SBA

SOLUTIONS

MANUFACTURING

Discrete Manufacturing Design Overview

SMART BUSINESS ARCHITECTURE

February 2013 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

`month year` Series

For example, the series of guides that we released in February 2013 is the "February Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

Table of Contents

What's In This SBA Guide

Cisco SBA Solutions

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

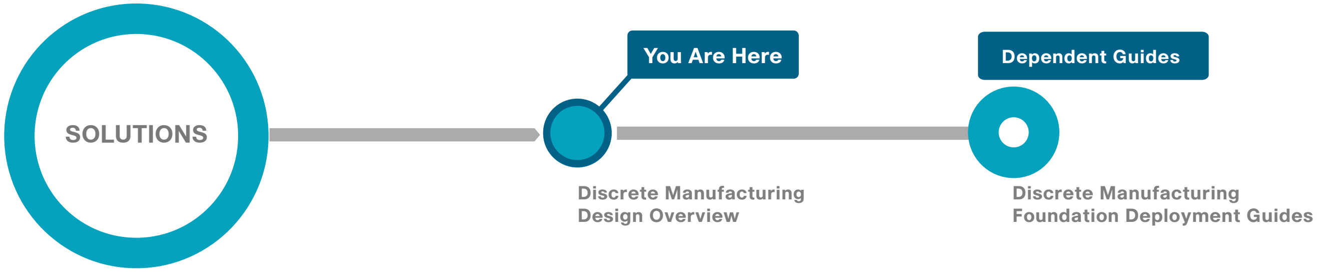
This *design overview* provides the following information:

- An introduction to a Cisco SBA design
- An explanation of the requirements that shaped the design
- A description of the benefits that the design will provide your organization

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel


SOLUTIONS
You Are Here
Discrete Manufacturing Design Overview
Dependent Guides
Discrete Manufacturing Foundation Deployment Guides

Introduction

The *Discrete Manufacturing Design Overview* was developed with both the best practices and expertise of IT networking and Industrial Automation and Control Systems (IACS). This guide integrates guidance from the Cisco Smart Business Architecture (SBA) platform and the Converged Plantwide Ethernet design model. The architecture and concepts herein were tested with actual IACS applications with key partners who supply them, for example, Rockwell Automation. This guide highlights a number of technologies, approaches, and implementation considerations that are targeted for networks in manufacturing production environments (for example, plants and factories). This guide is based on the *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide* and should be considered an evolution of that architecture:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns822/landing_ettf.html

Enterprise is a recognized term in regards to plant and industrial systems. For the purpose of this guide, enterprise refers to an organization's network and systems that are for typical IT uses. The term enterprise does not, in this sense, suggest any scale.

The *Discrete Manufacturing Design Overview* is divided into the following sections:

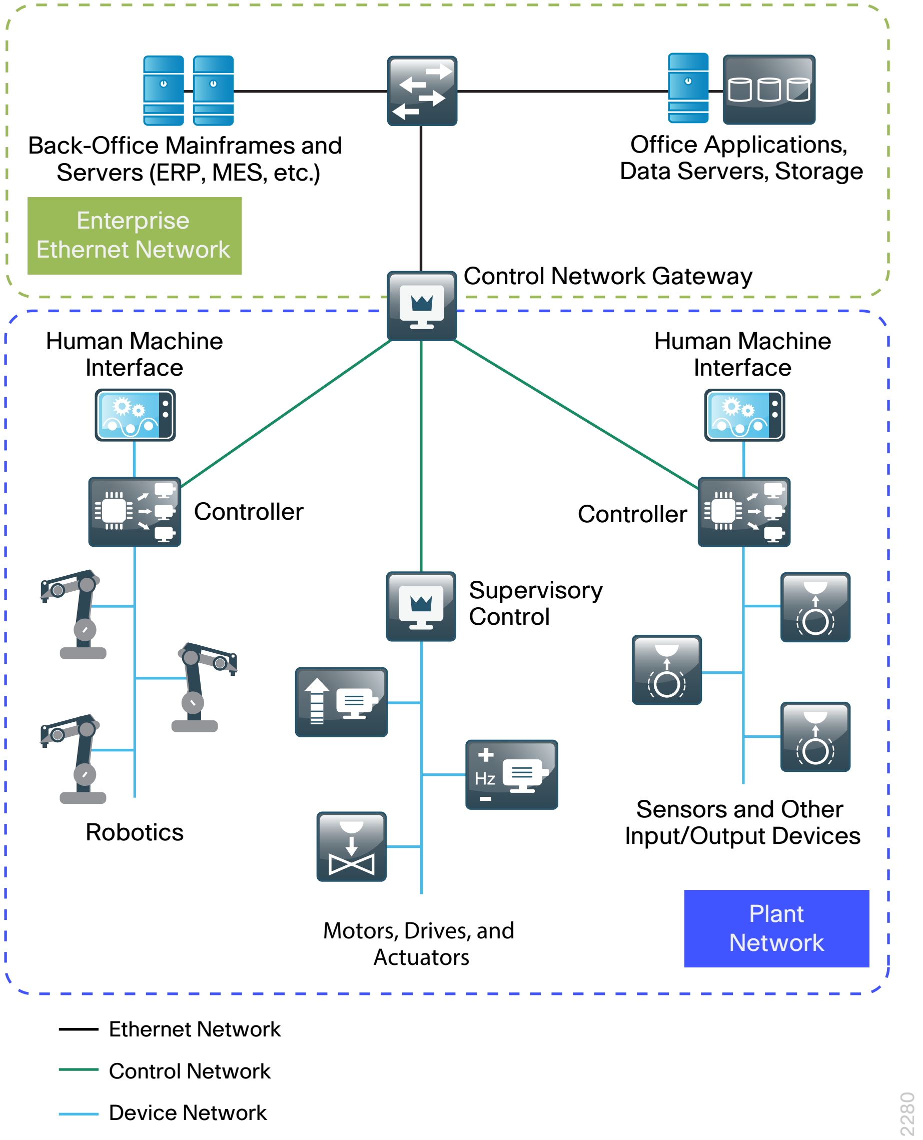
- Introduction—Provides an introduction to plant-specific operations, systems, and network requirements. It also provides an overview of the benefits of integrating the industrial Ethernet network with the enterprise network.
- Converged Industrial Ethernet Network Architecture—Highlights the differences between the converged industrial Ethernet network architecture and a typical enterprise network. It also discusses the routing and switching for the plant floor and lays out the key building blocks of a plant's wired network.
- Network Services—Describes the key differences for network services between a standard Cisco SBA architecture and an industrial Ethernet network.
- User Services—Describes the plant-specific services that are relevant to IACSs. One of the advantages of using a converged industrial Ethernet network is the ability to merge user services, such as voice and video communications, with the industrial Ethernet network.

Business 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*, and manufacturing is using them to replace the numerous industrial-optimized networks, called *IACS networks*, that are typically not connected to the rest of the organization.

As shown in the following figure, even those IACS networks that are in communication with the enterprise network must do so through a proxy or gateway that translates between IACS protocols and IP.

Figure 1 - Traditional, IACS network design


Back-Office Mainframes and Servers (ERP, MES, etc.)
Office Applications, Data Servers, Storage
Enterprise Ethernet Network
Control Network Gateway
Human Machine Interface
Human Machine Interface
Controller
Controller
Supervisory Control
Robotics
Sensors and Other Input/Output Devices
Hz
Motors, Drives, and Actuators
Plant Network
Ethernet Network
Control Network
Device Network
2280

The manufacturing industry faces continuous pressure to improve efficiency and reduce costs. Attaining operational excellence requires you to improve connectivity between plant and business systems, for real-time visibility and effective teamwork. Managing expenses and enhancing communications between operations teams are both critical factors for remaining competitive. You must reduce costly downtime, provide access to experts located thousands of miles away from the plant site, and reduce the need to bring experts on-site for diagnostic troubleshooting or system upgrades.

Traditional IACS networks do not support the flexibility that organizations need in order to control IT expenses and streamline operations. Traditional, proprietary systems create multiple networks in the same space. These networks have separate power, cabling, and communication requirements, and they have multiple sets of spares, skill requirements, and support programs.

Industrial Ethernet technology allows organizations to consolidate all device and control management functions into a single, standards-based infrastructure at a lower cost than multiple, traditional IACS networks. But a well-implemented industrial Ethernet network can do much more than emulate the functions of an IACS network. It allows organizations to integrate their enterprise network with the factory floor in order to enable more efficient operations, and it further enhances factory operations with secure user services based on IP voice and video communications.

Technology Overview

Cisco SBA industrial Ethernet design model for discrete manufacturing offers an architectural approach for controlling the costs of implementing and operating converged industrial Ethernet networks. Cisco SBA is a set of prescriptive guides that help customers design and quickly deploy end-to-end, converged, multiprotocol networks for manufacturing.

Cisco SBA is a tested, validated way to deploy Cisco industrial Ethernet networks with minimal risk. The Cisco SBA platform provides the long-term, extensible framework that supports manufacturing applications and devices as they come and go over the years. A predictable network platform helps customers rely on information technology to optimize manufacturing flows and processes.

This architectural approach offers you benefits such as the following:

- Enhances teamwork with unified communications services that allow plant personnel, IACS vendors, IT staff, and business operations teams to work together more effectively
- Improves the flow of manufacturing information between plant and business systems
- Reduces downtime and mean time to repair (MTTR) by enabling secure remote access for engineers, partners, and IACS equipment vendors in order to perform diagnostics and maintenance
- Reduces implementation costs and improves overall equipment effectiveness (OEE) by replicating validated configurations across multiple plants
- Reduces capital and operating costs with a single network infrastructure that is based on open standards and is relatively easy for skilled personnel to access and manage
- Improves overall security posture and reduces risk of a costly breach or incident

The IT infrastructure of a manufacturing floor is optimized to respond to the information flows and control requirements related to manufacturing processes. The industrial Ethernet network differs significantly from standard enterprise business networks. At the control level, industrial Ethernet networks connect control and monitoring devices such as programmable automation controllers, PC-based controllers, input-output (I/O) racks, drives, and human-machine interfaces (HMI). The device-level network connects these controllers with plant I/O devices with sensors such as transducers, photo eyes, and flow meters, and with automation and motion equipment such as robotics, variable frequency drives, and actuators.

Industrial operations, such as plants, factories, and field systems, are under the domain of plant or factory operational organizations. The systems, including the networks, are predominantly deployed and operated by people with roles such as plant manager, control engineer, or process engineer. The converged Industrial Ethernet architecture facilitates the convergence of IT and industrial operations with an architectural approach that both departments can agree upon. It uses a modular approach to building an industrial Ethernet network with tested, interoperable designs that incorporate concepts and best practices from both IT and plant operations perspectives.

Cisco SBA converged industrial Ethernet for discrete manufacturing is a comprehensive network design model that is optimized for infrastructures that connect thousands of IACS devices. The design model uses IEEE standards-based Cisco industrial Ethernet solutions, which are hardened against the harsh, often extreme environmental conditions of a manufacturing floor. Compared to traditional Ethernet networks in a corporate data network, industrial Ethernet equipment is hardened to endure severe environmental conditions, electromagnetic interference, and power surges. It includes industrial-grade components, convection cooling, and relay output signaling. It is designed to operate at extreme temperatures and withstand vibrations and shocks. Manufacturing often requires compliance with a variety of regulatory and environmental specifications, or non-natively compliant devices require hardened enclosures.

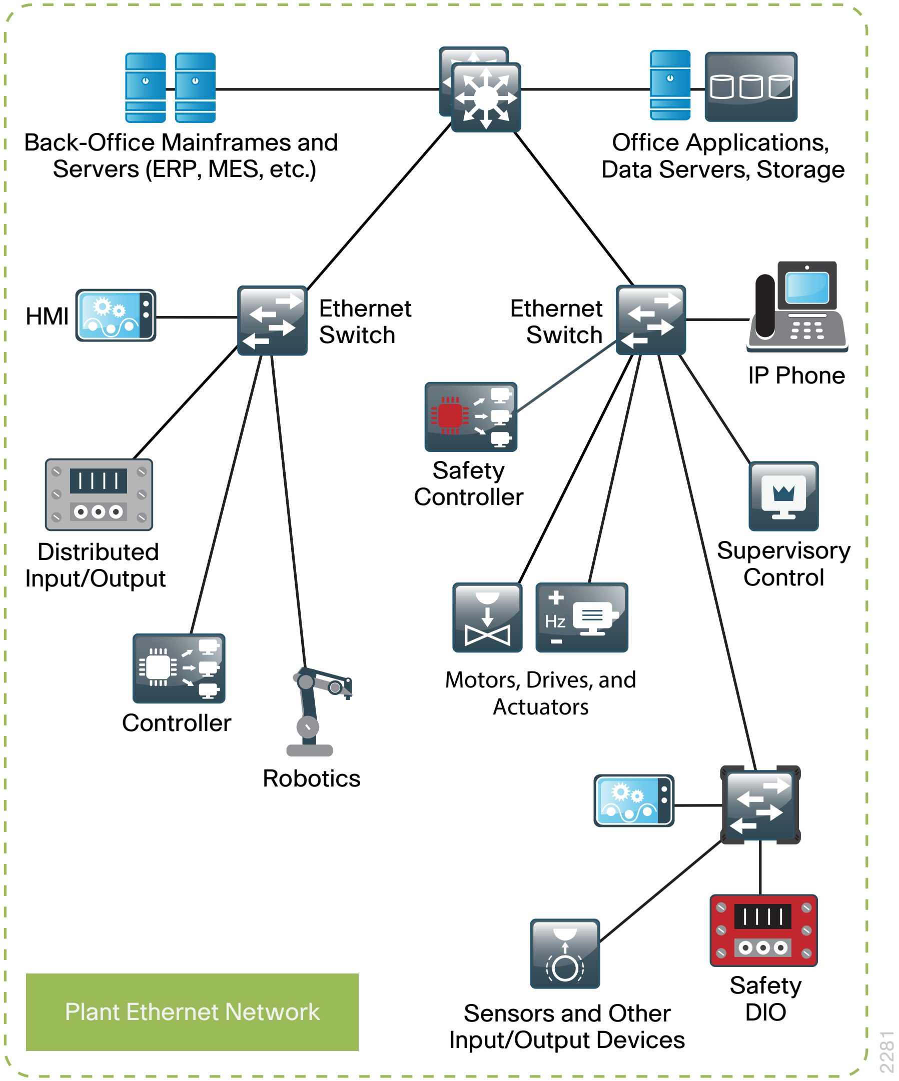
The industrial Ethernet design model balances availability with cost in order to increase OEE, reduce MTTR, and reduce the financial impact of failures. To maximize availability, industrial Ethernet equipment includes fault-tolerant features such as redundant power supplies. Its modular design supports flexible node counts along with copper and fiber wiring in order to accommodate specific requirements of a factory floor. Because power requirements for industrial environments differ from data networks, industrial Ethernet gear operates with 24 volts of DC power.

Industrial Ethernet automation and control protocols and their use of technologies such as unicast and multicast within the standard Ethernet and IP protocol suite often differ significantly from standard Ethernet implementations. Deterministic automation and control systems require real-time, consistent data transmission rates. Therefore, industrial Ethernet must support very predictable real-time data traffic performance.

Both Ethernet technology and the IP protocol suite include technologies and features that support these requirements. To optimize synchronous data access, Cisco solutions for industrial Ethernet include intelligent features such as multicast control with Internet Group Management Protocol (IGMP) snooping, quality of service (QoS), and virtual LANs (VLANs). It also supports other high-availability, security, and management functions to support specific automation and control application requirements.

The *Cisco SBA—Solutions Discrete Manufacturing Design Overview* discusses how to design and deploy an industrial Ethernet network in a discrete manufacturing facility. As shown in the following figure, this design model interconnects IACS devices with each other and with plant operational applications, and it securely integrates industrial Ethernet and enterprise networks.

Figure 2 - Connections within the converged industrial Ethernet design model


Back-Office Mainframes and Servers (ERP, MES, etc.)
Office Applications, Data Servers, Storage
HMI
Ethernet Switch
Ethernet Switch
IP Phone
Safety Controller
Distributed Input/Output
Supervisory Control
Motors, Drives, and Actuators
Hz
Controller
Robotics
Plant Ethernet Network
Sensors and Other Input/Output Devices
Safety DIO
2281

Cisco designed, built, and tested this architecture in order to yield the following capabilities:

- **Industrial characteristics**—Enduring harsh environments is essential to equipment in a manufacturing environment. The network infrastructure must withstand extreme temperature ranges, humidity, vibration, noise, explosiveness, corrosion, impact, ingress protection, and electromagnetic interference.
- **Interconnectivity and interoperability**—Integrating Ethernet and IP networking technologies into a range of IACS equipment facilitates efficient operations. As a standard, Ethernet technology is widely understood, so the barrier to integration is low.
- **Real-time communication, determinism, and performance**—Relaying messages with minimal *latency* (time delay between message sent and message received) and *jitter* (the variance of the latency), with very low tolerance for deviation, improves communication and performance.
- **Availability**—Avoiding outages, which in plant environments can cost tens of thousands of dollars per minute from idle personnel, idle capital assets, waste, and lost production, emphasizes the need for network availability.
- **Security**—Protecting information access, integrity, and confidentiality in industrial Ethernet networks requires multilayer IT security solutions.
- **Manageability**—Simplifying network setup, operation, and performance management allows control engineers and plant maintenance personnel, with varying levels of networking expertise, to carry some or all responsibility for the network's operation and performance.
- **Scalability**—Supporting thousands of IACS devices, the industrial Ethernet network architecture can scale according to an organization's requirements.

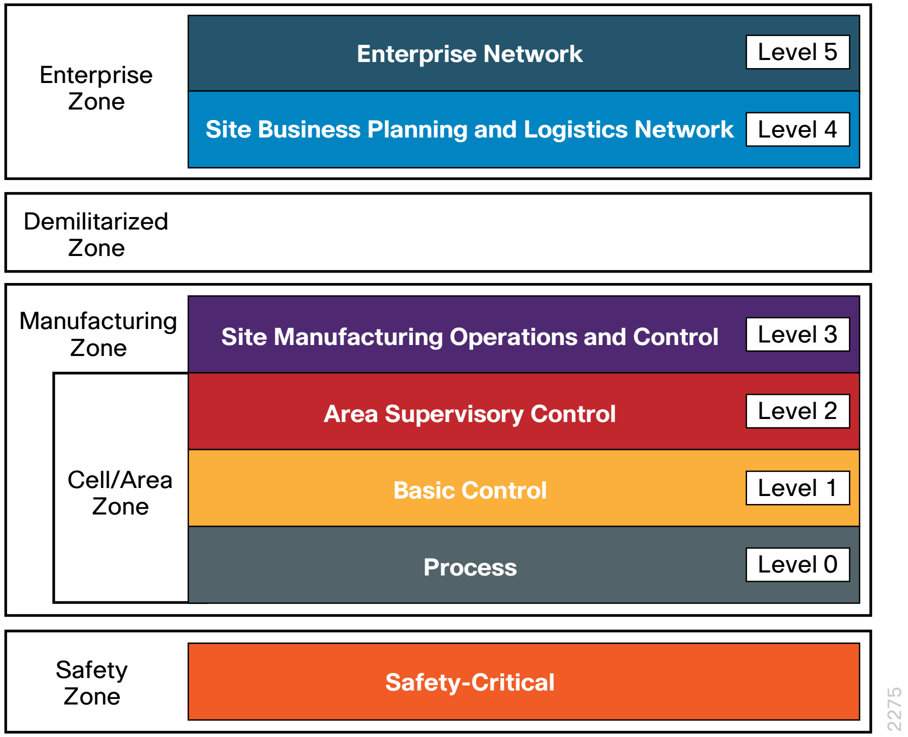
Converged Industrial Ethernet Network Architecture

The networking requirements of an industrial Ethernet network differ from a typical IT network. This section highlights the differences between the converged industrial 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. The DMZ allows traffic from the enterprise network to be filtered before entering the industrial Ethernet network, blocking unwanted users and applications and allowing secure access to the Manufacturing zone.
- A Manufacturing zone containing Cell/Area zones with IACS devices. These networks use different topologies and configurations (for example, quality of service and resiliency) than typical Cisco SBA networks.

To understand the security and network system requirements of an IACS, this solution 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 3. Each zone and the related levels are then subsequently described in detail.

Figure 3 - Converged industrial Ethernet architecture



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

For industrial Ethernet network users, the network is transparent when implemented correctly. Desktops, laptops, and servers intended for use on the industrial Ethernet network have access. Additionally, plant devices connect to the network quickly with minimal configuration. Many industrial Ethernet networks are stable after initial implementation (few devices are added or removed) until the plant or line is retooled or updated. Depending on the device, some configuration may be necessary in order to replace or add new devices. This changes as industrial Ethernet networks begin to deploy standard Wi-Fi-based devices, but it is still the case for the wired side of the network.

This guide looks in detail at the various zones and levels of the converged industrial Ethernet network and relates them to Cisco SBA design 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 separately 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 as part of the Cisco SBA for discrete manufacturing design model, safety applications can use the industrial Ethernet network and can be considered part of the Cell/Area zone.

Cell/Area Zone

The Cell/Area zone is a functional area within a plant facility; most plants have multiple Cell/Area zones. Even though the Cell/Area zone technically exists inside the Manufacturing zone, it can be thought of as a separate entity for design purposes. 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, 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 IT perspective, the Cell/Area zones are analogous to an access network. The key difference between industrial Ethernet networks and enterprise networks is the amount of local traffic that remains on the local VLAN. In the industrial Ethernet network, 80–90% of the Cell/Area zone traffic is local and occurs between IACS devices. Although not typically communicating via Layer 2, much of the traffic is multicast, and this traffic pattern is by design. In the enterprise network, typically less than 10% of the traffic is local. Most clients on access devices communicate with servers in data centers or on the Internet rather than other clients on the same subnet. The Cell/Area zone is changing; what had been treated like Layer 2 in the past really functions at Layer 3 and relies mostly on multicast.

This zone has essentially three levels of activity occurring, as described in the following subsections.

Level 0—Process

Level 0 consists of a wide variety of sensors and actuators involved in the basic manufacturing process. These devices perform the basic functions of the IACS, such as driving a motor, measuring variables, setting an output, and performing key functions such as painting, welding, bending, and so on.

Level 0 devices take direction from and communicate status to the control devices in Level 1 of the logical model. In addition, other IACS devices or applications may need to directly access Level 0 devices in order to perform maintenance or resolve problems on the devices. Once designed and installed, the length of time a device in this level is in place varies depending on the industry. Devices in some manufacturing sectors, such as high-tech industries, may only stay in place for a few months, and others in heavy, discrete manufacturing are not replaced altogether until the plant line is overhauled or replaced, which is typically five or more years.

Level 1—Basic Control

Level 1 consists of controllers that direct and manipulate the manufacturing process, and their key function is to interface with the Level 0 devices (for example, input/output (I/O), sensors, and actuators). Historically in discrete manufacturing, the controller is typically a *programmable logic controller*. In process manufacturing, the controller is referred to as a *distributed control system*. For the purposes of this solution, we use the terms *controller* or *programmable automation controller*, which refer to the multidiscipline controllers used across manufacturing disciplines, such as discrete, continuous process, batch, drive, motion, and safety.

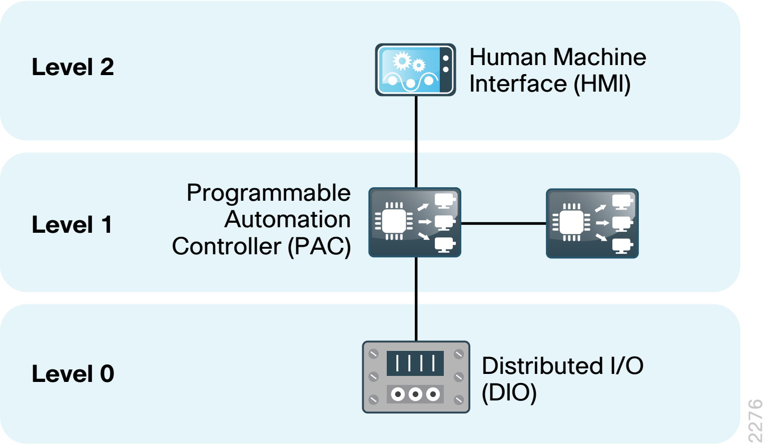
IACS controllers run industry-specific operating systems that are programmed and configured from engineering workstations. Typically, controllers are maintained by an application on a workstation, and the application uploads the controller's program and configuration, updates the program and configuration, and then downloads the program and configuration to the controller.

IACS controllers are the intelligence of the IACS, making the basic decisions based on feedback from the devices found at Level 0. Controllers act alone or in conjunction with other controllers in order to manage the devices and thereby the manufacturing process. Controllers also communicate with other Level 2 and Level 3 functions in the IACS (for example, historian, asset manager, and manufacturing execution system). The controller performs a director function in the Manufacturing zone, translating high-level parameters (for example, recipes) into executable orders, consolidating the I/O traffic from devices, and passing the I/O data on to the upper-level plant-floor functions.

Thus, controllers (as shown in Figure 4) produce industrial Ethernet network traffic in three directions, from a level perspective:

- Downward to the devices in Level 0 that they control and manage
- Peer-to-peer to other controllers in order to manage the IACS for a Cell/Area zone
- Upward to human-machine interfaces (HMIs) and information management systems in Levels 2 and 3

Figure 4 - IACS controller traffic flow


Level 2
Human Machine Interface (HMI)
Level 1
Programmable Automation Controller (PAC)
Level 0
Distributed I/O (DIO)
2276

Level 2—Area Supervisory Control

Level 2 represents the applications and functions associated with the Cell/Area zone runtime supervision and operation. They are often located near or in the same cabinet as the Level 0 and Level 1 devices with which they work. These applications and functions include the following:

- Operator interfaces or HMIs
- Alarms or alerting systems
- Maintenance and control-room workstations

These applications communicate with the controllers in Level 1 and interface or share data with the site-level (Level 3) or enterprise-level (Level 4 and 5) systems and applications through the DMZ. These applications can be implemented on dedicated IACS vendor operator interface terminals or on standard computing equipment and operating systems, such as Microsoft Windows.

As the primary location for IACS activities, Cell/Area zones have industry-specific requirements that are significantly different from a typical enterprise network. For more information about availability, performance, VLAN configuration, industrial protocols, prioritization, and quality of service (QoS) recommendations, see “Network Services” and “User Services” in this guide.

Manufacturing Zone

The *Manufacturing zone* is comprised of the Cell/Area zones (Levels 0 to 2) and site manufacturing operations and control (Level 3) devices and applications. 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 industrial Ethernet network, this zone requires clear isolation and protection from the Enterprise zone via the Demilitarized zone (DMZ). The DMZ is very important part of the defense-in-depth security approach for industrial Ethernet networks. The DMZ permits the Manufacturing zone to function entirely on its own for a period of time, irrespective of the connectivity status to the higher levels.

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

Key functions and features of the network architecture for the Manufacturing zone include the following:

- Interconnecting various Cell/Area zones
- Interconnecting Level 3 site manufacturing operations and control
- Providing network management and security services to Level 0 to 3 systems and devices

Level 3—Site Manufacturing Operations and Control

Level 3, the site level, represents the highest level of the industrial Ethernet. The systems and applications that exist at this level manage plant-wide IACS functions. Levels 0 through 3 are considered critical to site operations. The applications and functions that exist at this level include the following:

- Level 3 industrial Ethernet network equipment
- Reporting and plant historian
- Detailed production scheduling
- Site-level operations management
- Asset and material management
- Control-room workstations
- Patch launch server
- File server and domain services, for example, an Active Directory (AD) deployment separate from the enterprise AD deployment
- Dynamic Host Configuration Protocol (DHCP) and Dynamic Naming Services
- Network Time Protocol
- Terminal server for remote-access support
- Staging area

Systems in Level 3 of the industrial Ethernet network may communicate with Level 1 controllers and Level 0 devices, function as a staging area for changes into the Manufacturing zone, and exchange data with the enterprise (Levels 4 and 5) systems and applications through the DMZ. These applications are primarily based on standard computing equipment and operating systems (Unix-based or Microsoft Windows). For this reason, these systems typically communicate with standard Ethernet and IP networking protocols.

Additionally, because these systems tend to be more aligned with standard IT technologies, they may also be implemented and supported by personnel with IT skill sets. These IT people may belong to the plant or enterprise IT departments.

Demilitarized Zone (DMZ)

Converged industrial Ethernet calls for evolved security policies tailored for industrial networks, which no longer remain isolated. IACS assets have become susceptible to the same security vulnerabilities (for example, denial of service) as their enterprise counterparts. Protecting IACS assets requires a defense-in-depth approach to security that relies on multiple layers of controls in order to improve the availability, confidentiality, and integrity of IACS data.

In the design of the industrial Ethernet network, one of the critical elements is to ensure the separation between the Manufacturing zone and the Enterprise zone. This separation is necessary because real-time availability and security are the critical elements for the traffic in the industrial Ethernet network. The impact of downtime in a plant is much more costly than downtime of similar scale in an enterprise environment. The cost of capital, the loss of product and material, missed schedule, and the wasted time of plant personnel drive this very concrete impact on revenue and efficiency. Therefore, it is recommended that you deploy plant firewalls in order to establish the DMZ between the Manufacturing and Enterprise zones in order to securely manage the traffic flow between these networks.

It is a requirement to share data and services between the Manufacturing and Enterprise zones. Many of the benefits of a converged industrial Ethernet network rely on real-time communication and transfer of data between these zones. Without the security devices in the DMZ, the secure sharing of information from the industrial Ethernet network and the enterprise network is not possible. The DMZ implementation:

- Enforces authentication of users trying to access data or services.
- Strictly controls traffic flow by using IACS-specific security policies.
- Performs stateful packet inspection and intrusion detection and prevention.
- Provides security and network-management support.
- Terminates VPN sessions from external users or from internal users within the enterprise network.
- Provides web-portal services in order to offer proxies services, such as remote desktop, to servers in the Manufacturing zone.
- Secures access to virtual desktop and virtual applications.

The DMZ offers a network on which to place data and services to be shared between the Enterprise and Manufacturing zones. The DMZ enables communication and data sharing between the Manufacturing and Enterprise zones while still keeping devices on either side from having direct access to each other. With the deployment of DMZ firewalls, attacks and issues that arise in one zone cannot easily affect the other zone. In fact, by temporarily disabling the interface connected to the firewall in the DMZ, an IACS or IT network administrator can protect a zone from being attacked, preventing escalation, until the situation is resolved in the compromised zone.

Enterprise Zone

Enterprise refers to the portion of the network represented by the *Cisco SBA—Borderless Networks LAN Deployment Guide*. The industrial Ethernet network is connected to that network via the DMZ. A plant could also have an IT network similar to a Cisco SBA remote site if it is not at the enterprise headquarters location.

Level 4—Site Business Planning and Logistics Network

Level 4 is where the functions and systems that need standard access to services provided by the enterprise network reside. This level is viewed as an extension of the enterprise network. The basic business administration tasks are performed here and rely on standard IT services. These functions and systems include wired and wireless access to enterprise network services such as the following:

- Access to the Internet
- Access to email (hosted in data centers)
- Non-critical plant systems and overall plant reporting, such as inventory and performance
- Access to enterprise applications such as SAP and Oracle (hosted in data centers)

This level is analogous to the Cisco SBA branch. Although important, these services are not viewed as critical to the industrial Ethernet and thus the plant-floor operations. This level is typically under the management and control of the IT department.

Level 5—Enterprise Network

Level 5 is where the centralized IT systems and functions exist. Enterprise resource management, business-to-business, and business-to-customer services typically reside at this level.

The industrial Ethernet network must communicate with the enterprise applications in order to exchange manufacturing and resource data. Direct access to the IACS is typically not required. One exception to this would be remote access for IACS management by employees or partners, such as system integrators and machine builders. Access to data and the industrial Ethernet network must be managed and controlled through the DMZ in order to maintain the security, availability, and stability of the IACS.

The services, systems, and applications at this level are directly managed and operated by the enterprise IT department.

Network Services

This section describes the key services the network provides for proper functioning of the systems and applications that rely upon it. This section considers the following network services that are critical or modified from standard Cisco SBA architectures:

- Network availability—Resiliency protocols and multipath topologies
- Segmentation and virtual LANs (VLANs)
- Prioritization and quality of service (QoS)
- Physical media—Use of fiber-media uplinks for fast convergence
- IP addressing

Although security for an industrial Ethernet network is a very important and a significant consideration, the main difference from a security perspective between the industrial Ethernet and enterprise network is the functionality added by the deployment of the DMZ. The DMZ is where proxy services, virtual desktop interfaces, and VPN and application-specific access secured with an authentication, authorization, and accounting (AAA) service exist, and the DMZ also allows access from the enterprise network to the industrial Ethernet network. Other security functionality found in the Cisco SBA platform is directly applicable in a similar manner as found in the enterprise network.

Network Availability—Resiliency Protocols and Multipath Topologies

The availability of the Cell/Area zone is critical to the manufacturing process. Without a properly functioning Cell/Area zone, some or all of the plant operations may come to a halt. This can severely impact plant efficiency and your bottom line. Availability itself is a function of equipment, infrastructure, configuration, software, etc., and it impacts the network design, topology, and even the type of network infrastructure used.

This section focuses on the resiliency protocols that allow multiple diverse paths in the network, particularly 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 a failure
- Use redundant network hardware for key network functions, such as the distribution layer

There are a number of topologies deployed today in industrial Ethernet networks. Figure 5 and Figure 6 show two very common models. The ring topology and the linear, or *daisy-chained*, topology should be considered legacy models that are no longer recommended. The ring topology introduces a looped topology that relies on Spanning Tree Protocol to recover; it is difficult to troubleshoot problems, and recovery times are too long for manufacturing environments. The linear topology is very simple but lacks resiliency, and any failure requires operator intervention and can cause a production stoppage.

Figure 5 - Ring topology

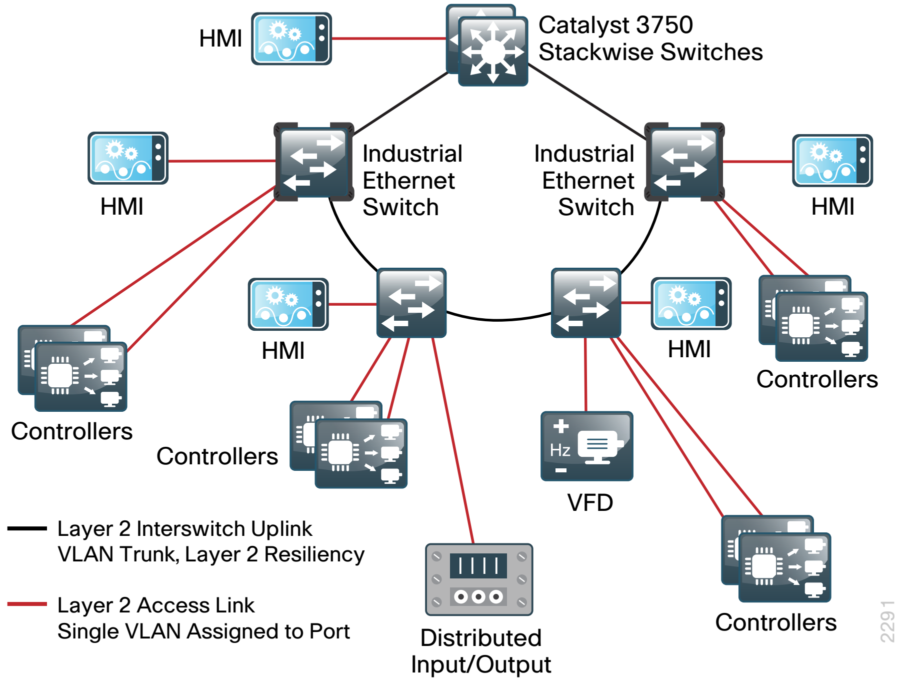
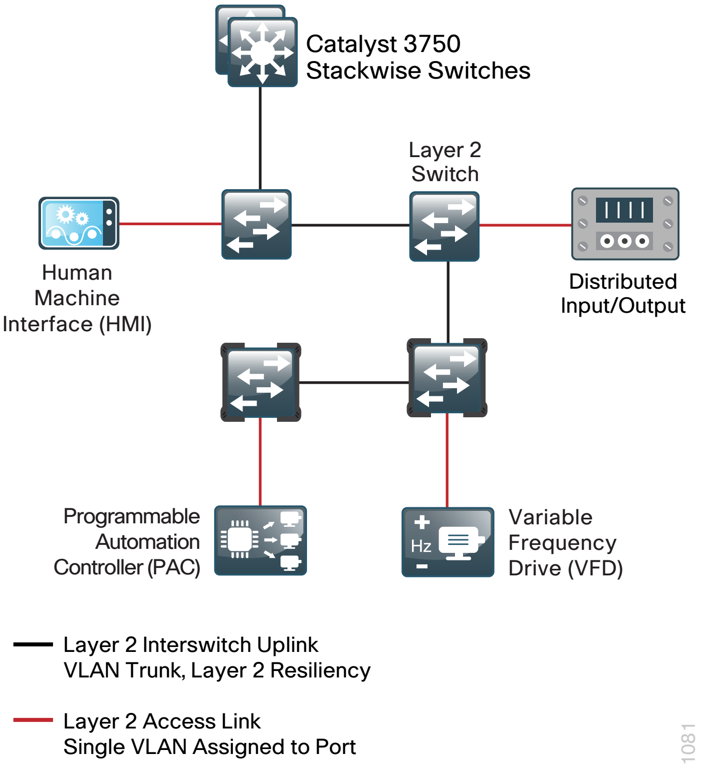


Figure 6 - Daisy-chained topology

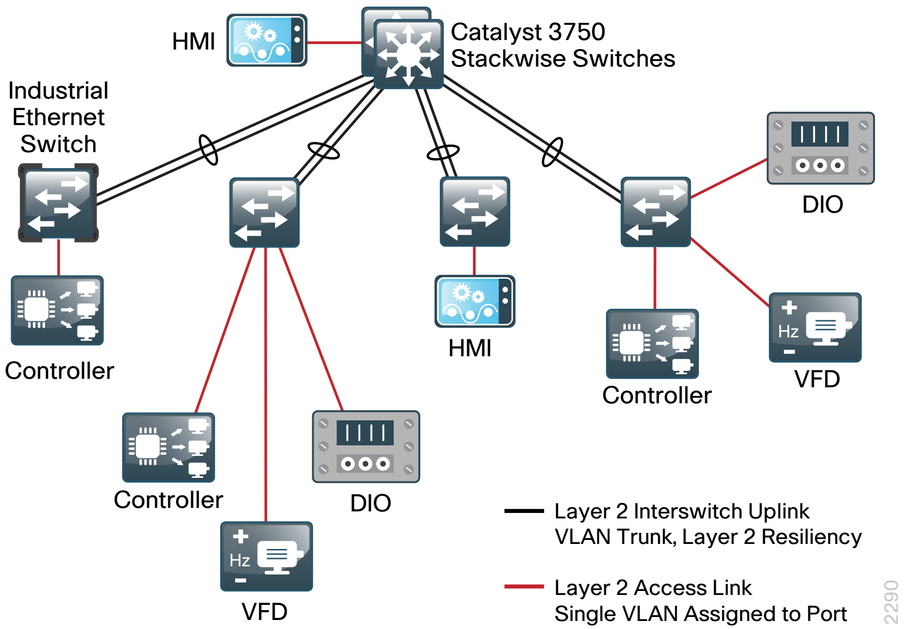


Redundant Star Topology

The redundant star topology (as shown in Figure 7) is the recommended design for a number of reasons. The design has a good level of resiliency and continues to operate in the event of a failure. Recovery from a network hardware or link failure is very fast, minimizing MTTR. If a redundant star topology is used, it is recommended that you use the following resiliency protocols on that topology:

- EtherChannel or Link Aggregation Control Protocol (LACP)—These protocols may be used if high bandwidth is required between the access and distribution switches, for example, to carry streaming video or voice communications. Although a bit slower than FlexLinks, EtherChannel and LACP typically recover fast enough to ensure key IACS communication is not disrupted.
- Virtual Switching System (VSS)—A network system virtualization technology that combines two Cisco Catalyst 6500 Series switches into one virtual switch. VSS allows for simplified management and configuration, improved performance, and faster stateful failover.
- Rapid Per-VLAN Spanning Tree Plus (RPVST+)—An updated implementation of Spanning Tree Protocol that allows you to create one spanning-tree topology for each VLAN and recovers faster than standard Spanning Tree Protocol. Although this design model does not rely on RPVST+ for typical recoveries, RPVST+ is still enabled in order to provide fast recovery in the event of a configuration error.
- Multichassis EtherChannel (MEC)—A Layer 2 multipath technology that creates simplified loop-free topologies, eliminating the dependency on Spanning Tree Protocol and greatly reducing failure recovery times.

Figure 7 - Redundant Star Topology



Segmentation and Virtual LANs (VLANs)

In networking terms, the Cell/Area zone is a Layer 2 network. Each Cell/Area zone should be a subnet with a defined VLAN. Careful consideration should be given when designing an industrial Ethernet network, identifying which IACS devices belong to which Cell/Area zone, and minimizing the size of the Cell/Area zone.

Logical Segmentation

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, and it is important in order to help manage the real-time communication properties of the network and yet to support the requirements 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.

The key difference between an enterprise and an industrial Ethernet network is that the VLAN segments should be provisioned based on the grouping of IACS devices that are communicating regularly with each other, usually performing a specific function in the plant. Simply stated, a Cell/Area zone equals a VLAN which equals a subnet. Some plant applications use User Datagram Protocol (UDP) multicast with a Time-to-Live (TTL) of 1 between controllers and other IACS devices. The TTL of 1 requires that these devices be in the same VLAN in order to communicate. Other plant applications can use multicast for inter-zone I/O and rely on multicast routing in order to communicate between VLANs.

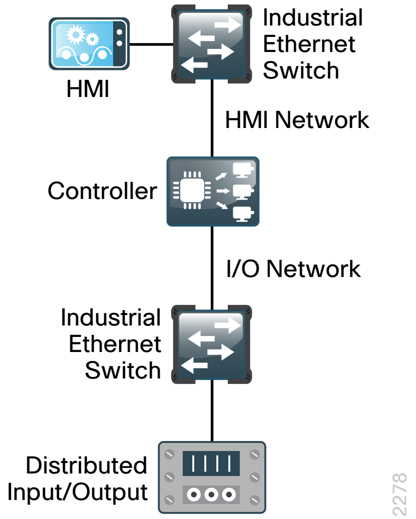
The following are logical segmentation and VLAN recommendations:

- Segment the industrial Ethernet 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, and it is recommended that you use 50 devices or fewer per zone. It is recommended that Cell/Area zones use a /24 size subnet for ease of implementation and contain less than 255 total devices.
- Ensure all devices communicating with each other via Layer 2 multicast that is marked TTL=1 are in the same VLAN.
- Use Layer 3 switches or routers in order to route traffic between VLANs.
- Configure the native VLAN to a VLAN other than VLAN 1 and to a VLAN that is not being used for production traffic.
- Ensure each VLAN consists of a single IP subnet.
- If non-manufacturing traffic (for example, PC traffic) must connect to the same physical topology, use a separate VLAN.
- Configure VLAN Trunking Protocol (VTP) mode to transparent in order to avoid operational error.
- Assign all access ports a VLAN and apply the appropriate template from the *Cisco SBA—Solutions Discrete Manufacturing LAN Deployment Guide*.
- Do not use VLAN 1 for production traffic.
- Connect all uplinks as 802.1Q trunks.
- Prune all unused VLANs from trunks.

Physical Segmentation

There is another topic to consider under segmentation—physical segmentation is a highly common approach in current industrial Ethernet implementations, but in some cases, it has been taken to an extreme. For example, a common approach in current deployments is to physically separate I/O traffic from HMI traffic and not to connect the I/O traffic to an interconnected Layer 3 distribution switch. In these cases, a controller has separate network interface connections 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 Common Industrial Protocol (CIP) traffic.

Figure 8 - 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, and much of the network infrastructure has to be replicated

The physical segmentation of traffic in the Cell/Area zone is not necessary (there are other ways described here to achieve that) and can lead 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)

The Cell/Area zone must be designed to meet the latency and jitter requirements of the IACS it supports. This can impact the size of the LAN, the number of routing hops, the VLAN configuration, and a number of other network parameters. Therefore, recommendations are included for prioritization and quality of service (QoS) that are significantly different from enterprise deployments.

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, use the following guidelines:

- Network traffic originating from IACS devices should take priority over other data-plane applications (for example, web, voice, or video) in the Cell/Area zone.
- Network traffic originating from IACS devices that is very sensitive to latency, jitter, and packet loss should be put into the priority queue. 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 should maintain the relative importance as found in enterprise networks (for example, network control and voice traffic receive higher priority than application data traffic).

Table 1 compares the QoS prioritization recommendations for a typical enterprise network to the Cell/Area zone of an industrial Ethernet network.

Table 1 - QoS prioritization recommendations

Typical enterprise QoS	Cell/Area zone QoS	Output queue
Voice	Precision Time Protocol (PTP) event	1
Call signaling Network control	CIP motion PTP management, safety I/O, and I/O Network control Voice	3
Video Critical data	CIP explicit messaging Call signaling	4
Bulk data Best effort Scavenger	Video Critical data Bulk data Best effort Scavenger	2

QoS can be challenging to configure and maintain, but the template, platform-specific approach in the Cisco SBA—Solutions Discrete Manufacturing deployment guides makes it much easier and adds significant value to the overall availability and reliability of the data transmission on the industrial Ethernet network. Therefore to implement QoS, it is recommended that you:

- Apply the plant QoS configurations described in the Cisco SBA—Solutions Discrete Manufacturing deployment guides.
- If changes are made to the Cisco SBA templates, verify the configuration in a lab in order to ensure it operates as expected prior to deployment in production.

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 Table 1, 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 and, by design, may give that traffic lower priority than other types of traffic.

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 every message. The load this has on end devices increases linearly 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 it 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. This is a fundamental driver for intelligent switches in the Cell/Area zone rather than unmanaged networking devices. Intelligent switches allow you to see and manage this traffic at a Layer 2 level.

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 (this is on by default).
- 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, statically defined.
- Protocol Independent Multicast (PIM) sparse mode builds unidirectional shared trees that are rooted at a rendezvous point (RP) per group, and it scales well, even in WAN environments. This should be configured on all Layer 3 interfaces in order to control multicast traffic.
- Anycast RP provides load-sharing and redundancy in PIM sparse mode networks. This is the recommended configuration for the Layer 3 switches at the distribution layer.

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. This is due to the fact the IEEE allows a copper uplink to 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.

Fiber-based media has more resistance to electromagnetic interference than copper-based media. This is often a significant advantage in plant environments.

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 last blocks of public IPv4 address have be allocated to the Regional Internet Registries (RIRs), and they have either allocated it or are in the process of doing so at this time. At this time, IPv4 is still the most commonly deployed address space and will remain so for some time inside of organizations with the use of Network Address Translation (NAT) and newer IPv4-to-IPv6 translation techniques. IPv4 is used for the deployment currently.

IPv4 Address Range Selection

The IACS traffic is typically confined to the Manufacturing zone. Because of this, either public IP or private RFC 1918 addresses can be used in the Manufacturing zone. Public IP addresses are an extremely limited resource, and not all organizations have assigned public IP address space. If an organization has public IPv4 addresses, they are typically used in the Internet edge for public-facing services, and the organization uses private IPv4 space for internal networks. For ease of use and to simplify security policies, it is recommended that for the Manufacturing zone, use a private contiguous block of addresses that is not in use in the enterprise network. If that is not possible, features are available, such as NAT, that can be used in the DMZ in order to address any legacy issues.

Reader Tip

For more information on IPv4 and IPv6 addressing design, please refer to the following:

Cisco SBA—Borderless Networks IPv4 Addressing Guide
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_IPv4AddressingGuide-Feb2013.pdf

Cisco SBA—Borderless Networks IPv6 Addressing Guide
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_IPv6AddressingGuide-Feb2013.pdf

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 using 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 DHCP service. The device then maintains that IP address throughout its life unless a major production upgrade occurs.

Another option enabled by Cisco switching infrastructure is to use a persistent DHCP option where the switch (and only the switch) to which the IACS device is connected gives the device an IP address assigned to that port and blocks DHCP replies from any other source. This solution supports the static IP address model prevalent in the IACS applications but eases the replacement of any IACS device. When a device is replaced, specialized expertise is not needed in order to assign the right IP address. Once a device has an IP address, the IACS can automatically deploy any configurations or updates required.

Notes

User Services

The focus of the Cisco SBA discrete manufacturing design model is the deployment of networks for Industrial Automation and Control Systems in production environments. As such, IACSs have limited “user” concepts as most of their traffic is between the automation devices themselves. You can deploy networks in such a way as to enable the voice, video, communication, and collaboration services of typical enterprise deployments, albeit with priority given to the IACS applications. The true advantage of relying on a converged industrial Ethernet network is the ability to merge all of the enterprise user services with the critical IACS.

This section describes the plant-specific or factory-specific services that are relevant in particular for the IACS. This section describes the following:

- Industrial protocols used by the IACS
- IACS applications, including:
  - Information
  - Input/Output (I/O)
  - Safety
  - Schedule of Events and Precision Time
  - Motion
  - Call home
  - Statistics, maintenance information, and diagnostics
- Secure remote access

As mentioned earlier, the main difference between the industrial Ethernet and enterprise networks is the IACSs. Although these systems do have users and the user services from the general Cisco SBA guidance are applicable, the IACSs do have specific application or network traffic types that, in many ways, have differing network requirements and can be considered as user services. This section focuses on those user services that are different in this part of the network.

Industrial Protocols

As mentioned in the Introduction, IACSs are going through a technology shift towards industrial Ethernet networks. The IACS protocols, considered Layer 7 user applications, are a big part of that shift. The IACS protocols enable the IACS end devices to communicate and function in a standard manner. These IACS protocols have historically been based on proprietary, closed network technologies optimized for a very specific function. Examples of such include ControlNet, DeviceNet, Serial Real-time Communications System (SERCOS), Highway Addressable Remote Transducer (HART), Foundation Fieldbus, Modbus, and Profibus.

These protocols are migrating or adopting standard network technologies. Many now have variants that are based wholly or partially on open, standard network protocols (Ethernet, IP, TCP, and UDP). For example, Modbus has Modbus/TCP, Profibus has Profinet, and SERCOS has SERCOS III. The Open Device Vendor Association (ODVA), an industrial protocol standards organization, has focused the Common Industrial Protocol (CIP) to function on standard network technologies such as Ethernet, IP, TCP, and UDP. This variant is known as *EtherNet/IP*, where *IP* stands for Industrial Protocol.

In so far as an industrial protocol is based on standard network technologies, this design overview can be used as a guide for the network implementation. Some of these protocols have adopted non-standard, closed networking concepts and technologies that are not supported by this guide. For example, Profinet has an Isochronous Real-Time (IRT) application that incorporates non-standard communication and cannot run on standard network infrastructure. Many Profinet applications do not use this service and can indeed operate on a standard network infrastructure.

IACS Applications and Traffic Types

For most industrial applications, the Cell/Area zone is where the primary IACS activities are performed, and the availability and performance requirements are distinct from the requirements in a typical IT network. This is the zone that connects sensors, actuators, drives, controllers, and any other IACS devices that need to communicate in real-time.

Table 2 - Typical applications and their level in the network

Level	Application
Level 4—Site Business Planning and Logistics Network	Manufacturing execution system—Measures and controls production facilities; it tracks and measures key operational criteria such as product, equipment, labor, inventory, defects, etc.; a key interface to the enterprise-level applications
Level 3—Site Manufacturing Operations and Control	Historian—Collects historical data from the factory floor applications and reports or displays the data in various report formats
Level 3—Site Manufacturing Operations and Control	Supervisory control and data acquisition—Manages large-scale distributed measurement and control systems, usually covering a geographical area
Level 2—Area Supervisory Control Level 1—Basic Control	Programmable automation controller—Controls a subset (cell/area) of manufacturing, for example, a line or function, as well as the relevant devices in that cell/area
Level 1—Basic Control	Human-machine interfaces (HMIs)—Displays operational status to manufacturing personnel and may allow them to perform basic functions (for example, start or stop a process)
Level 0—Process	Input/Output (I/O) device—Measures or controls key functions or aspects of the manufacturing process

IACS protocols support a variety of applications types with a varying degree of network requirements. The ODVA has a good example of the type of applications supported.

In addition to supporting the IACS protocol traffic, increasingly, the network infrastructure is critical because IACS devices are communicating directly via these protocols. Support for these protocols is a network requirement in plant environments.

The application types are described below, and Table 3 summarizes their network requirements.

Table 3 - Network requirements by application type

Requirement class	Typical cycle time	Typical request packet interval (RPI)	Connection timeout	Target network convergence
Information or process (for example, HMI)	<1 s	100-250 ms	Product dependent For example, 20 seconds for RSLinx	<1 sec
Time critical processes (for example, I/O)	30-50 ms	20 ms	4 intervals of RPI, default=100 ms	<100 ms
Safety	10-30 ms	10 ms	24–1000 ms	<24 ms
Motion	500 µs-5 ms	50 µs-1 ms	4 intervals	<1 ms

Information

Information services are used in order to allow the IACS to talk to users of the application and other plant applications, such as historians, asset management systems, and manufacturing execution systems.

Although this type of traffic may be important to the operational functioning of the plant, it tends not to be involved in the closed-loop control cycles based on short time intervals. Information traffic often uses the less deterministic, although reliable, features found in TCP. Information packets may also be larger and communicated in bursts upon events that may occur.

Control and I/O

At its most basic, an IACS has a controller that aggregates inputs from the IACS devices, and the controller runs a variety of control loops that produce outputs for those IACS devices. This I/O function usually entails the regular and scheduled sending of data between IACS devices and a controller. This I/O data is typically small packets (approx. 64 bytes) of information sent via UDP unicast or multicast mechanisms.

Safety

Safety applications are usually a network of separate IACS devices designed to manage the safety of the IACS application. For example, when someone enters a zone where robots are operational, this system should detect the intrusion and put the system in a safe state.

There is a range of safety certifications and standards, most of which apply to the overall system rather than to parts of the systems, such as the network infrastructure. The safety certifications are not covered in this guide.

Sequence of Events and Precision Time

The idea of precise clock synchronization is a powerful concept for Industrial Automation and Control Systems. If all the IACS devices have precise clocks that are tightly synchronized, it is possible to maintain a precise Schedule of Events (SOE). SOE enables the control engineers to precisely understand the events that led to a failure or outage and enables the ability to schedule actions.

The clocks in this SOE concept are synchronized via a network service based upon the Precision Time Protocol (PTP) found in the IEEE 1588 standard. This protocol allows a network-based Grand Master to pass time to the IACS devices in a precise manner. In this concept, the network infrastructure plays a critical role as the messages are passed throughout the network. It is possible to implement a system where all the device clocks are synchronized to within 100 nanoseconds, enabling a very precise SOE.

Motion

Motion in IACSs refers to the ability to control fast-moving systems with precision. The systems may be moving paper very quickly under printing machines or finely controlling the application of paint on an object. Often, it includes tight synchronization of tens or hundreds of drives or axes.

Motion applications are some of the most challenging from a networking perspective. The control applications have some of the tightest control loops found in a plant or factory applications. The control loops may be running in hundreds of microseconds and keeping drives synchronized within microseconds.

Often, these are the applications for which some control protocols have varied from the standard networking protocols in order to optimize the network for latency and jitter. The ODVA's EtherNet/IP has incorporated IEEE 1588 precision time protocol (PTP) in order to achieve these levels of precision and remain based on standard network protocols. In these configurations, the network infrastructure must be capable of delivering the precise time to all the IACS devices involved in the motion control.

Remote Access

The latest collaboration tools and secure remote access to manufacturing assets, data, and applications provides you with the ability to apply the right skills and resources at the right time, independent of their physical location. You effectively become free to deploy internal experts or the skills and resources of trusted partners and service providers, such as original equipment manufacturers and system integrators, without needing someone onsite.

To deploy secure remote access, the following are recommended:

- **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.
- **Keep industrial Ethernet protocols at home**—Industrial Ethernet network protocols, such as CIP, Profinet, OPC-DA, Modbus TCP, 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 and executing the appropriate IACS applications on the remote access servers.
- **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.

Notes

Summary

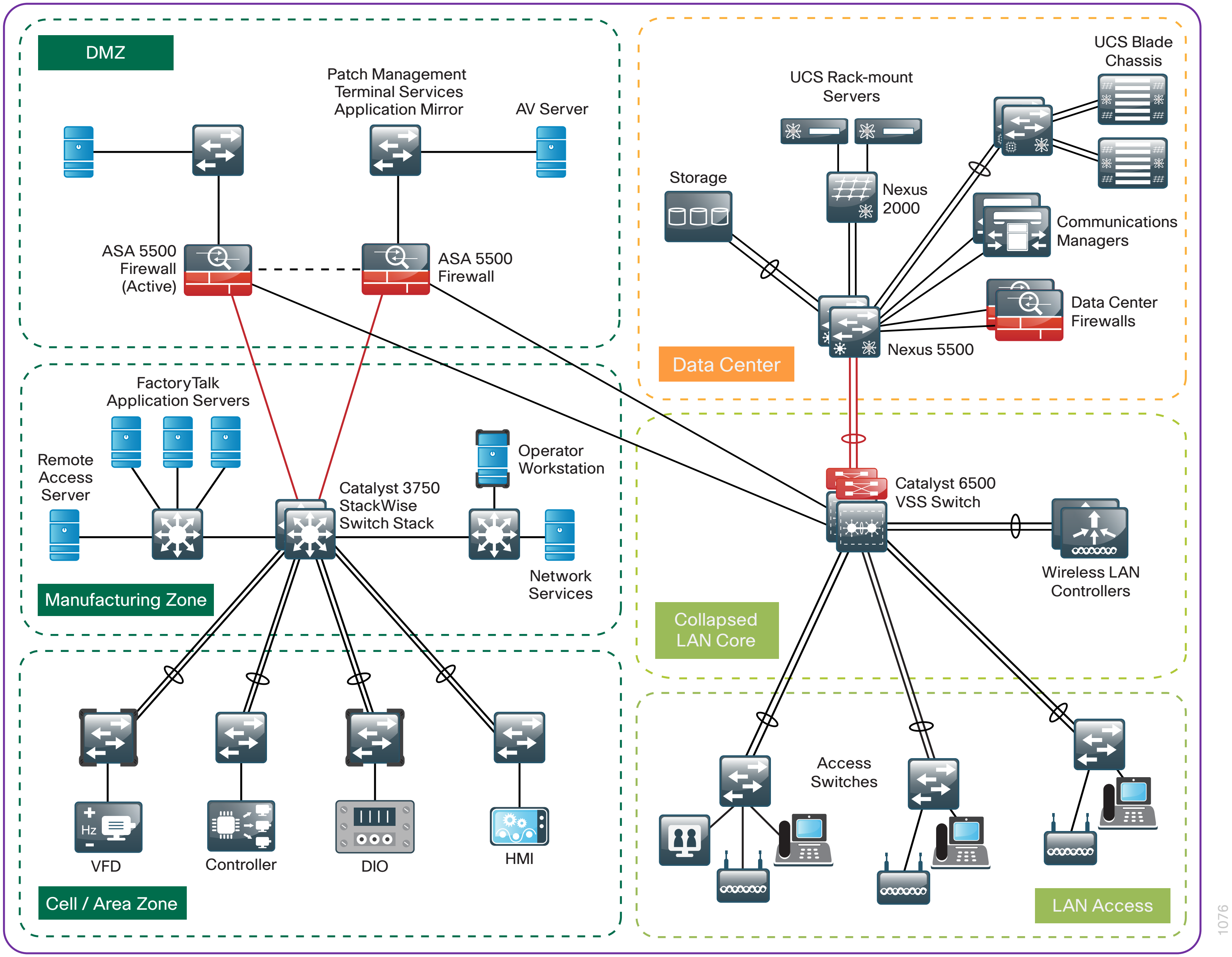
In many ways, the converged industrial Ethernet network is a replication of the Cisco SBA platform. From a networking perspective, the key two differences are:

- **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**—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, is highly recommended.

The converged industrial Ethernet design model consists of zones that that are divided into separate functional levels. Figure 9 summarizes the architecture of the converged industrial Ethernet network.

Notes

Figure 9 - Converged industrial Ethernet network architecture



By combining the recommendations in this guide with the approach from the general Cisco SBA guides, you can successfully deploy industrial Ethernet networks in plant and operational environments, thereby receiving the wealth of value from lower costs, higher OEE and productivity, and the ability to deploy innovative solutions (for example, voice, video, and collaboration).

Notes

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLiERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.