CHAPTER 1

Ethernet-to-the-Factory Solution Overview

Executive Summary

This design and implementation guide represents a collaborative development effort from Cisco Systems and Rockwell Automation. It is built on, and adds to, design guidelines from the Cisco Ethernet-to-the-Factory solution and the Rockwell Automation Integrated Architecture™.

Faced with internal pressures to cut costs and external demands for better products and services, manufacturers are realizing the benefits of a converged network, such as the following:

- Greater visibility
- Better data integration
- Shorter lead times
- Increased turnaround
- Reduced costs
- Simplified management

The key targets are industrial automation and control systems, which benefit greatly from the transition to modern networking technologies from the factory-optimized networks typically in use today. New services and streamlined efficiency result when the information contained within these automation and control systems is available and shared throughout the larger enterprise. Access to existing production information is presently gated by disparate, proprietary, and closed systems. Manufacturers and their industrial suppliers are discovering that standard communication and uniform networking of industrial systems is the key to optimized services, greater visibility, and lower total cost of ownership (TCO). They are starting to embrace standard information technology, particularly Ethernet and IP, for industrial automation and control environments.

Although most manufacturers recognize that Ethernet and the IP protocol suite will be the de-facto networking standard in manufacturing environments in the near future, only a few have fully adopted standards-based Ethernet network architectures for industrial automation. Much of this resistance can be attributed to the aversion to disrupting existing systems, the accounting realities of fully-depreciated assets, and the general ebb and flow of production investment cycles. Resistance to migration also comes from the market being serviced by small niche vendors with narrowly-designed products or limited support capabilities. As bigger players start to enter the market and create an industry-wide industrial networking standards organization, the market is poised to explode.

Cisco and Rockwell Automation believe standard networking technology offers value inside industrial operations when the technology is part of larger integrated, industrial automation architectures. Cisco calls this the Ethernet-to-the-Factory (EttF) Architecture. Rockwell Automation calls this *Integrated Architecture*.

The purpose of this architecture is to accelerate the convergence of standard networking technologies with the industrial automation and control environment. This solution architecture and relevant design and implementation guidelines will give customers, partners, and the marketplace the confidence and background necessary to employ EttF. This solution architecture must be tailored to support automation and control systems. By adopting the solution architecture, the manufacturing process will have to operate at higher levels of performance, efficiency, and uptime as under the previous solutions. At the same time, it must also safely and securely integrate these systems into the broader manufacturing environment; only at this point will all the benefits be available to the manufacturing enterprise.

Introduction

Cisco EttF 1.1 Solution—Description and Justification

The industrial manufacturing environment of today is very similar to the IBM legacy mainframe environments of the mid 1990s. Although these legacy industrial systems are functional, they are costly to maintain, difficult to connect, and slow to evolve. With their factory floor-optimized protocols, specific operating requirements, and separate staffs, manufacturers are also struggling to evolve. Whether their industrial automation and control systems are discrete, process, batch, or hybrid, manufacturers need their systems to interact in real-time with the other enterprise applications, supply chain partners, and end customers. To accomplish this, manufacturers are bringing their industrial automation systems online. When doing this, manufacturers encounter a number of challenges, such as the following:

- Production reliability—As manufacturing operations become globally integrated, manufacturers are challenged to provide consistent access to data while making the manufacturing environment programmable and flexible. Security, availability, and asset use are critically important to manufacturing companies because industrial automation and control equipment is mission-critical, and efficiency is important to remain competitive.
- Cost—Legacy industrial automation and control systems, although often fully depreciated in existing manufacturing environments, can be difficult to bring online and can require significant investment.
- Product design integration—Data silos and closed systems hinder the ability to reduce time to market for new products.
- Service integration—In an effort to provide differentiated service, manufacturers are struggling to create systems to capture and incorporate data from their products that are in operation.
- Data interaction and management—Incorporating real-time factory productivity and operational data into manufacturing execution systems (MES), customer relationship management (CRM), supply chain management (SCM), and other enterprise resource planning (ERP) systems is an increasingly complex data translation exercise.
- Partner connections—With an aging and decreasing workforce and increased production complexity, manufacturers are trying to find ways to leverage relationships with industrial automation and control vendors to support their factory floor systems.

These challenges are pushing manufacturers to adopt standard Ethernet and IP technologies throughout the manufacturing environment. By moving to standard technologies, manufacturers can:

- Realize significant cost savings—Standard Ethernet and IP technology has greater market penetration and thus is more likely than existing factory floor networking technologies to give manufacturers a significantly lower total cost of ownership (TCO).

- Provide better maintenance—As access to skilled production staff becomes difficult, legacy industrial automation and control technology is becoming more complex to maintain than standard Ethernet and IP networking technology.
- Enhance their flexibility—Standard Ethernet and IP technology allows for rapid production gains, new functionality, and evolving capabilities in the manufacturing environment and beyond.
- Increase efficiency—Standard Ethernet and IP technology eases integration with business systems by using a common network to share information between production and business systems.

Manufacturing organizations and their production operations want to use the newer standard networking technologies in industrial automation and control networks, but there has been little guidance from industrial networking or automation suppliers to date. In addition, although the automation and control industry as a whole has embraced standard networking over legacy, proprietary networking, some industrial automation and control vendors continue to suggest that standard Ethernet and IP technology is not good enough for manufacturing environments. The principle argument has been that deterministic and time-sensitive manufacturing environments require more than what Ethernet and IP technologies can deliver. Others question the inherent determinism, reliability, and resiliency of Ethernet and IP technologies. Some have even asserted that standard networking technology in production environments makes manufacturers more susceptible to security risks. Although there is some basis for these concerns, there is little substantive data to make or support these claims. Modern, full-duplex, switched Ethernet networks offer real-time performance, including latency, jitter, and (non) packet loss capabilities, that equals or surpasses the older fieldbus networks they replace. In addition, these modern networks have mature and tested technologies to safely secure the network and the systems they interconnect beyond what is available for the older fieldbus networks.

EttF is an architecture that provides standards-based network services to the applications, devices, and equipment found in modern industrial automation and control systems, and integrates them into the wider enterprise network. The Cisco EttF 1.1 solution gives design and implementation guidance to achieve the real-time communication requirements needed for determinism as well as the reliability and resiliency required by the industrial and automation control systems. By bringing the Cisco EttF Architecture to market, Cisco can enable manufacturing customers to meet all the challenges of a fully-integrated industrial automation system. The Cisco EttF Architecture also enhances the status of Cisco as a trusted business partner, not only for manufacturing customers but also for industrial automation partners.

Target Customer

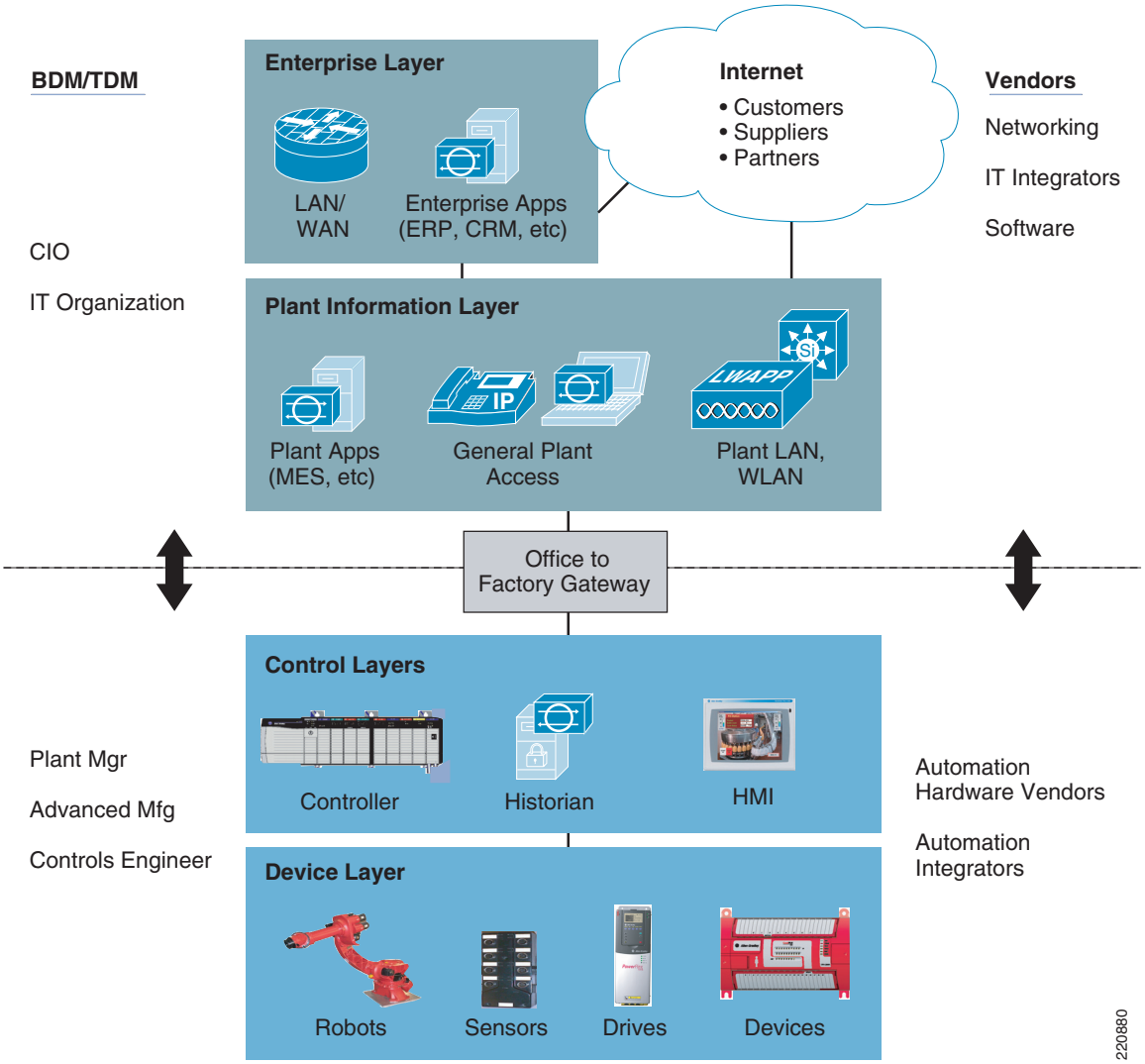
The Cisco EttF solution is targeted at manufacturing customers seeking to integrate or upgrade their industrial automation and control networks to standard networking technologies. These customers want to do the following:

- Lower the TCO of their current industrial automation and control network approach
- Integrate the industrial automation and control systems with the wider enterprise
- Take advantage of the networking innovations provided by using standards-based technologies

Decisions impacting industrial automation and control networks of the factory floor are typically driven by plant managers and control engineers, rather than the IT department. Additionally, they rely on a completely different vendor and support supply chain for their industrial automation and control systems than typically found in the IT department. This is driven by the different requirements of a factory floor. That being said, the IT departments of manufacturing customers are increasingly engaging with plant managers and control engineers to leverage the knowledge and expertise in standard networking technologies.

The Cisco EttF solution recognizes and targets the IT department *and* the plant managers and control engineers. Each camp has different perspectives and requirements for a successful EttF implementation (see Figure 1-1).

Figure 1-1 Business/Technical Decision Makers—IT versus Automation and Control



For the IT department, it is critical to understand the various factory floor requirements and operating environment, and to implement an appropriate solution. For the plant managers and control engineers, a deeper knowledge of the capabilities and functioning of standard networking technologies is required. The Cisco EttF solution includes a large number of references to “basic” networking concepts to recognize the need to raise the level of knowledge and expertise of business and technical decision makers.

To increase its value and impact, the Cisco EttF solution will be brought to market with a key industrial automation and control systems partner, Rockwell Automation. This will allow the Cisco EttF solution to benefit not only from the deep expertise in industrial automation and control systems found in this partner, but also to more effectively target the various business and technical decision makers.

To summarize, the industrial automation and control systems toward which the Cisco EttF solution is targeted see various business and technical decision makers introduced into the decision process. These decision makers often have differing business objectives and concerns that must be recognized. These decision makers rely on different vendors and integrators for solutions and their implementation. In addition, the typical decision makers (IT) stay involved, but may need awareness levels raised concerning the differences and challenges posed by the manufacturing environment.

Plant Managers and Control Engineers

As mentioned, plant managers and control engineers are key decision makers for the Cisco EttF solution.

Plant managers are business decision makers for this solution and are responsible for achieving production targets by ensuring plant reliability, uptime, and energy efficiency. Their performance is typically measured by plant profitability, throughput, quality, and return on assets. Technology decisions are made related to reliability, risk-free operation, environment fit, and company-wide standards. Plant managers usually depend on vendors for support based on track record and industry knowledge.

Control engineers are technical decision makers for this solution, and are responsible for the design, implementation, and operations of the industrial automation and control systems that operate the production facility. They are responsible for the automation equipment that supports the basic manufacturing process. They have a direct share of the responsibility of the quality and consistency of the end product, and often report to the plant manager.

For both these decision makers, the key business drivers include the following:

- Reliability—The solution must support the operational availability of the production facility.
- Cost—Capital comes at a premium, and additional costs (or costlier components) must add clear value that is understood by the plant manager.
- Ease of integration—Not just with enterprise applications, but ease of integrating remote or vendor expertise in a secure manner.
- Flexibility—The ability to rely on common off-the-shelf (COTS) equipment, provided by a number of vendors and supported from a common expertise (often found in the IT department).

Key concerns include the following:

- Performance—Ability of the network infrastructure to meet the real-time communications requirements of the industrial automation and control systems.
- Availability—Both the ability to limit the impact on operations of upgrading or maintaining the Cisco EttF solution, and the reliability of the supported base network infrastructure features to handle outages with minimal impact.
- Manageability—Ease of configuring, maintaining, and fixing the Cisco EttF solution.
- Compatibility—How the network infrastructure supports various types of industrial communications (see Industrial Automation and Control System Communication Protocols, page 1-23) and the devices, controllers, human-machine interfaces (HMIs), and applications already in use.

Both plant managers and control engineers typically rely on vendors with strong knowledge and track records in industrial automation and control. These vendors have varying degrees of capability and knowledge in deploying standards-based networking technologies and the relevant technical issues. By going to market with this solution jointly with a key vendor, the objective is to bring the relevant partners, channels, and integrators up to speed on the availability and capabilities of industrial Ethernet in general and specifically the Cisco EttF solution.

Manufacturing IT

Although IT managers are typically the business and technical decision makers for network infrastructure, they have not typically been involved with network infrastructure for industrial automation and control systems for a wide variety of reasons. They are often seen by the plant managers and control engineers as an obstacle to be avoided, rather than a partner to be relied on for skills, expertise, and services. They are usually making decisions to focus on standardized solutions, to re-use whenever possible, and to reduce cost. There is often a cultural gap between IT and the manufacturing world. However, because IT managers often have the deepest knowledge and expertise in standard networking technologies within the enterprise, their involvement is often required for a truly successful implementation of industrial Ethernet. To help overcome the cultural gap, the Cisco EttF solution does the following:

- Raises IT awareness of the particular challenges and requirements for industrial automation and control systems
- Outlines a solution and relevant design and implementation guidance that allows both to focus on a mutually-acceptable solution
- Pulls IT into the environment to deliver expertise and services based on their strength in standards-based networking technologies

Applications and Services Supported by the Cisco EttF Solution

The Cisco EttF solution primarily supports industrial automation and control systems and their integration into the overall enterprise network. Industrial automation and control systems consist of the following:

- Automation devices, such as robots, sensors, actuator, and drives
- Human-machine interfaces (HMIs) that provide visual status reports and control of the automated manufacturing process
- Controllers such as programmable automation controllers (PACs) and the distributed control system (DCS)
- Higher level plant systems, including the manufacturing execution system (MES) and historians

This version of the architecture focuses on the above items that support EtherNet/IP, which is driven by the Common Industrial Protocol (CIP) (see Industrial Automation and Control System Communication Protocols, page 1-23) and in particular are tested with Rockwell Automation devices, controllers, and applications.

The key networking services that are supported in this version of the EttF architecture include the following:

- Local area networking (typically defined as OSI Layers 1 and 2) to all the above items, including topology, port configuration, subnet and VLAN configuration, network protocols for spanning tree, and quality of service (QoS)
- Routing (typically defined as Layer 3) for all the above items, as well as to other areas of an enterprise network
- Design and implementation recommendations for network technical considerations such as topology, resiliency, and redundancy (including Spanning Tree Protocol), and handling of multicast traffic (including Internet Group Management Protocol configuration)
- IP address allocation, assigning, and related services (for example, DHCP, BootP, and DNS)
- Basic network management

- Network security for the industrial automation and control systems including demilitarized zone (DMZ), firewall, intrusion protection, endpoint security, and security monitoring, analysis, and response

These will be applied to small (up to 50 Ethernet nodes) to medium (up to 200 Ethernet nodes) environments.

Cisco EttF Solution Benefits

The value proposition for the Cisco EttF solution is as follows:

- Enables and simplifies integration of industrial automation and control systems with enterprise networks to improve the flow and integration of production information into business systems.
- Enables remote access for production engineers, partners, and industrial automation and control equipment vendors for diagnostics and maintenance. Increases efficiency and response time and enables industrial automation and control vendors to provide services to customers that may have limited subject matter expert (SME) resources.
- Reduces operating and capital costs by using open standards to eliminate the need to support multiple protocols in industrial automation and control networks and to provide manufacturing companies more options when purchasing automation equipment.
- Integrates more quickly advances in networking technology that come from working with standards-based technologies (for example, voice, video, and security).

Integrating advanced technologies and working with leading industrial automation and control vendors such as Rockwell Automation allows Cisco to have a unique value proposition relative to the rest of the industry by providing benefits beyond those associated with integration and use of open standards, including the following:

- Combining two areas of expertise: the networking expertise of Cisco with the industrial automation and control expertise of Rockwell Automation for the benefit of the customer.
- Providing integrated security specifically configured for industrial automation and control networks to protect vital manufacturing assets, limit access to production equipment, and help address issues such as patch management.
- Providing a foundation for deploying additional advanced technologies such as voice, video, and wireless on the converged network at the control level as the technology matures and the business requires.
- Simplifying deployment and helping to bridge the gap that often exists between IT and industrial automation and control networks by integrating and validating architectures with leading partners in the industrial automation and control market that ensure compliance with relevant industry standards.

The above capabilities depend on the deployment of technologies based on standard Ethernet and IP, and help demonstrate the value of open standards to differentiate Cisco and its partners from other “standards-based” Ethernet and non-standard solutions on the market.

Cisco EttF Solution Features

Industrial automation and control network environments have evolved over the years, driven by a number of key design features. These features are not specific to industrial Ethernet, but to networking for industrial automation and control systems in general. In the move towards industrial Ethernet, many of these design features still apply, although the importance sometimes shifts. For example, with Ethernet and IP-based industrial networks, security is a pressing issue, particularly if there are no access restrictions between industrial automation and control systems and the larger business system. This section defines the following eight key features that the industry expects as best practices:

- Real-Time Communication, Determinism, and Performance
- Availability
- Security
- Manageability
- Logical Segmentation
- Physicality and Topology
- Compatibility
- Scalability

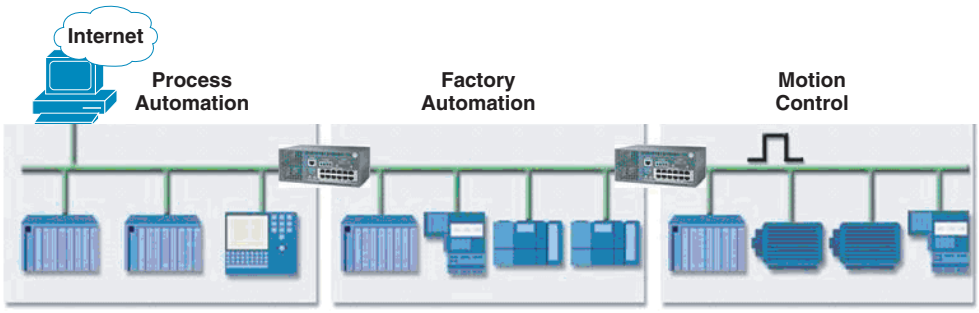
This document provides details on why and how to take advantage of these benefits. The industry, and especially manufacturing participants such as plant managers, control engineers, and their partners and vendors, are looking for simple guidelines and recommendations. Each chapter in this document highlights key recommendations and steps to follow when designing and implementing an industrial Ethernet solution.

Real-Time Communication, Determinism, and Performance

Industrial automation and control systems differ from their IT counterparts in their need to support real-time communications, which means communicating messages with minimal latency (time delay between message sent and message received) and jitter (the variance of the latency). Real-time communications help the industrial automation and control systems become more deterministic. Although the network plays a role in determinism, a number of other factors, such as end-device latency and response time, are also involved. Therefore, the capabilities of standards-based networks to support challenging real-time communications are described in this document.

Industrial automation and control networks have various real-time communications requirements based on the type of application, as shown in Figure 1-2.

Figure 1-2 Real-Time Applications (Source: ARC Research, 2006)



Function	Information Integration, Slower Process Automation	Factory Automation	Motion Control
Comms Technology	.Net, DCOM, TCP/IP	Standard Ethernet + RT Protocol	Hardware/software solution
Period	1 second or longer	10 ms to 100 ms	<1 ms
Industries	Oil and gas, chem, energy, water	Auto, food and bev, elect. assembly, semiconductor, metals, pharma	Subset of factory automation
Applications	Pumps, compressors, mixers Monitoring of temp, press, flow	Material handling, filling, labeling, palletizing, packaging Welding, stamping, cutting, metal forming, soldering, sorting	Synchronization of mult. axes: printing presses, wire drawing, web making, picking and placing

220881

The Cisco EttF solution provides design and implementation guidance to help customers achieve the real-time communications requirements of their industrial automation and control systems.

Key considerations in achieving real-time communications include the following:

- Number of switches and routers and amount of traffic in the Layer 2 network, which affects latency and jitter.
- Ratio of LAN ports to uplink ports based on traffic loads and patterns. Typically, this means using 10/100 Mbps for devices and 10/100/1000 Mbps for uplinks.
- Use of Internet Group Management Protocol (IGMP) to manage the efficient delivery of multicast traffic.
- Use of QoS parameters to meet the real-time requirements of various traffic flows.

Availability

Availability of the industrial automation and control systems has a direct correlation to the operational efficiency of a production facility. Because the network is a key aspect of the overall system, these requirements translate directly to the network.

Note that limitations in the network technology may also limit the application of high availability features. For example, the lack of the ability of the network to converge quickly enough and the cost associated with redundant wiring have often led to non-redundant topologies being implemented in industrial networking environments. The Cisco EttF solution outlines the capabilities so as to let customers and integrators make decisions on the level of network availability needed for the overall system.

High availability considerations are identified in each aspect of the Cisco EttF solution. Key considerations include the following:

- Creating alternative data communication paths, regardless of physical layout. Risk profile, opportunity cost, culture, and other variables determine how much and to what level redundant paths are required.
- Eliminating single points of failure with critical operations, including such items as dual power supplies, alternate routes for redundant media, redundant industrial automation and control network infrastructure, such as routers, switches, and firewalls.
- Using advanced network resiliency and convergence techniques to improve availability, such as EtherChannel/trunks, 802.1w Rapid Spanning Tree Protocol (RSTP), Hot Standby Routing Protocol (HSRP),
- Although redundant star topology offers the best convergence capabilities, consider alternative ring recovery techniques when configured in a ring topology.
- Using routing protocols such as EIGRP or OSPF to achieve high availability.

Security

IP-based networking facilitates interconnection of the industrial automation control system with the enterprise LAN. Many industries have implemented enterprise applications for more efficient production, as well as Internet business applications to communicate more efficiently with their suppliers, customers, and business partners. Internet-based enterprise resource planning (ERP) and supply chain management (SCM) systems simplify connections both to other organizations and to internal business processes. These connections can enable greater efficiencies in processes and manufacturing. In large manufacturing or utility operations, small percentage increases in efficiency can translate into significant cost savings.

However, connecting the industrial automation and control network to the enterprise network brings the security risks of the Internet and enterprise network to the industrial automation and control system. Mitigating these risks is more difficult and more critical than in the enterprise network because of the higher requirement for availability in an industrial automation and control system and the sensitivity of these systems to various disruptions. Of the three security properties of confidentiality, integrity, and availability, control systems are primarily concerned with availability and integrity. Many of the applications that industrial automation and control networks support cannot be stopped or interrupted without serious physical or loss of productivity with measurable financial damage. On the other hand, in enterprise networks that are the primary design consideration for the Internet Protocol (IP) suite, confidentiality and integrity are the primary design considerations. For example, it is preferable for an e-commerce server to be temporarily unavailable rather than for it to lose transactions or divulge credit card numbers. Consequently, the network architectures, firewall configurations, intrusion detection configurations, and other aspects of a security deployment require tuning and customization to properly

support industrial automation and control systems. The industrial automation and control systems industry has been struggling for several years to determine how to build secure, reliable control systems based on IP.

Although standards bodies such as ISA SP99 are still debating security design axioms, there is at least an approximate consensus on what a secure industrial automation and control architecture should provide. This includes an industrial automation and control network that is highly available and redundant, has fast convergence, thus being more deterministic and therefore more suitable for real-time control, and is secure against both outside and inside threats. The specific security principles of the EttF architecture are as follows:

- Control data flows between different levels (ACLs, firewall rules, etc).
- Prevent direct communication between industrial automation and control systems and enterprise systems.
- Restrict real-time production data to the industrial automation and control network.
- Restrict enterprise access to the mirror version or copies of production data to the DMZ.
- Authenticate and authorize user access based on the level within the industrial automation and control network and the role (read/read-write/local/remote/vendor/partner).
- Control rogue access inside the industrial automation and control network (port level MAC address controls, administratively shutdown unused ports, etc).
- Control which devices can be plugged into the switch (for example, port security, DHCP snooping).
- Detect and mitigate malicious traffic originating from infected devices that are plugged into the industrial automation and control network.
- Detect and mitigate malicious traffic originating from the corporate IT network.
- Secure connectivity for remote access to automation devices.
- Use DMZ design options based on costs and levels of security and redundancy required.
- Limit rogue network communication activity from impacting networking devices (set root bridge, SNMP capabilities, and so on).
- Regarding data and services in the DMZ, connection initiation should originate from either the manufacturing or enterprise zone and terminate in the DMZ. Connections originating from the DMZ should be exceptions.
- Document and define policy and risk appropriate for the environment.

The above are provided as principles, with the understanding that customers may choose to make exceptions.

Manageability

Manageability is a key consideration for industrial automation and control systems. Individuals with a basic level of networking skills should be able to manage and monitor the network.

Key manageability concerns include the following:

- Configuring switches using the command-line interface (CLI), element management system (one GUI configures one switch), solution management system (one GUI configures multiple switches), or by downloading pre-defined templates
- Leveraging existing SNMP-based management systems when and where they make sense
- Using other network devices such as routers and security appliances with similar configuration functionality

- Using SmartPort templates for easy port configuration based on application types
- Assigning consistent IP addresses to devices. IP addresses are often coded into the logic of various industrial automation and control devices, rather than using dynamic IP address services such as Dynamic Host Configuration Protocol (DHCP).
- Considering various easy replacement options for network infrastructure elements
- Using systems that offer notification of critical network events (for example, if an Ethernet link goes up or down), and the means to diagnose and debug problems within the network infrastructure
- Staging software upgrades for network devices
- Allowing for patch management of Windows-based automation devices
- Standardizing hardware and software elements wherever possible
- Driving the integration of basic network administration into the existing applications based on various industrial automation and control network protocols

Logical Segmentation

Standard networking technologies provides logical segmentation: managed and controlled inter-connectivity between various parts of the network. Logical segmentation integrates logically (or physically) isolated networks of the production facility with the enterprise and external networks to safely and securely share data, services, and access from the industrial automation and control systems. Logical segmentation is critical for industrial Ethernet because it helps ensure that availability, determinism, performance, manageability, and security requirements are maintained. Logical segmentation means allowing required communication between devices while preventing extraneous traffic from interfering with critical communications between devices on the industrial automation and control network. Logical segmentation is required because industrial Ethernet network architectures may generate traffic that is not readily compatible with general enterprise traffic, and vice versa. For example, multicast traffic in a manufacturing environment may use multicast addresses that overlap with those in the enterprise zone, or traffic in either zone may set QoS markings that create issues in the other zone. The fundamental tenet of logical segmentation is that the manufacturing traffic be separate from the enterprise traffic.

Insulation can be achieved via numerous mechanisms. The Cisco EttF solution provides design and implementation guidelines on the key considerations and mechanisms that can be applied, including the following:

- Using an additional physical or logical De-Militarized Zone (DMZ) to segregate the manufacturing control network from the corporate IT network, especially to do the following:
  - Halt the mixing of incompatible traffic
  - Create clear administrative boundaries to manage organizational control and configuration differences between the manufacturing and enterprise zones
  - Safely and securely share data and services between the zones
- Using hierarchically-tiered switches inside the industrial automation and control network to further segment manufacturing functional areas. (See the following subsections for related parameters in this situation.)
- Limiting the number of devices per Layer 2 domain in industrial automation and control networks to devices that must talk to each other in order to maintain more control over performance characteristics and easily develop a more granular security model.
- Using virtual LANs (VLANs) to create logical structures around Layer 2 domains.
- Using routers/Layer 3 switches to interconnect VLANs.

- Controlling broadcast, multicast, or unicast storms with port-level rate controls where appropriate.

Physicality and Topology

Another key differentiator of industrial automation and control systems is the environment in which the manufacturing process is occurring. Physical constraints in the manufacturing industry are significant. The networking systems need to recognize challenges in spatial and environmental conditions. End devices, such as controllers, drives, and HMIs, located in harsh environments such as the production floor often need to meet environment specifications such as IEC529 (ingress protection) or National Electrical Manufacturers Association (NEMA) specifications. The end device may be located in physically disparate locations (up to miles away), and in non-controlled or even harsh conditions in terms of temperature, humidity, vibration, noise, explosiveness, electronic interference, and so forth. These requirements are conditions of the network device and are not a specific focus of the Cisco EttF solution. Additionally, the physical media infrastructure is also driven by the location of the end-devices and physical requirements of the environment, with special consideration given to the potential for high noise, but is not currently a specific focus of this solution.

The physical layout of the manufacturing facility or the automation equipment also impacts the network topology for automation networks. Unlike traditional IT networks, which are largely redundant star topology networks, industrial automation and control networks have significant physical limitations that drive the use of topologies such as linear-bus and ring. In manufacturing plants with long production lines, or equipment with long runs and interconnected operations (such as a printing press, or similar types of equipment), it is often not feasible or cost-effective to use a redundant star topology. In manufacturing environments, the costs of cabling are significantly higher than typical office conditions to meet the harsh physical requirements. Although the redundant star network topology offers the best resiliency, convergence, and overall performance, the additional cabling complexity and constraints of a redundant star limit its applicability in manufacturing environments.

In addition, current industrial automation and control applications do not use significant bandwidth, and are therefore not significantly impacted by the potential bandwidth limitations of ring or linear-bus topologies. In many cases, the industrial automation and control network is a combination of topologies, with large rings connecting multiple star-based manufacturing cells.

Cost considerations also drive the architectural and technology directions of many manufacturing companies. Given the physical layout of a manufacturing plant and industrial automation and control equipment, it is often significantly cheaper to implement a ring topology than a redundant star topology.

Based on these considerations, the design guidelines provide information regarding the trade-offs between the various topologies to help customers, partners, and account teams to make appropriate design decisions. Because of their significant use in manufacturing, bus topologies are discussed, as well as the associated trade-offs between bus, ring, and redundant star architectures (such as availability, and etc).

For a summary of the advantages and disadvantages of each topology, see Cell/Area Topology Comparison, page 2-25.

Figure 1-3 shows a star topology. Note that Figure 1-3 to Figure 1-5 are meant to depict the network device topology and not necessarily the number or type of end devices.

Figure 1-3 Star Topology

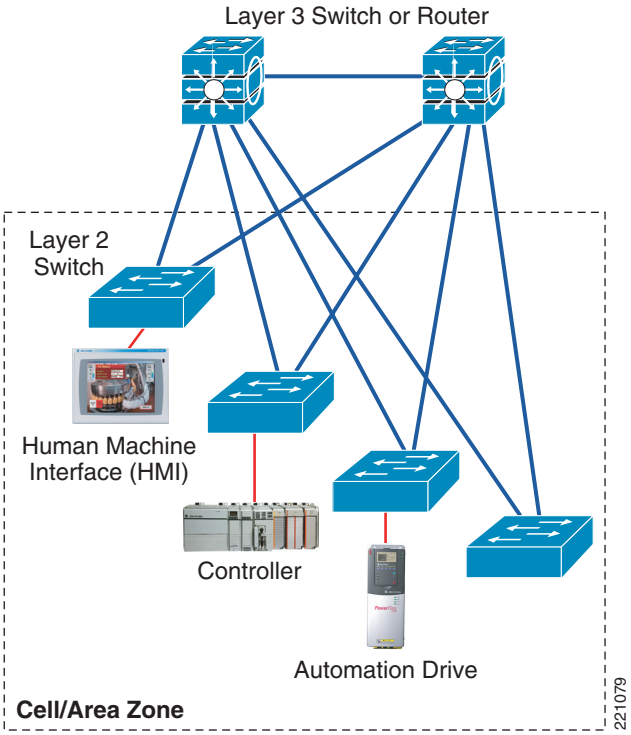


Figure 1-4 shows a ring topology.

Figure 1-4 Ring Topology

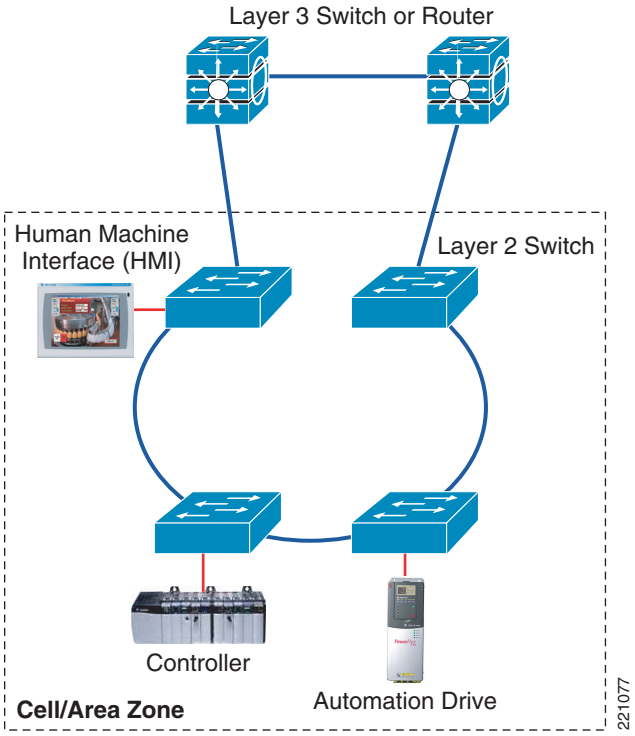
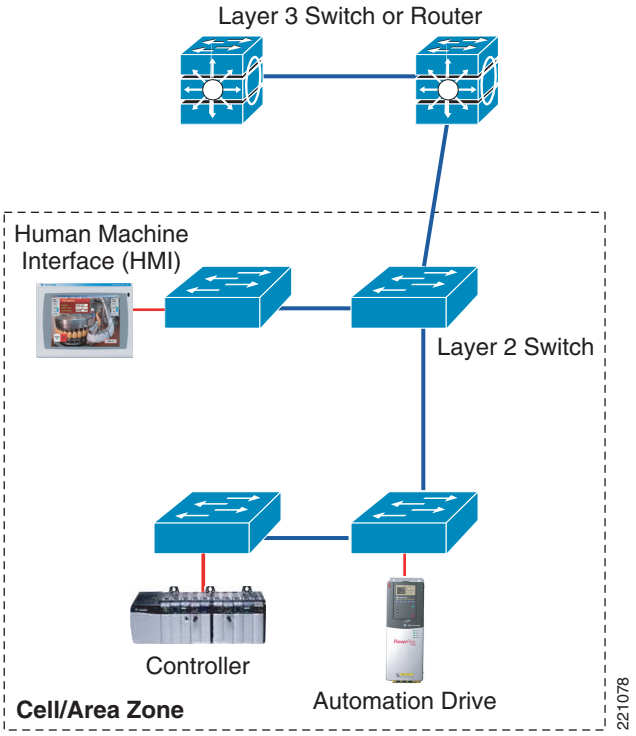


Figure 1-5 shows a bus topology.

Figure 1-5 Bus Topology



The Cisco EttF solution design and implementation guidelines include the following key considerations:

- Choose a topology that meets the performance, cost, and spatial requirements of the automation and control application.
- The layout of plant operations, conduit/wiring paths, cost, and desired level of availability determine whether the network topology follows a tree, ring, star, or trunk and drop topology, or a hybrid.
- Use ruggedized/hardened network devices in the factory environment where needed, but consider using non-industrial routers, switches, and firewalls where possible to reduce cost.
- The number of automation devices and grace ports for programming/troubleshooting and 10 percent spare for future expansion determines the type and size of switch needed at various levels.
- Hierarchically-layered switches may be required to address density, distance, or communication path challenges.

Compatibility

By definition, industrial Ethernet (IE) protocols should operate on standard networking technologies and infrastructure. However, standard networking technologies have a wide range of service and configuration options that need to be considered to effectively support the industrial automation and control application. As well, various IE protocols rely upon various networking features to operate at required performance levels.

EttF must show compatibility with the IE protocols and communication models of the applications that run on it. This typically means supporting the types of traffic they generate, such as TCP and UDP (multicast and unicast), as well as any features and functions they expect of the network, such as quality

of service (QoS). A large number of types of traffic may exist in an industrial Ethernet network, including automation and control protocols such as CIP, Modbus/TCP or OPC, as well as common protocols such as web browsing (HTTP), file transfer (FTP), and many others. The Cisco EttF solution outlines how to design and implement compatible network architectures.

Industrial Automation and Control System Communication Protocols, page 1-23 lists the relevant general industrial protocols and the corresponding industrial Ethernet versions. This solution architecture focuses on the Common Industrial Protocol (CIP). Other network protocols are considered (see the sub-sections on traffic flows in Cell/Area Zone, page 2-2 and Manufacturing Zone, page 2-33).

Scalability

Once installed, industrial automation and control systems, once installed, tend not to grow, but rather are replaced or have additional lines, systems, or functions. Industrial automation and control systems come in a wide range of sizes, from the small OEM solutions to the extremely large factory complexes (for example, an automotive plant). The industrial automation and control system may include only a small number of devices (up to 50) to multiple 10,000s of devices. The solution architecture concepts and recommendations need to be applicable to that range, noting the considerations for various sizes.

This version of the solution architecture focuses on basic concepts, tested in typical small-to-medium network installations. Rather than focusing on full-range and scalability testing, this solution architecture focused on defining and testing core concepts that are applicable to a full range of factory floor sizes. The basic concepts in this guide are applicable to the range of industrial automation and control systems.

Key scalability considerations include the following:

- Network infrastructure sizing and performance constraints
- Network infrastructure tiering to meet spatial, size, and performance criteria
- Link aggregation to achieve higher bandwidth requirement
- IP addressing schema and allocation mechanism
- Maintenance and management considerations as manual tasks have greater impact in large environments

Scope of the Cisco EttF Solution

This phase of the Cisco EttF solution is meant to introduce a basic network architecture based on standard technologies to provide services to industrial automation and control systems. The first phase is a starter kit for customers, partners, and vendors seeking to implement a basic EttF solution.

Key aspects of this phase include the following:

- The Cisco EttF 1.1 solution focuses on wired solutions for the industrial automation and control systems.
- The Cisco EttF 1.1 solution is designed for small (less than 50 Ethernet endpoints or nodes) to medium (less than 200 Ethernet nodes) manufacturing environments.
- The Cisco EttF 1.1 solution introduces key technical considerations such as the following:
  - Topology
  - Real-time communications
  - OSI Layers 2 and 3 configuration including basic routing protocols
  - Insulation and segmentation including VLANs and DMZ design

  - Multicast traffic handling including IGMP protocol
  - Quality of service (QoS)
  - Redundancy and resiliency (including application of the standard RSTP)
  - IP address allocation, assignment, and related services (for example, DHCP, and DNS) in a manufacturing perspective
  - Basic network management
  - Network security for the automation and control systems including DMZ, firewall, intrusion protection, endpoint security, and security monitoring, analysis, and response
- Design and implementation is based on EtherNet/IP (driven by CIP) based automation and control systems.

Key Terms and Definitions

- *Industrial Automation and Control systems*—Refers to the set of devices and applications used to automate and control the relevant manufacturing process. Rather than use various terms with a similar meaning e.g. production systems, factory floor systems, we standardized on this term for use in this paper. That is not to suggest any specific focus or limitations. We intend that the ideas and concepts outline herein are applicable in various types of manufacturing including but not limited to batch, continuous, discrete, hybrid and process.
- *Cell/Area Zone*—A logical section or subset (physical, geographical or function) of the production facility. It typically contains Level 0-2 devices (see Automation and Control Reference Model).
- *Demilitarized Zone (DMZ)*—Refers to a buffer or network segment between 2 network zones. A DMZ is commonly found between a corporate network and the internet where data and services can be shared/accessed from users in either the internet or corporate networks. A DMZ is typically established with network firewalls to manage and secure the traffic from either zone.
- *Determinism*—is a property of an overall automation and control system that behaves determined only by initial state and input. Many factors impact the deterministic nature of a system, including network performance. For the purposes of this document, we will consider the network low latency, minimal jitter and minimal packet loss as the key network criteria that impact the deterministic nature of the overall automation and control system.
- *Ethernet*—is a family of frame-based networking technologies or standards (IEEE 802.3) for local area networks. It defines standards for common addressing format and the physical and data link (or Media Access Control) layers of the OSI Model. See the IEEE 802.3 working group's site (http://www.ieee802.org/3/) for more details on the set of standards.
- *Factory or Factory Floor*—This document chose to use *Factory Floor* as the keyword to describe the area in which the manufacturing process and control takes place. This is not to exclude similar words such as plant, production facility, or any other term used to refer to the area in which the manufacturing process exists. In fact, they can be used interchangeably, but for the purpose of consistency, we chose to use *Factory Floor.*
- *IP Protocol Suite*—Is a set of networking standards on which the internet and most enterprise networking is based. It includes the Layer 3 Internet Protocol (IP), the layer 4 Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- *Jitter*—Refers to the variation in Latency (see definition below). Jitter is important as often larger variations in the delay due to communications can negatively impact the 'deterministic' nature of the relevant system.

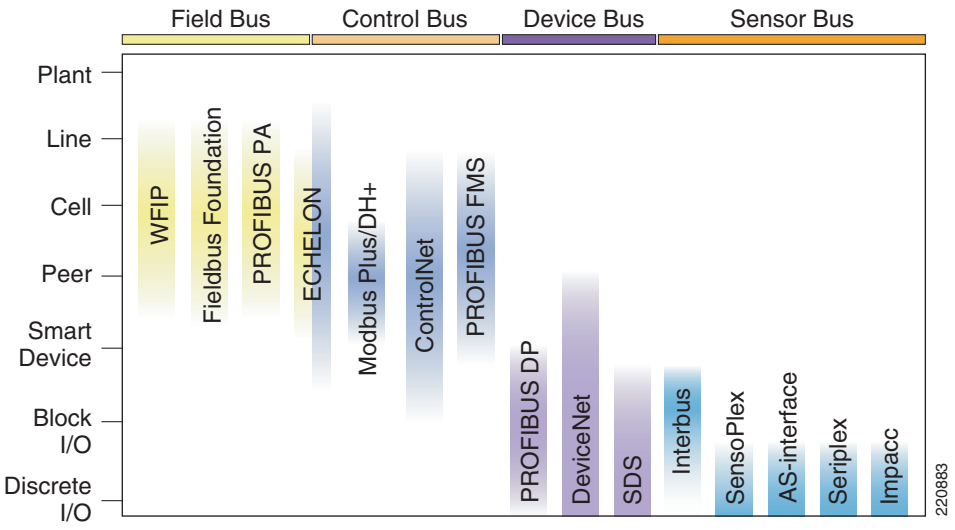
- *Latency*—Refers to the delay in communications due to transmission media (Switches, Routers and cables) between any two end-devices. Latency could also refer to the processing time in an application to process a message.
- *Layer*—Refers to layers of the OSI Model which logically describe the functions that make up networked communications (see Networking Equipment, page 1-20).
- *Level*—Refers to levels of the Automation and Control Reference Model that describe functions and domains of control within manufacturing organizations.
- *Manufacturing Zone*—Refers to the complete set of applications, systems, infrastructure and devices that are critical to the continued operations of the factory floor.

Industrial Automation and Control Background

History of Industrial Automation and Control Networks

From the beginning, manufacturing environments have relied on numerous technologies to enable communication at the plant, cell, or I/O level. Typically, the technologies deployed were purpose-built and vendor-specific. Figure 1-6 provides a list of some of the types of protocols used in manufacturing environments.

Figure 1-6 Control Protocols Overview (Source: David Humphries, ARC)



The industrial automation and control industry as a whole has been moving away from the purpose-built and vendor-specific communication protocols for reasons that include the following:

- Difficulty of finding and training people who can debug a specific communication network technology
- Difficulty of extracting data for production reporting with older fieldbuses
- Expense of using vendor-specific technology to tie industrial automation and control systems together

- End user frustration in procuring industrial automation and control systems because of the confusion related to various fieldbus technologies
- Complexity of integrating various technologies into the overall industrial automation and control system

Ethernet and the IP protocol suite are now the ultimate solution to the multiple standalone industrial automation and control protocols. Ethernet and the IP protocol suite are standard technologies that provide a robust, cost-effective, easy-to-implement, and easy-to-troubleshoot mechanism for transmitting industrial automation data. Industrial networks based on standard Ethernet and IP technologies define the physical and transport layer for moving data. However, these technologies do not replace fieldbus communication standards per se. For example, fieldbus communication standards still define the data and its meaning and determine how messaging occurs. Each technology has its purpose, depending on the protocol and the data that is in the device.

Industrial Automation and Control System Components

Physical Layer

Many of the purpose-built and vendor-specific industrial technologies have specific physical media requirements that often require unique cabling (such as co-axial) and specialized termination (such as serial connectors). These various physical layer specifications result in a complete physical media upgrade when migrating from one system to another. In comparison, industrial Ethernet uses standard Ethernet wiring; either twisted pair cables, or multimode or single mode fiber. The connectors for these various types of Ethernet wiring are also standardized with RJ45 connectors for copper cables, and SC or ST connectors for fiber optic cables. In extreme cases, sealed connectors may be required. The benefit of Ethernet is that after the Ethernet physical plant is installed, it can be used to connect hardware and software from multiple vendors.

Typical Ethernet speeds are 10Mbps, 100Mbps, and 1Gbps. 10 Gbps is mainly being deployed in enterprise-wide backbone networks. Most industrial automation and control installations rely upon 10Mbps or 100Mbps Ethernet and Gigabit Ethernet is appearing in industrial system backbones.

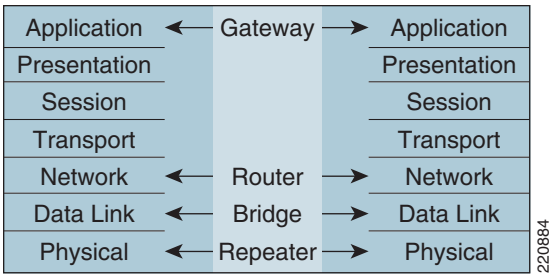
The physical layout and communication requirements of a manufacturing environment dictate how various Ethernet-based resources are physically connected. Typical Ethernet environments have full duplex connection via a redundant star topology. Other options are possible such as ring, trunk and drop, and daisy chain. Specific operating constraints when using Ethernet in these other models are discussed in Chapter 4, “Implementation of the Cell/Area Zone .”

Networking Equipment

As the industrial automation and control industry adopts standard Ethernet and IP technologies, it benefits from the access to a wide range of standard networking equipment. The type of device required depends on many factors, the first being what type of communication protocol is in use. As Figure 1-7 shows, various types of devices work at different layers of the OSI model and common devices that perform representative interconnect functions.

Note For the purpose of this document, the term *layer* refers to layers of the OSI model. For example, Layer 3 refers to the Network layer of the OSI model, and in standard networking refers to the IP protocol.

Figure 1-7 OSI Model



Many early factory floor Ethernet networks used simple, cheap repeaters (also known as hubs) to connect industrial automation and control systems together. In many cases, these were the same Ethernet hubs that were handling front-office workstations. As a multi-port broadcast device, a hub does the following:

> "Creates one big collision domain, with all traffic shared. As more network nodes are added or traffic increases, every node in the collision domain has a greater chance of slowing communication or having a collision. Additionally, because industrial automation and control networks are not configured to differentiate between the relative importance of Ethernet packets, it is possible for non-essential traffic on the network (perhaps people backing up their computers to the network server or printing a large document across the network) to slow or collide with essential traffic (such as inter-PLC communication or HMI polling)."
> (Source:http://www.cisco.com/warp/public/779/smbiz/languide/p4.html)

The next advancement in industrial network design was to use switches; a type of multi-port Layer 2 bridge. Switches can divide networks into VLANs that segment devices into logical work groups. Ethernet switches also typically have a fast internal backbone, which helps eliminate collisions among data packets. Switches separate collision domains and map Ethernet nodes based on address and port. When an industrial automation and control device is directly connected to a non-blocking switch in full-duplex mode, potential collisions are eliminated. This occurs because full-duplex Ethernet devices can both send and receive packets of Ethernet data at the same time. This increases the level of determinism of Ethernet, assuring that packets arrive with much greater certainty, and that each port has more bandwidth available for communication at any time.

Adding some intelligence to the switch improves traffic management capabilities, meaning that the switch can provide more granular quality-of-service (QoS) for industrial automation and control networks. One example is the management of multicast traffic to communicate critical I/O data applied in most implementations of EtherNet/IP. Management of the multicast (rather than treating it as broadcasts as unmanaged switches do) significantly reduces the number of messages that end devices and network infrastructure must process, leading to better network and device performance. As another example, by assigning a priority to time-sensitive data, intelligent Ethernet switches can prioritize that traffic above lower-priority data. This ensures that high-priority traffic always traverses the network, even if the network becomes congested. Switches can also classify, reclassify, police, mark, and even drop incoming data packets as application priorities require. The use of managed versus unmanaged switches is a key consideration facing those implementing industrial automation and control networks today. Both Cisco and Rockwell Automation highly recommend the use of managed switches. For further details on managed versus unmanaged switches, see Network Design Overview, page 2-26.

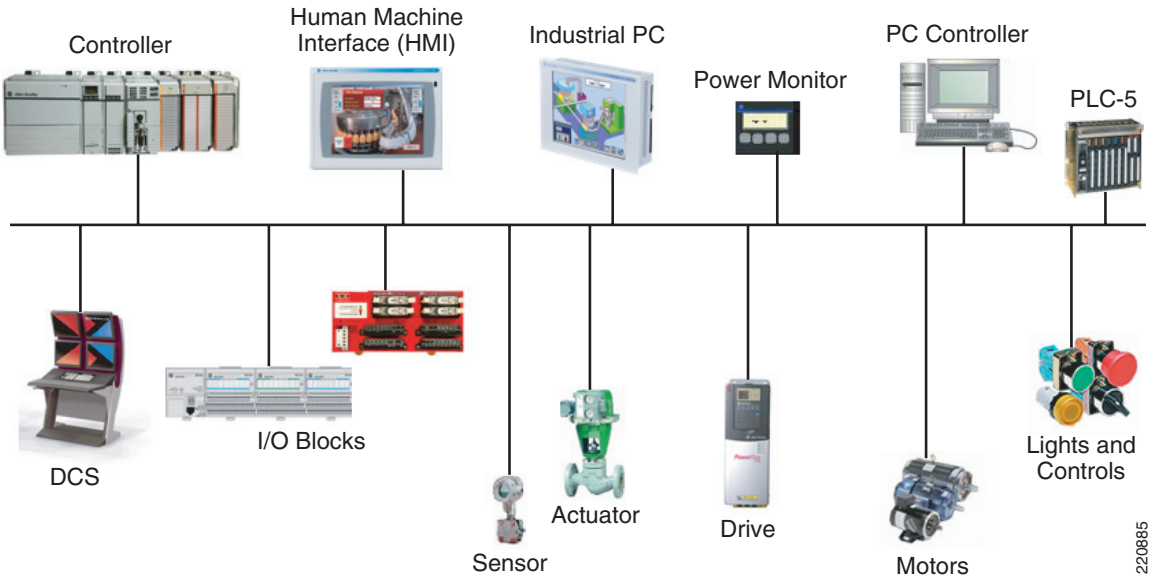
In some cases, Layer 3 switches or routers are used in manufacturing environments. Layer 3 switches or routers connect LANs or VLANs. They use information in the IP header (Layer 3) to do so. Regardless of the specific layer being connected, switches provide industrial automation and control networks with many of the safeguards that were realized by the natural separation inherent in existing factory floor optimized networks.

The specifics of how a Layer 2 switch is used compared to a Layer 3 switch, how to implement multi-cast management and how QoS can be implemented is addressed in Cell/Area Zone, page 2-10.

Industrial Automation and Control Devices

Numerous types of devices are used in industrial automation and control systems. Some are small, simple, single function sensors or input/output devices (e.g., a light or on-off switch), while others are complex, programmable automation controllers (PACs). The breadth and depth of available devices is driven primarily by industrial automation and control vendors and their partners and suppliers. Figure 1-8 shows some of the various types of devices used in the manufacturing environment.

Figure 1-8 Industrial Devices



Older lower-level industrial automation and control devices tend to use specific industrial automation and control protocols and are capable of only low data rates and volumes, albeit with deterministic characteristics. More advanced industrial automation and control devices have internal logic optimized for I/O control with the ability to support higher data rates and volumes. Many of these newer industrial automation and control devices now come standard with more communication options including Ethernet and IP. For example, controllers now come with options of 512 K to 100+ MB of memory, integrated serial communication interfaces (integrated RS-232-C, RS-422 or RS-485 ports for SCADA, ASCII, or peer-to-peer communication), modular and scalable EtherNet/IP, and ControlNet and/or DeviceNet communication interfaces.

The trend with most industrial automation and control devices is to add more functionality and capabilities at all levels. This is occurring because of the continual evolution in the microelectronics industry and access to lower cost components with more functionality. The low cost of microcontrollers is already making it easy for design engineers to include Ethernet and IP in a growing number of products that exist in common industrial automation and control systems. As with many electronic technologies, after a few high-end products incorporate a feature or function, it rapidly becomes a common attribute on many of the emerging new products.

Even so, there is and will continue to be a place for simple, low cost, and lower capability devices in industrial automation and control systems. When Ethernet and IP represents too much of a cost and capability increase for the end device itself, these devices will continue to communicate via simple, non-Ethernet I/O networks; for example, a distributed I/O device used as an Ethernet network concentrator connecting a number of simple devices, such as a push button, to a controller.

Industrial Computing

Computing technology has been used for years in purpose-built and vendor-specific manufacturing environments. Just as with IT, the technology has migrated from mainframes and mini-computers with dumb terminals to standalone, dedicated computing platforms. With the cost of computing highly commoditized, the trend now is to put computing power anywhere in the industrial automation and control network using high performance CPUs. By using fanless and diskless PCs with features such as capacitive touchscreens, class 1 division 2 environment certification, and mission-critical solid-state drives, computing platforms are now suitable for any harsh industrial or embedded device application.

From an operating system perspective, most industrial automation and control vendors have moved away from legacy or custom-built operating systems to common off-the-shelf operating systems based on Microsoft or Unix derivatives (including Linux) for many products. The benefit of this development is a simpler and faster application programming environment both for vendors as well as end users. This migration has coincided with the overall general trend in the software industry towards Internet browser-based technology. This gives automation vendors the ability to embed web interfaces directly into industrial automation and control devices.

The downside of all these developments is a significant amount of system complexity related to security and patch management. The specific application requirement of industrial automation and control systems is discussed in Chapter 2, “Solution Architecture.”

Industrial Automation and Control System Communication Protocols

Communication Model

The communication messaging model in manufacturing environments has only loose ties to traditional client-server or peer-to-peer IT models. Unlike the typical IT environment, standards-based Ethernet and IP industrial automation and control communications have different patterns, loads, and frequencies required by the manufacturing process they support. Standards-based industrial automation and control communications are also driven by status polling between devices, cyclic data transfer, or change of state message patterns. The various requirements of the layers previously discussed have led key industrial automation and control providers to define a variety of communication models, including OSI layers 1 to 7 networking protocols.

These communication models have both strong commonalities and differences. In common, they differentiate the control or I/O traffic between devices and the PACs (EttF levels 0–1) and administration traffic within the upper layer applications down to the PAC (EttF levels 1–3). This differentiation is made to meet the stringent requirements at these lower levels (see Industrial Automation and Control Reference Model, page 2-1). However, the models can differ greatly at the control or I/O level. One example is the producer-consumer model applied in the Open Device Vendor Association (ODVA) Common Industrial Protocol (CIP). This model describes how devices “produce” data to be “consumed” by other devices; in particular, the PACs that take action on their data and control their behavior. These models are incorporated into the industrial automation and control protocols described below. They are important because they impact or shape the network traffic that is produced by the applications that use them.

CIP, for example, defines two distinct message types: *explicit* messages and implicit messages. In an explicit message, the action is explicitly implied in the message; for example, read the value of a variable. Explicit is a request/response, client/server-like protocol typically used for "information" and administrative messaging and is implemented over the Layer 4 TCP protocol. In an implicit message, the data is implied; the communicating parties inherently know how to parse the message content because of contextual knowledge. Explicit messages are information messages used for additional device configuration and diagnostics of features of the industrial automation and control device. Explicit messages are highly variable in both size and frequency based on configuration and application.

Implicit messages are typically used for cyclic, Input/Output messages to/from controllers and devices. Implicit messages are sent either unicast or multicast over the Layer 4 UDP protocol. Implicit messaging or real-time control is sent at specified intervals, and although the size can vary, it is consistent after the configuration is set and is generally smaller than explicit messages. Implicit messages contain control data that must be interpreted very quickly by the receiving device, which demands network and end-device performance that is different than other traffic. With implicit traffic, the UDP protocol is used (either unicast or multicast) to minimize processing resources and time on the end device.

Network traffic in manufacturing environments can include significant and varying amounts of unicast, multicast, or broadcast traffic driven by the communication models applied (e.g., producer/consumer, client/server, master/slave, multi-master, or peer-to-peer relationships). For the purpose of this document, we focused on the network implications of the Producer consumer model applied in CIP. These differing communication models and the protocols into which they are embedded drive various configuration considerations for the networks that support the automation and control systems. For example, the CIP use of multicast traffic generates different network configuration considerations. However, these differences are focused on specific areas of a manufacturing network where the networking requirements are the most significantly different than standard IT networks. Chapter 2, “Solution Architecture,” introduces a framework and model for industrial automation and control to clearly describe these areas and the network implications to be considered when designing and implementing the systems.

Industrial Automation and Control Protocol Overview

Most Ethernet and IP-based industrial automation and control protocols have a common core. This includes the physical transmission technology (Ethernet, Layer 1), the bus access method (Ethernet, Layer 2), the Internet Protocol (IP, Layer 3), the TCP and UDP protocols (Layer 4), the Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), and the Simple Network Management Protocol (SNMP). All these are established in the IT industry and are being implemented to varying degrees, unchanged in industrial automation and control applications.

The goal of an Ethernet and IP-based industrial automation and control network is to ensure that the control protocol of choice, assuming it is based on standard Ethernet and IP, is supported to meet the operating constraints of the industrial automation and control systems.

Table 1-1 shows a list of some industrial automation and control protocols that support or partially support standard networking.

Table 1-1 Control Network Protocols

Fieldbus Protocol	Ethernet Implementation	Leading Vendors	Standards Body	Application
DeviceNet, ControlNet	EtherNet/IP (EIP)	Rockwell Automation, Schneider (EIP), Omron, Eaton	ODVA	Industrial automation process control
PROFIBUS DP, PA, and so on	PROFINET CBA, I/O, IRT, and so on	Seimens	PROFIBUS Foundation	Industrial automation process control
Modbus	Ethernet Modbus TCP	Schnieder	Modbus.org	Industrial automation process control
Foundation Fieldbus	Foundation Fieldbus High-Speed Ethernet	Emerson, Honeywell, ABB	Fieldbus Foundation	Process control
CAN/ CAN-Bus	ETHERNET Powerlink	Bernecker, + Rainer	ETHERNET Powerlink Standardization Group	Motion control
Sercos Interface	Sercos III	Bosch Rexroth	SERCOS International	Motion control

However, there are some differences in the application protocols for real-time communication as well as the object and engineering models for system configuration. These differences lead to different considerations and deployments of industrial automation and control networks. Of these protocols, EttF Architecture Phase 1 is focused on exploring only the ODVA implementation of CIP on the Ethernet and the IP protocol suite referred to as EtherNet/IP.

In addition to the approach taken to integrate with Ethernet (physical and data layers) and the IP protocol suite, these application protocols have also identified various messaging frameworks that dictate the type of traffic and traffic patterns found in the industrial automation and control network.

Table 1-2 briefly describes some of the key characteristics of the various protocols.

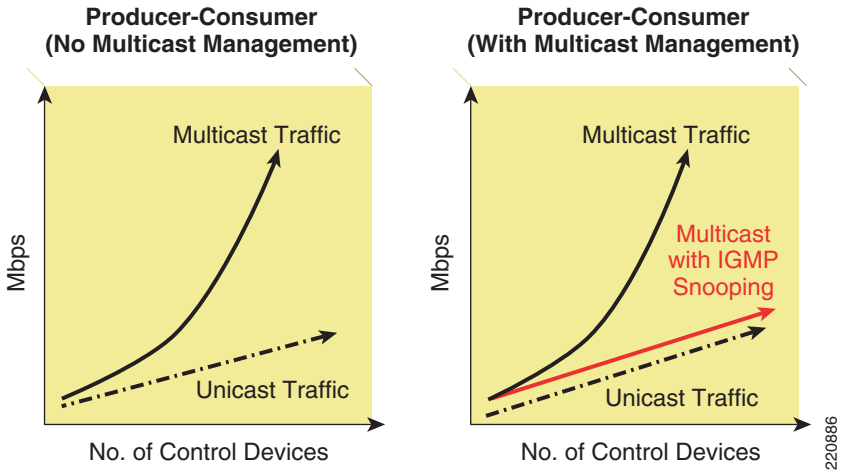
Table 1-2 Various Features of Different Industrial Ethernet Protocols

IE Protocol	Encapsulated Telegram	TCP/IP UDP/IP	Port Usage	Profile/Object Support
EtherNet/IP	Common Industrial Protocol (CIP)	TCP/IP explicit UDP/IP implicit	44818 2222	Legacy
Modbus/TCP	Modbus	TCP/IP	502	Legacy
PROFINET CBA PROFINET I/O and IRT	Profibus Plus	TCP/IP Special Data link	Dynamic	ORPC
OPC (OLE for Process Control)	DCOM/XML	TCP/IP	Dynamic	DCOM / XML
MMS TCP/IP	MMS	TCP		MMS
.NET for Manufacturing	COM	TCP/IP	80	DCOM/ XML
Foundation Fieldbus HSE	H1	UDP/TCP Optimized	Dynamic	Legacy plus
iDA	N/A	UDP/IP	Dynamic	XML
AADS-net	N/A	UDP/IP	Dynamic	Possible

The various protocols and their application of the Ethernet/TCP/IP stack drive particular considerations in the configuration of the network. Using CIP and the "producer-consumer" model as an example, the control-level devices use UDP unicast and/or multicast to send critical, cylic I/O data out on the network. Although the choice to use multicast or unicast is the choice of the device vendor, multicast is the default mode of communication of I/O data in CIP implementation in EtherNet/IP.

The ability to control multicast traffic in the control levels of the network is a very important aspect of the network devices. Figure 1-9 shows how without multicast control features, the bandwidth requirements in an industrial automation and control network application increase exponentially (versus a linear increase) with the increase in the number of devices. This is just an example of the type of network design, configuration, and implementation considerations specific to industrial automation and control protocols.

Figure 1-9 Producer-Consumer Network Impact

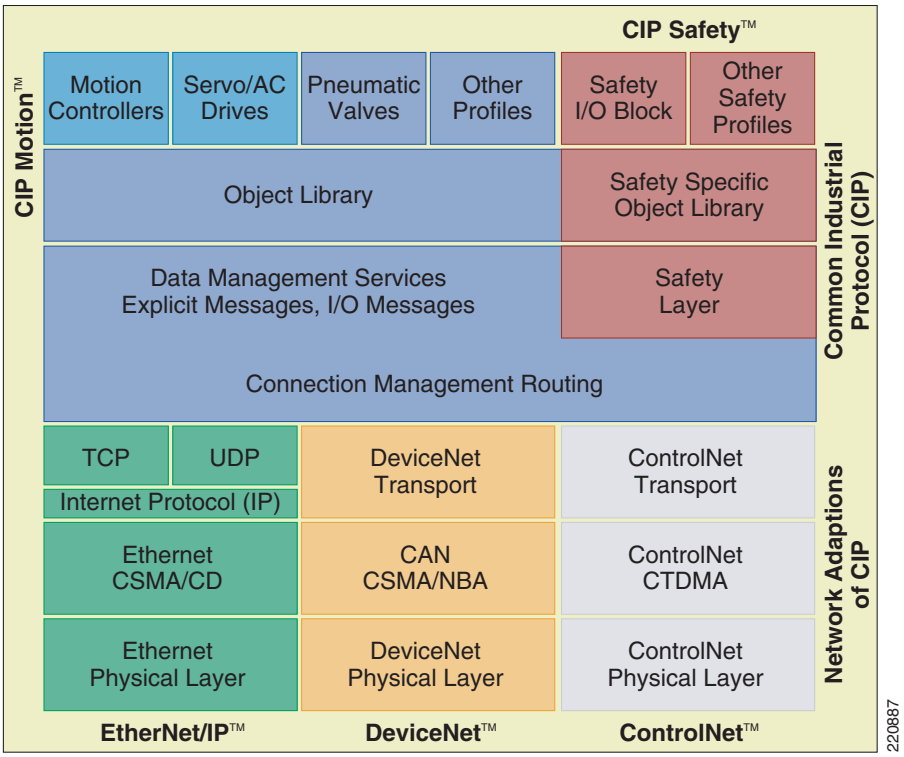


In summary, a wide number of protocols are in operation in industrial automation and control networks. Design and implementation guidelines need to consider the various protocols and their underlying communication models. This initial version covers EtherNet/IP and the CIP protocol along with the producer-consumer communication model. Over time, this architecture and the subsequent deliverables will take into account the various communication relationships, protocols, and Ethernet/TCP/IP implementations when designing, implementing, and operating an industrial automation and control network.

Common Industrial Protocol Overview

CIP is a messaging protocol that defines how various industrial automation and control devices, systems, and applications come together to form an industrial automation and control system, as shown in Figure 1-10. CIP is an application-layer protocol (OSI Layers 5–7). EtherNet/IP extends the application of Ethernet TCP/IP to the factory floor for CIP-based applications.

Figure 1-10 Common Industrial Protocol (Source: ODVA)[1]



CIP is a connection-based protocol and offers two main types of messaging: explicit and implicit. The protocol specifies a set of objects and services used to develop industrial automation and control systems. CIP is implemented on three network layers: DeviceNet, ControlNet, and EtherNet/IP. This document is concerned only with EtherNet/IP.

For more information on CIP and the various network layers, see the ODVA website at the following URL: http://www.odva.org; and ControlNet International at the following URL: http://www.controlnet.org.

The important aspects of the CIP implementation of EtherNet/IP are the various types of messaging that are used and how they are implemented in standard Ethernet TCP/IP.

1. EtherNet/IP, ControlNet, DeviceNet, and CIP are trademarks of ODVA, Inc.

Table 1-3 provides a brief overview of the CIP messaging types and their key networking characteristics.

Table 1-3 CIP Communication Overview

CIP mode	CIP message type	Description	Response time requirements	Layer 4 type	Packet Size (Bytes)[1]	Port[2]
Unconnected	Unconnected	Basically used to open a CIP connection with another device. This mode is only temporarily used.	Seconds	TCP	~500	44818
Connected	Explicit	Non-time-critical information data. For example, between a controller and a manufacturing historian application.	100s of milliseconds to seconds	TCP	~500	44818
	Implicit or I/O	Time-critical control information usually passed on regular intervals in a "producer-consumer" multicast communication model. For example, between a controller and a drive (PAC to device) or between controllers (PAC-to-PAC).	< Millisecond to 10s of milliseconds	UDP multicast and unicast	100 - 200	2222

1. These are typical numbers, although depending on the application and customer can be different
2. These are registered ports for EtherNet/IP, although non-registered ports may be used in EtherNet/IP.

Other key technical considerations for EtherNet/IP implementations include the following:

- The producer-consumer model specifies that "producers" of I/O data communicate via UDP unicasts or multicasts. The consumers (for example, controllers) typically respond with UDP unicast messages. Rockwell Automation and the ODVA therefore recommend the application of IGMP to manage the multicast traffic flow.
- Multicast traffic in current installations is stamped with a time-to-live (TTL) value of 1, rendering the multicast packets un-routable. This limitation forces all nodes that produce and consume information from one another to exist in the same subnetwork/VLAN. The capability to change/increase this value has been outlined in the most recent version of Volume 2 (EtherNet/IP Adaptation of CIP) of the CIP Specification release 1.3, which was published in December, 2006. For the purpose of this solution architecture, it is assumed CIP-based multicast traffic is not routable.
- By the current EtherNet/IP standard, a multicast group is created for each Ethernet adapter that "produces" information, and for each "produced" tag (shared piece of data) established by a controller. EtherNet/IP specifies an algorithm to establish the multicast address and the commands to join and leave multicast groups. Current EtherNet/IP multicasting is based on IGMP version 2, although there are devices (producers) that may still be based on IGMP version 1. IGMP version 1 devices should function in a version 2 environment. This was not tested in the Cisco EttF solution.
- Depending on the device producer, options may be enabled to configure whether the traffic generated by the PAC for each "produced" tag is unicast and multicast. This allows more flexibility in cell/area design and a means to manage the number of multicast groups within a cell/area.
- No CIP-EtherNet/IP QoS guidelines have been developed, so devices and applications typically do not mark either MAC-layer class-of-service (CoS) or IP-layer Differentiated Services Code Point (DSCP) fields. The ODVA has included a placeholder in the specification for QoS and work is currently ongoing to develop an approach.