/IP and standard networks, Rockwell Automation and Cisco developed the reference architecture, *Converged Plantwide Ethernet* (CPwE). CPwE is a comprehensive network design that targets industrial Ethernet networks that support hundreds to tens of thousands of Industrial Automation and Control System (IACS) devices. The architecture indicates how to converge industrial Ethernet and enterprise networks and how standard networking supports IACSs and also supports enterprise voice, video and data services. The architecture and concepts were tested with actual IACS applications including a focus on EtherNet/IP devices and applications. The architecture provides recommendations and options designed to meet the particular requirements of a plant environment and IACSs deployed with EtherNet/IP.

This architecture facilitates the convergence of IT and production by highlighting an approach both sides can agree upon. This guide relies on the best practices of Enterprise networking tuned and tailored for IACS applications.

Using this solution's modular approach to building your industrial Ethernet network with tested, interoperable designs allows customers to reduce risks and operational issues and to increase deployment speed.

The Architecture was designed, built, and tested this architecture with the following key features that manufacturers expect:

- **Industrial characteristics**—IACS end-devices and network infrastructure are located in harsh environments in terms of extreme temperature, humidity, vibration, noise, explosiveness, corrosion and electronic interference. Manufacturers often require specialized equipment compliant to a variety of environmental specifications and specific network topologies designed for typical plant layouts.

- **Interconnectivity and interoperability**—The ability to interconnect and interoperate a wide range of IACS devices and applications through a common, standard network infrastructure is a key goal for an industrial Ethernet network. Standard Ethernet and IP network technologies offer the best opportunity to do such, as the barriers for IACS vendors to integrate this into their product is low, and the concepts and technology are widely available. This architectures focuses on the use of standard Ethernet and IP networking technologies and IACS systems based on EtherNet/IP.

- **Real-time communication, determinism, and performance**—Industrial Ethernet networks differ significantly from their IT counterparts in their need to support real-time communications. Messages should be communicated with minimal *latency* (time delay between message sent and message received) and *jitter* (the variance of the latency), and these rates should be significantly lower than typical enterprise applications. Real-time communications help the IACS become more deterministic. The reference architecture takes particular note of EtherNet/IP traffic such as CIP Sync (based on IEEE 1588 Precision Time Protocol), CIP Motion, I/O (a.k.a. implicit traffic) and regular CIP based messages (a.k.a. explicit traffic).

- **Availability**—In plant environments, the cost of outages is measured in $10,000s per minute, based on idle personnel, idle expensive capital assets, wastage, and lost production. The critical IACS equipment that keeps the plant operational is interconnected through the industrial Ethernet network infrastructure. Therefore, network availability is a major requirement. Every major design decision is made by balancing availability with cost considerations. These considerations increase OEE by reducing the impact of a failure, and they lower MTTR by speeding recovery from an outage.

- **Security**—Going hand-in-hand with availability, the ability to avoid outages caused by intentional or unintentional actions is critical. Additionally, the integrity and confidentiality of the information contained in IACS applications and devices is also important. A security approach based on common and standard security guidelines and incorporating plant-specific considerations. The Security guidelines here also match those referred to in the ODVA's Securing EtherNet/IP Networks (PUB00269R0) under Enterprise Connected Industrial Networks.

- **Manageability**—Control engineers and plant maintenance personnel, with varying and limited degrees of industrial Ethernet networking expertise, are likely to have some or all responsibility for the network operations and performance. Therefore, the industrial Ethernet network needs to incorporate features that ease implementation and tailor management for typically lower network competence than found in IT network organizations.

- **Scalability**—Currently, industrial Ethernet networks may contain hundreds to thousands of networked IACS devices. Typically, the number of users may be limited, but the scalability of the network architecture is nonetheless important. This solution considers scalability of the overall network architecture.

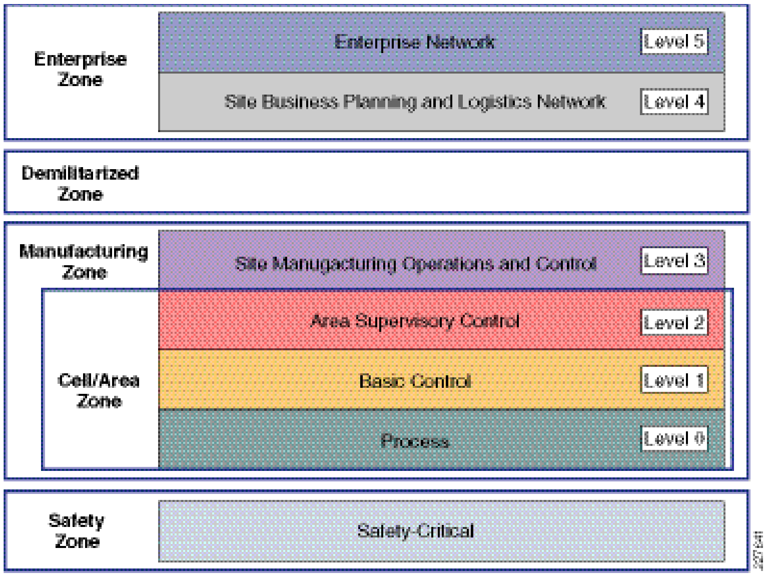
Converged Plant-wide Ethernet

The networking requirements of an IACS network often differ from a typical IT network. This section provides the background and description of an IACS network model and highlights the differences between the Converged Plantwide Ethernet architecture and a typical enterprise network. The significant differences include:

- A demilitarized zone (DMZ) to segment the industrial Ethernet network from the enterprise network.
- Cell/Area zone networks with IACS devices. These networks use different topologies and configurations (for example, quality of service (QoS) and resiliency) than typical Cisco Enterprise networks.

To understand the security and network system requirements of an IACS, this architecture uses a logical framework to describe the basic functions and composition of a manufacturing system. The Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) is a common and well-understood model in the manufacturing industry that segments devices and equipment into hierarchical functions. It has been incorporated into many other models and standards in the industry. Based on this segmentation of the plant technology, the International Society of Automation ISA-99 Committee for Manufacturing and Control Systems Security has identified the levels and logical framework, as shown in Figure 2. Each zone and the related levels are then subsequently described in detail.

Figure 2 Converged industrial Ethernet architecture



This model identifies levels of operations and defines each level. In this architecture *levels* refer to this concept of levels of operations. The *Open Systems Interconnection (OSI) reference model* is also commonly referred to when discussing network architecture, and it refers to layers of network communication functions. Unless specified, *layers* refer to layers of the OSI model.

This guide looks in detail at the various zones and levels of the converged industrial Ethernet network and looks at how they relate to some enterprise-specific concepts of network hierarchy. The three key foundational building blocks of the industrial Ethernet architecture are the Cell/Area zone, the Manufacturing zone, and the Demilitarized zone. All of them are required for a properly functioning, scalable and secure network.

Safety Zone

Historically, safety systems have been hard-wired, dedicated, and segmented from the IACS. The function of the safety system is to provide predictable, fail-safe shutdown of the IACS application in order to protect personnel, the environment, and the IACS application itself, upon the occurrence of a safety event. Safety applications now use standard networks for communication and, under this solution's recommendations, can use the same network.

Cell/Area Zone

The Cell/Area zone is a functional area within a plant facility; most 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. It may be as small as a single controller and its associated devices on a process skid, or it may be multiple controllers on an assembly line. Each plant facility defines the Cell/Area zone demarcation differently and to varying degrees of granularity. For the purposes of this solution, 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 manufacturing process. To control the functional process, they are all in real-time communication with each other.

From an enterprise perspective, the Cell/Area zone is analogous to a Layer-2 access network. The key difference between industrial Ethernet and enterprise networks can be somewhat summarized by the amount of local traffic. In the industrial Ethernet network, 80 - 90% of the Cell/Area zone traffic is local and occurs between IACS devices. In the enterprise network, typically less than 10% or less of the traffic is local. In this zone, the key focus is switching concepts. Most of these are considered Layer-2 functions, but in some cases, the functions utilize information in the IP or Layer-3 portion of the packets.

Network Considerations and Requirement

It is important to consider the Cell/Area zone as a separate entity of the Manufacturing zone. For most industrial applications, the Cell/Area zone is where the primary IACS activities are performed and where most of the EtherNet/IP traffic is passed. This is the network that connects sensors, actuators, drives, controllers and any other IACS devices that need to communicate in real-time. The availability and performance requirements are most distinct in the Cell/Area zone. These requirements are different than those typically found in an IT network. Key networking functions for Cell/Area zones include:

- Segmentation and Virtual Logical Area Networks (VLANs)
- Prioritization and Quality of Service
- Network Resiliency - Resiliency Protocols and Multipath Topologies
- IP Multicast Control and IGMP
- Physical Media—Use of Fiber-Media Uplinks for Fast Convergence
- IP Addressing

Each of these is explored in the subsequent Networking Services section.

Manufacturing Zone

The *Manufacturing zone* is comprised of the Cell/Area zones (Levels 0 to 2) and site-level (Level 3) activities. The Manufacturing zone is important because all the IACS applications, devices, and controllers critical to monitoring and controlling the plant-floor IACS operations are in this zone. To preserve smooth plant-wide operations and functioning of the IACS application and IACS network, this zone requires clear isolation and protection from the Enterprise zone via security devices within the Demilitarized zone (DMZ). This approach permits the Manufacturing zone to function entirely on its own, irrespective of the connectivity status to the higher levels.

From an enterprise perspective, the Manufacturing zone is analogous to the distribution and core networks. These are the networks that interconnect the Cell/Area zone and other Layer-2 networks, such as server environments housing plant applications.

A key function of the Manufacturing zone is to provide the Layer 3 or Routing functions of the Plant network:

- Interconnecting the various Cell/Area zone levels
- Interconnecting the Level 3 site manufacturing systems
- Providing network management and security services to the Level 0 to 3 systems and devices
- Resiliency and availability of the Manufacturing zone network are critical to the Plant operations, but recovery in the same timeframes as the Cell/Area zone that carries the IACS applications is not required

Key Network Services

Segmentation and Virtual LANs (VLANs)

Logical *segmentation* is the process of outlining which endpoints need to be in the same LAN. Segmentation is a key consideration for a Cell/Area zone. Segmentation is important to help manage the real-time communication properties of the network and yet to support the 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 the 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.

In networking terms, the Cell/Area zone is a Layer 2 network. The Cell/Area zone should be a subnet with a defined VLAN. Careful consideration should be considered when designing a Plant network of identifying which IACS devices belong to which Cell/Area zone and minimizing the size of the Cell/Area zone. 250 devices in a single Cell/Area zone is considered a maximum number of devices and we recommend keeping the size below that if possible. See the VLAN section for more detailed considerations.

The key difference or consideration in an industrial Ethernet network is that the VLAN segments should be determined on the grouping of IACS devices that are communicating regularly with each other, usually performing a specific function in the plant. In particular, plant applications may use User Datagram Protocol (UDP) multicast traffic flows between controllers and other IACS devices with a Time-to-Live stamp of 1. This requires that these devices are in the same VLAN or subnet.

The following are logical segmentation and VLAN recommendations:

- Segment the IACS network into Cell/Area zones, where each zone is a subset of devices that communicate consistently with each other. All devices should have an IP address in the same IP subnet and be in the same VLAN. Smaller Cell/Area zones are in general better. It is recommended that Cell/Area zones stay under the Class-C size subnet, therefore less than 250 devices.

- All devices communicating with each other via multicast (I/O) traffic must be in the same VLAN.

- Layer-3 switches or routers are required in order to route traffic between VLANs, which may impact traffic flow.

- Configure the native VLAN to be a dedicated and specific VLAN not already in use (for example as the IACS Cell/Area Zone VLAN). The native VLAN should not be routed to or from, and therefore, it is never enabled on the router or Layer-3 aggregation switch and therefore not reachable outside of network infrastructure devices. The native VLAN is used to carry network control traffic (such as resiliency protocols). No industrial Ethernet traffic should flow in the native VLAN.

- Each VLAN should consist of a single IP subnet.

- If non-manufacturing traffic (PC and so-on) must exist in the physical topology, it should be on a separate VLAN.

- Configure VLAN Trunking Protocol (VTP) mode as transparent in order to avoid operational error because very few VLANs are used.

- Assign all end-device or host ports a VLAN and set to switchport mode access.

- Do not explicitly use VLAN 1, as it is easily misused and can cause unexpected risks.

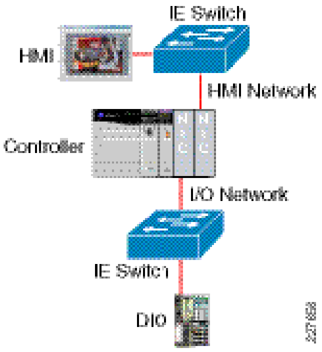
- All uplinks are connected as 802.1Q trunks.

- Use an unused VLAN as the native VLAN on all trunk ports.

- Prune all unused VLANs from a trunk.

There is another topic to consider under segmentation—physical segmentation is a highly common approach in current plant network implementations (as depicted in the diagram below). It is a design habit from historical IACS systems where designers had to use different and incompatible network technologies for various types of communications. For example, a common approach is to physically separate I/O traffic from HMI traffic and not to connect the I/O traffic to any interconnected Layer-3 distribution switch. In these cases, a controller has separate network interface connections (NICs) 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.

Figure 3 Separated I/O and HMI traffic



The effects of this separation include the following:

- Devices on the I/O network are not accessible via non-CIP protocols (such as Simple Network Management Protocol or HTTP), limiting overall interconnectivity
- A controller is not designed to route, switch, or bridge continuous network traffic, and it may introduce delays when used in this manner
- Network-based services (such as security, management, IP address allocation, and so on) must either be replicated in each network or are not available
- Increased costs occur because the available network resources in the HMI network (for example, open ports) are not available in the I/O network

The physical segmentation of traffic in the Cell/Area zone is not necessary (there are other ways described here to achieve that) and leads to difficult-to-manage networks.

Although physical segmentation dedicates network resources to these various traffic types and helps increase the level of certainty that the traffic receives sufficient network resources, it is recommended that these networks be at least connected to Layer-2 or Layer-3 switches so as to enable interconnectivity via other methods than the controller. In this way, the networks stay interconnected and get the full benefits of the converged industrial Ethernet network. Additionally, it is recommended that you consider other ways (for example, application of prioritization and QoS) to ensure that critical network traffic (such as Implicit I/O) receives appropriate network performance.

Prioritization and Quality of Service (QoS)

QoS refers to network control mechanisms that can provide various priorities to network traffic or data flows. In a converged industrial Ethernet network, it is important that the network assign priority to the IACS traffic in order to deliver improved performance for these applications. In setting the QoS configuration recommendations, the following guidelines were used:

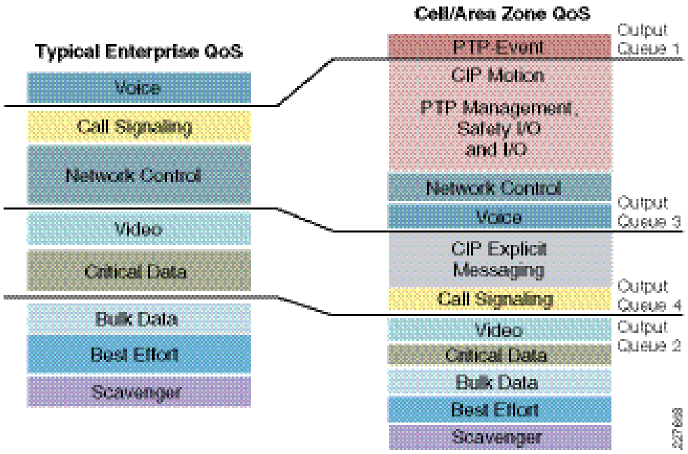
- IACS network traffic should take priority over other applications (for example, web-based voice or video) in the Cell/Area zone.
- IACS network traffic tends to be very sensitive to latency, jitter, and packet loss. The service level for IACS network traffic should minimize these.

- Different types of industrial Ethernet traffic (Motion, I/O, and HMI) have different requirements for latency, packet loss, and jitter. The service policy should differentiate service for these types of flows.

- Non-IACS traffic (voice, video, HTTP, email, etc.) should have little or no effect on the IACS application and therefore be given lower priority than IACS traffic; yet it should maintain the relative importance as found in enterprise networks (for example, network control and voice traffic receive higher priority than application data traffic).

Figure 4 compares the QoS prioritization recommendations for a typical enterprise network to the Cell/Area zone of an industrial Ethernet network.

Figure 4 QoS prioritization recommendations



QoS can be challenging to configure and maintain, but it has significant value to the overall availability and security of the industrial Ethernet. Therefore to implement QoS, we suggest that you:

- Apply the plant QoS configurations embedded in the Cisco Industrial Ethernet switches as startup and port-based macros.

- Ensure that the design is sufficient and use tests in order to verify changes to the QoS configurations.

The macros and QoS configurations reflect the following:

- Use differentiated services code point (DSCP), or *type-of-service*, markings whenever possible, because these are end-to-end, more granular, and more extensible than Layer-2 markings

- Apply the prioritization as highlighted in Figure 4, where critical IACS traffic is given priority in the network

Tech Tip

The application of standard enterprise QoS may negatively impact IACS traffic that uses local DSCPs in order to distinguish that traffic and, by design, may give that traffic lower priority than other types of traffic.

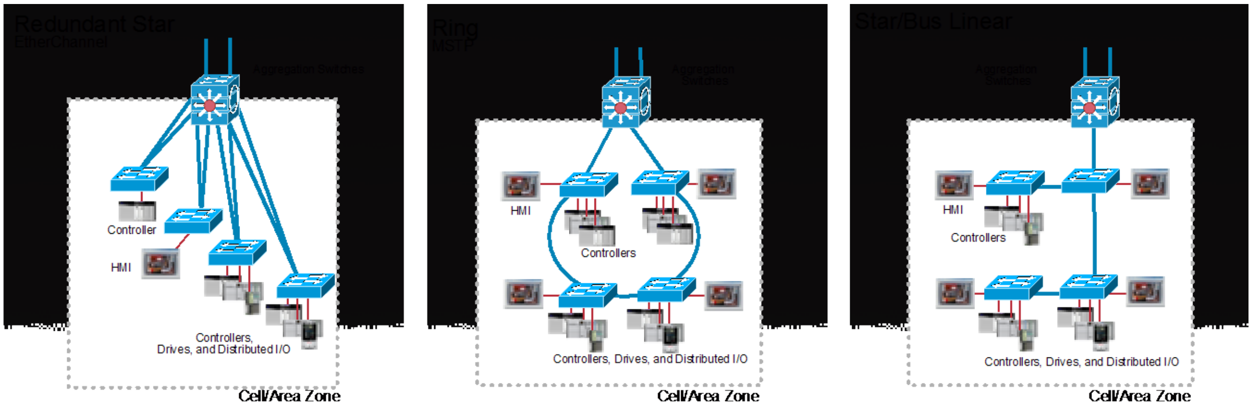
Network Availability—Resiliency Protocols and Multipath Topologies

There are a number of factors that influence the availability of the network, including network design, component selection, and redundancy. This section focuses on the resiliency protocols that allow multiple diverse paths in the network, especially for the Cell/Area zone. These protocols allow multiple paths in the network while preventing network loops. The recommendations that are important to availability are as follows:

- Use a network topology that offers redundant uplink paths in order to allow the network to quickly recover from an uplink failure
- Use redundant network hardware for key network functions, such as the distribution switch

In choosing a multipath topology, common best practices are summarized in the depiction below.

Figure 5 Multipath topology recommendations



	Redundant Star	Ring	Linear
Cabling Requirements	🟥	🟨	🟩
East of Configuration	🟥	🟨	🟩
Implementation Costs	🟥	🟨	🟩
Bandwidth	🟩	🟨	🟥
Redundancy and Convergence	🟩	🟨	🟥
Disruption During Network Upgrade	🟩	🟨	🟥
Readiness for Network Convergence	🟩	🟨	🟥
Overall in Network TCO and Performance	Best	OK	Worst

It is recommended that a redundant star topology is used, but often due to the physical layout of a plant, a ring topology may be more appropriate given the challenges of the cabling infrastructure. The use of a linear, or *daisy-chain*, topology is not recommended, but if they are used, it is recommended that you use Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP).

Redundant Star Topology

If a redundant star topology is used, it is recommended that you use one of the following for resiliency protocols on that topology:

- **Link Aggregation Control Protocol (LACP)**—This protocol is typically used if high bandwidth is required between the access and distribution switches, for example, to carry streaming video or voice communications. LACP typically recovers fast enough (less than 100ms) to ensure key IACS communication is not disrupted.

Ring Topology

The use of ring network topologies for Cell/Area zones is not supported in Enterprise networks, but is a common topology in plant and industrial networks. If a ring topology is selected for network infrastructure, it is recommended that the network infrastructure is configured with RSTP or MSTP in order to manage the loops in the network. In this case though, Spanning Tree variants are not typically able to recover the network in the case of a link-loss or outage fast enough to avoid timeouts in the IACS applications. In the case the ring is of devices with small, dual-port switches, the Device Level Ring ring protocol can be used.

For this reason, there are a wide variety of proprietary technologies that have been developed by switching infrastructure vendors to recover a ring. These typically do recover the ring fast enough

ODVA has developed the Device Level Ring technology that is typically deployed in two-port enabled end-devices. This protocol will recover a ring network of end devices in roughly 1-2 ms, fast enough for most IACS applications, including Motion and Safety.

Linear or Daisy-Chain Topology

The use of linear, or daisy-chain, network infrastructure is not recommended due to the lack of resiliency if any uplinks are lost or disrupted. If such a topology is used though, it is recommended that the network infrastructure is configured with Spanning Tree protocol (RSTP or MSTP) in order to manage any loops that may inadvertently be created during maintenance or changes to the network.

IP Multicast Control and IGMP

Multicast traffic is an important consideration of a Cell/Area zone because it is used by many of the key IACS communication protocols, such as Common Industrial Protocol (CIP). Unmanaged multicast traffic is treated by the network infrastructure as a Layer-2 broadcast; every endpoint on the network receives the message. The load this factor has on end devices increases exponentially as more multicast-producing endpoints are added to the LAN. Internet Group Management Protocol (IGMP) is the standard method to manage multicast traffic. IGMP enables the network infrastructure to understand which endpoints are interested in which multicast data, and thus enables the network infrastructure to forward the messages only to those endpoints that want them. This reduces the amount of traffic the network and endpoints must handle.

The key multicast management recommendation is to enable the IGMP process in the Cell/Area zone. To enable and configure IGMP, it is recommended that you:

- Enable IGMP snooping and querier on all the industrial Ethernet switches as well as the distribution switch or router. Do not change any of the IGMP snooping default settings.

- Configure the IGMP querier on the distribution switch or central to the Cell/Area zone topology. When multiple IGMP queriers are on a VLAN, IGMP calls for the querier with the lowest IP address to take over the querier function. Therefore, the distribution switch should have the lowest IP address in the subnet.

Physical Media—Use of Fiber-Media Uplinks for Fast Convergence

During resiliency testing, we noticed a significant difference in network convergence between topologies with fiber uplinks versus copper uplinks (all using the 1 Gb dual-use ports). This is due to the fact the IEEE specifies that a copper uplink can take up to 750 ms to detect link loss. As availability is a significant concern in industrial Ethernet networks, using fiber-based media for inter-switch uplinks is recommended. Of course, if a linear topology is chosen (not recommended), then the link-loss detection of the uplink media is not a relevant consideration. Copper-based uplinks should be considered.

Fiber-based media often has more resistance to electromagnetic interference than typically found in copper-based media. This is often a significant advantage in plant environments. It has become a best practice to use fiber-based media for inter-switch cabling.

IP Addressing

IP addressing in industrial Ethernet networks tends to be a little different from the deployment found in enterprise networks. Here are some of the differences.

IPv4

IPv4 is prevalent, and the use of IPv6 is very limited and not widely supported in the IACS applications at this time. The ODVA has not yet adopted IPv6.

Private IPv4 Address Range

The IACS network traffic is confined to the Manufacturing zone. Because of this, either private or public IP addresses can be used for the Manufacturing zone. Routable IP addresses are an extremely limited resource. Not all organizations have been assigned routable IP addresses. If an organization has public addresses, they typically have a relatively small number of addresses assigned to them. Using private IP addresses in the Manufacturing zone frees up the public addresses for other purposes. It is important that a unique summarizable block of IP addresses is assigned to the Manufacturing zone.

Static IP Address Schema

IACS devices tend to be installed once and left with little or no additions, changes, or moves during the lifecycle of the system. Therefore, a common practice in IACS applications is to use IP addresses in programs and configurations in order to refer to devices instead of logical references (for example, Domain Name Services). Changing a device's IP address means changing code. In this model, when a device is installed or swapped out, the IP address is given to the new IACS device manually or via a temporary Dynamic Host Configuration Protocol (DHCP) service. The device then maintains that IP address throughout its life unless a major production upgrade occurs.

There are concepts in the IT world to enhance DHCP to deliver a consistent IP address to a device, for example Option 82. The challenge with many of these is to issue IP addresses with the consistency Plant operations require. They are often undermined by unexpected DHCP servers and rely on the DHCP servers consistent operations. Devices with inappropriately issued IP addresses are notoriously difficult to identify and fix.

Lately though, network infrastructure vendors have been deploying DHCP services right into the switches. These can be configured to consistently deploy IP addresses with appropriate configuration. The advantage of such is to ease device replacement where. When a device fails and is replaced, the network issues to the new device the same

IP address to the device when connected to the same port of the failed device. When a device is replaced, specialized expertise is not needed in order to assign the right IP address.

Security

The key security concepts applied in the reference architecture were designed to maintain availability, integrity, and confidentiality of the plant, the IACS applications and the IACS network. 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.

Properly applied security approaches do allow for secure remote access to manufacturing assets, data, and applications, along with the latest collaboration tools, provides manufacturers with the ability to apply the right skills and resources at the right time, independent of their physical location. Manufacturers effectively become free to deploy their internal experts or the skills and resources of trusted partners and service providers, such as Original Equipment Manufacturers (OEMs) and System Integrators (SIs), without needing someone onsite. One of the biggest advantages of deploying standard networks – the ability to remotely monitor and maintain the IACS applications.

The following are recommended:

- **Develop Plant or Manufacturing Security Policies**—Most enterprises have IT Security policies. These policies drive the behavior, processes and awareness of all enterprise network users Plant networks have distinctly different requirements and priorities. Therefore, a specific Plant Security policy should be developed and put into place.

- **Use IT-approved user access and authentication policies and procedures**—Access to enterprise and plant resources and services should be monitored and logged. Every user must be a known entity to the organization and use a unique account. Unfortunately, these are typically based on users entering account and passwords and having certificates available. IACS devices are often not capable of any of these and are therefore not authenticated when connected to the network. Thus the following are important.

- **Strong Physical Security of Network Infrastructure** – Access to Plant network infrastructure should be limited. Switches are typically installed in locked or hard to reach locations. Unused ports are turned off or even blocked. Specific ports for appropriate personnel are clearly marked and authentication policies are applied to them.

- **Endpoint Hardening –** Antivirus applications, regularly deploying security updates and turning of or removing unnecessary applications and services on systems with common operating systems are considered best practices

- **Keep industrial Ethernet protocols at home—**Industrial Ethernet network protocols, such as CIP and others, shall be contained to the Manufacturing zone. These protocols tend not to include enough security considerations, such as encryption or authorization, to be opened to generally available networks. They were designed to run in segmented networks where trust is implicit based on tight physical control of the network.

- **Control the applications**—As a best practice, partners and remote engineers should use versions of IACS applications on controlled application servers when accessing the IACS remotely. This suggests creating remote access servers within the Manufacturing zone, on which the appropriate IACS applications are executed.

- **Don't allow direct traffic**—It is recommended that no direct traffic is permitted between the Enterprise zone (including the Internet) and the Manufacturing zone. The plant firewall acts as a proxy between remote users or applications and target IACS applications in the Manufacturing zone. The firewall also strictly polices the traffic into and out of each zone.

- **Create only one path in or out**—The path from the DMZ through the lower firewall (or firewall instance) into the Manufacturing zone should be the only path in or out of the Manufacturing zone.

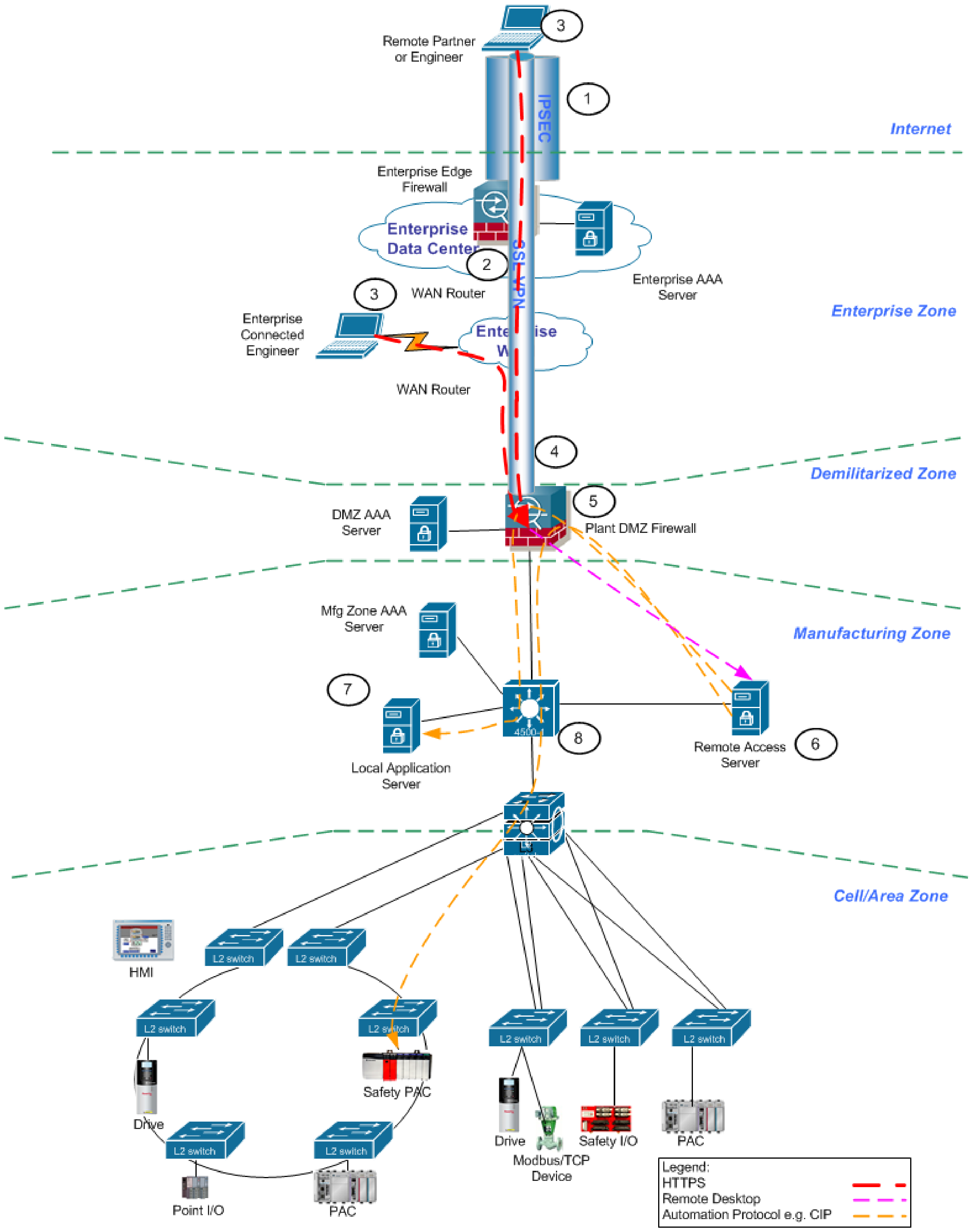
- **Protecting the Interior—**Plant networks tend to be stable. With appropriate assistance, the network can be configured to limit traffic flows through the use of access control lists (ACLs). In addition, there are a host of recommendations to protect the key functions of the network:

- **Domains of Trust—**Users should segment the network into smaller areas (VLANs) based on function or access requirements. These then form the basis on which to manage traffic flows, drastically simplifying application of additional Security functions.

The steps to implement remote access to industrial applications are as follows. Details are depicted in Figure 6.

1. Use standard enterprise remote access solutions in the form of client-based, IPsec encryption VPN technology to connect to the enterprise edge and for confidentiality over the Internet. The establishment of a VPN requires RADIUS authentication of the remote person and is typically implemented and managed by the IT organization.
2. Limit access of remote partners connecting via IPsec to plant floor DMZ/firewalls using ACLs. Connect to the plant floor DMZ through a secure browser Hypertext Transfer Protocol Secure (HTTPS) only.
3. Access a secure browser (HTTPS) portal application running on the DMZ/firewalls. This requires an additional login/authentication.
4. Use a Secure Socket Layer (SSL) VPN session between the remote client and the plant DMZ firewall and restrict application usage to a remote terminal session (e.g. Remote Desktop Protocol) over HTTPS.
5. Utilize intrusion detection and prevention systems (IPSs/IDSs) on the firewall to inspect traffic to and from the remote access server for attacks and threats, and appropriately stop them. This is important to prevent viruses and other security threats from remote machines from traversing the firewall and impacting the remote access server.
6. Allow the remote user to execute, via the terminal session, a selected set of automation and control applications that reside on the remote access server. Application-level login/authentication is required.
7. Implement application security that restricts users from the remote access server to a limited set of application functions (such as read-only, non-line-of-site functions).
8. Segment the remote access server on a separate VLAN and have all traffic between the remote access server and the manufacturing zone go back through the firewall. Apply intrusion protection and detection services to this traffic to protect the manufacturing zone from attacks, worms, and viruses.

Figure 6 Remote Access for Plant Networks



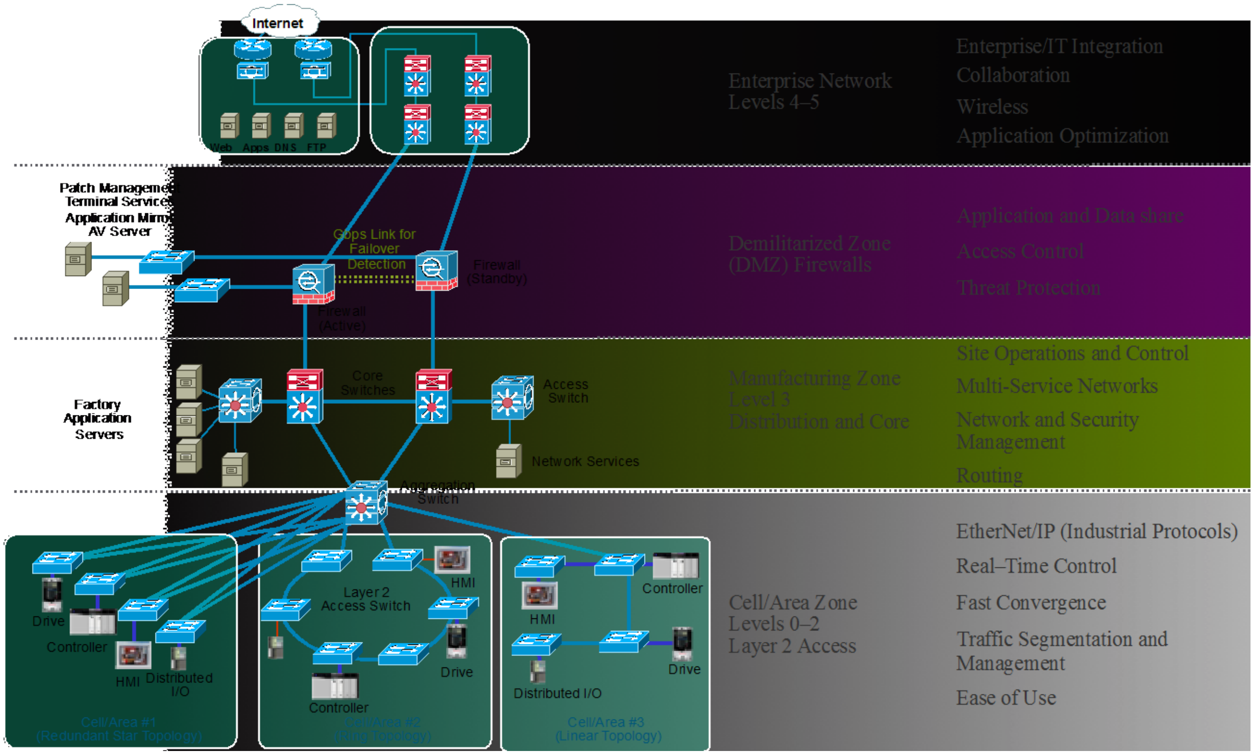
Summary

In many ways, the converged industrial Ethernet network is a replication of the Cisco SBA platform. From a networking perspective, the key two differences are:

- **Layer-2 zones (Cell/Area zones) are different and important**—Topologies, resilience, prioritization, and security are done differently than the Cisco SBA platform, as the devices and applications are distinctly different. Most of an IACS's traffic is local, and when devices are talking to other local devices, network requirements for latency, jitter and recovery vary.
- **Demilitarized zone and firewall**—The applications and devices in an industrial Ethernet network are sensitive and associated with expensive downtime. Therefore, strong segmentation from the IT network in the form of a DMZ and firewall is highly recommended.

The converged industrial Ethernet design consists of zones that that are divided into separate functional levels. Figure 6 summarizes the architecture of the converged industrial Ethernet and the various zone functions.

Figure 7 Converged industrial Ethernet architecture and functions



References

Rockwell Automation and Cisco System: Converged Plantwide Ethernet Design and Implementation Guide.

ODVA: Securing EtherNet/IP Networks (PUB00269R0)

****

The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of CIP Networks and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because CIP Networks may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying CIP Networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use.