CHAPTER 1

Converged Plantwide Ethernet Overview

Executive Summary

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

- Globalize operations through IT integration with Industrial Automation and Control Systems, enabling plant-to-business network convergence, thus driving strategic business decisions that are backed by real-time data from IACS.
- Visibility into the IACS for optimized supply chain management.
- Provide visibility into the plant floor for optimized supply chain management.
- Improve operational costs and efficiency through ease-of-use features and capabilities of common tools that improve productivity for plant maintenance and engineering personnel.
- Reduce mean-time-to-repair (MTTR) and increase overall equipment effectiveness (OEE) through secure remote access for employees and partners.
- Mitigate risks by improving network uptime and equipment availability with industry-leading security features and a defense-in-depth approach that protect critical manufacturing assets.
- Shorten lead times of deploying new products as communication and collaboration between business decision makers and plant personnel become richer and easier through converged networks.
- Reduced costs and improved asset utilization by relying on standard Ethernet and IP networking technology for IACS networks, such as personnel training, spares and development tools.
- Simplified management through better integration with Industrial Automation and Control System applications and use of remote management capabilities.
- Realize productivity improvements as ready-to-deploy collaboration technology (voice-over-IP phones and IP security cameras) become more common in IACS networks.

The key industrial Ethernet applications are Industrial Automation and Control Systems (IACS) networks. For the purpose of this *Design and Implementation Guide (DIG)*, the term IACS is generically used to represent industrial systems such as: Industrial Automation and Control Systems, Process Automation System, Process Control System, Supervisory Control and Data Acquisition. IACS benefit greatly from the transition to modern Ethernet and IP networking technologies from the vendor-optimized networks typically used in the past. New services and streamlined efficiency result when the information contained within the IACS is available and shared throughout the larger enterprise. Access to existing manufacturing information may be gated by disparate, proprietary, and closed systems as the move to open systems continues. Manufacturers and their industrial suppliers are discovering that standard communication and uniform networking of an IACS is the key to optimized services, greater visibility, and lower total cost of ownership (TCO). They are starting to embrace standard information technology, particularly standard Ethernet and standard IP, for IACS networking environments.

Although IACS vendors recognize that Ethernet and the IP protocol suite are the de-facto networking standards in IACS environments, full adoption of standard Ethernet and IP is still very much a work in progress. The pace of progress can be attributed to the aversion to disrupting existing systems, the accounting realities of fully-depreciated assets, legacy migration and the general ebb and flow of manufacturing investment cycles. Despite these challenges, industrial Ethernet is being deployed today on a broad scale. The rate of global adoption will continue to increase with greater application and end-device support from an increasing number of industrial equipment suppliers offering industrial Ethernet products.

Cisco and Rockwell Automation believe standard Ethernet and IP networking technology offers value inside industrial operations when the technology is part of larger integrated, IACS architectures. Cisco calls this the Ethernet-to-the-Factory (EttF) architecture. Rockwell Automation calls this Integrated Architecture. The Converged Plantwide Ethernet (CPwE) architecture joins these architectures.

The purpose of the CPwE architecture, a set of manufacturing focused reference architectures, is to help accelerate the successful deployment of standard networking technologies and convergence of manufacturing and enterprise/business networks. This solution architecture and relevant design and implementation guidelines will help provide confidence and background necessary to successfully deploy standard networking technologies and integrate IACS and business networks. This CPwE solution architecture must be tailored to support IACS. By adopting the solution architecture, the manufacturing process will operate at higher levels of performance, efficiency and uptime than under the previous solutions. At the same time, the solution must also safely and securely integrate the IACS into the broader manufacturing environment; only at this point will all the benefits be available to the manufacturing enterprise.

Introduction

Description and Justification

Manufacturing companies are increasingly expanding their global operations to address new opportunities and reduce operational costs. They are also seeking to continuously improve efficiency and drive down costs for existing facilities and processes. In fact, a recent study by Aberdeen (May 2009) noted that reducing costs is identified as by far the greatest business pressure of 63 percent of manufacturers.

Achieving these goals of globalization and operations excellence requires increased connectivity between IACS and business systems for real-time visibility to information and effective collaboration to:

- Ensure consistent quality and performance across global operations
- Balance manufacturing with demand to optimize material usage and asset utilization
- Improve and meet regulatory compliance

- Implement more flexible and agile manufacturing operations to respond to rapidly changing market conditions
- Meet demanding requirements and metrics for on-time delivery through reduced MTTR and increased OEE
- Reduce the cost of design, deployment, and support of manufacturing and IT systems at global manufacturing plants.
- Improve response to events that occur on the plant floor, regardless of location IACS manufacturers are currently falling short of these objectives. The key to resolving this problem is better access to information. With a constant flow of data, companies can develop more efficient ways to connect globally with suppliers, employees, and partners, and to more effectively meet the needs of end customers.

The key to achieving these goals is better access to information. With a constant flow of data, manufacturers can develop more efficient ways to connect globally with suppliers, employees, and partners, and to more effectively meet the needs of their customers.

The industrial manufacturing environment was 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 IACS-optimized protocols, specific operating requirements, and separate staffs, manufacturers were also struggling to evolve. Whether their IACS is 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 converging their IACS networks with their enterprise networks. When doing this, manufacturers encounter a number of challenges, such as the following:

- Reliability—As manufacturing operations become globally integrated, manufacturers are challenged to provide consistent access to data while making the manufacturing environment flexible. Security, availability, and asset use are critically important to manufacturing companies because IACS equipment is mission-critical, and efficiency is important to remain competitive.
- Cost—Legacy IACS, although often fully depreciated in existing manufacturing environments, can be difficult to integrate with the enterprise and can be costly to operate due to the multiple networks in use that require management, training, integration, gateways, spares, etc.
- Product design integration—Limited access to local subject-matter experts constrain collaborative manufacturing, impacting the ability to quickly respond to events, collaborate with engineering on new products and increasing cost to resolve problem.
- Service integration—In an effort to provide differentiated service, manufacturers are struggling to create systems to capture and incorporate genealogy data about their products.
- Data interaction and management—Incorporating real-time plant productivity and operational data into manufacturing execution systems (MES), customer relationship management (CRM), supply chain management (SCM), and other enterprise resource planning (ERP) systems restrict and constrain the ongoing move to service-oriented architectures.
- Partner connections—With an aging and decreasing workforce and increased manufacturing complexity, manufacturers are trying to find ways to leverage relationships with IACS vendors to support their plant floor applications.

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

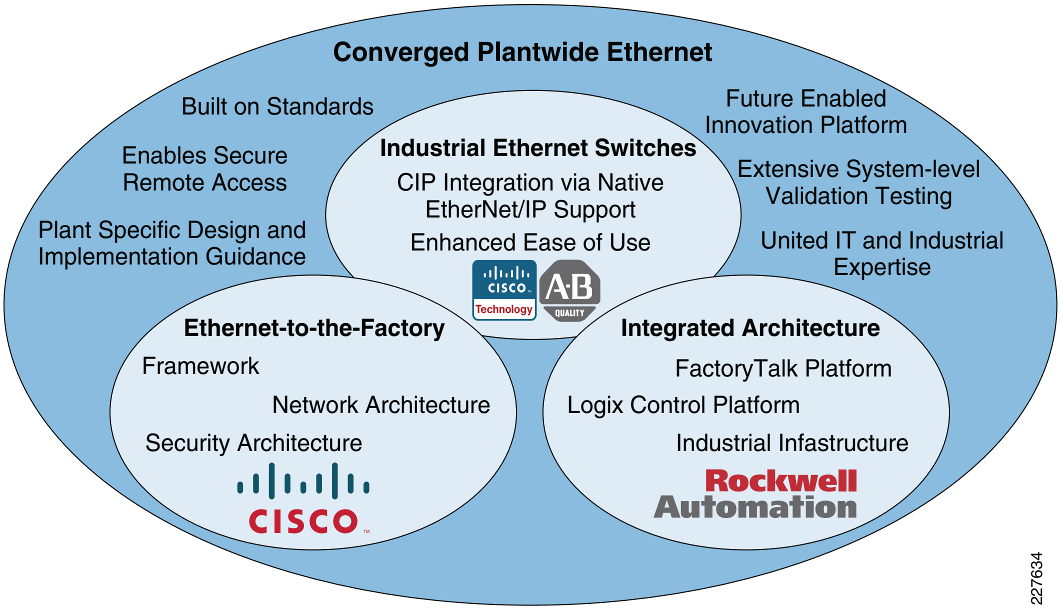
- Realize significant cost savings—Standard Ethernet and IP network technology with a broader base of IACS suppliers, resources and innovation are more likely than existing IACS networking technologies to give manufacturers a significantly lower total cost-of-ownership (TCO). On top of this, savings generated from better integration, easier management and the ability to operate more applications on one network create significant costs savings to the business.
- Simplify Maintainability—Legacy IACS network technology is becoming more complex to maintain than standard Ethernet and IP networking technology. Not only are resources competent in standard Ethernet and IP networking technologies more readily available, reliance on standard Ethernet and IP networking technologies offers more options to allow skilled personnel to securely access the plant systems.
- Enhance flexibility—Standard Ethernet and IP technology allows for rapid manufacturing gains with higher availability and better performance than legacy networking technologies. Additionally, new functionality and evolving capabilities in the IACS are focused on standard networking technologies.
- Increase efficiency—Standard Ethernet and IP technology improves visibility for business decisions and ability to transform business process due to integration of IACS and business systems.

Manufacturers recognize the benefit of using standard Ethernet and IP networking technologies in IACS networks, but there have been challenges that has slowed the adoption. One challenge has been the lack of consistent guidance and recommendations that are relevant to both IT and control engineers. Another challenge is that some IACS vendors continue to promote legacy or application-specific IACS networking technologies. The principle argument from these IACS vendors has been that deterministic and time-sensitive manufacturing environments require more than what standard Ethernet and IP technologies can deliver. Others question the inherent reliability and resiliency of Ethernet and IP technologies. Some have even asserted that standard Ethernet and IP networking technology in manufacturing environments makes manufacturers more susceptible to security risks. Modern, full-duplex, switched Ethernet networks offer real-time performance, including latency, jitter, and packet-loss avoidance capabilities that meet or exceeds the needs of IACS applications while offering better benefits than the older field-bus 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 are available for the older field-bus networks.

Cisco and Rockwell Automation's initial collaboration to outline the basics of IACS-to-business network convergence is documented in *Ethernet-to-the-Factory (EttF) Design and Implementation Guide* (versions 1.1 and 1.2). EttF outlined a logical networking framework built on industry standards. EttF also provided best practices and guidance for basic networking design and implementation. CPwE is the next phase of that collaboration and represents continuing IACS-to-business network convergence. CPwE builds upon EttF and more fully integrates the IACS using the Rockwell Automation Integrated Architecture.

Figure 1-1 depicts the key characteristics of CPwE. The inner circles represent the foundation of CPwE: EttF, the Rockwell Automation Integrated Architecture, and the line of industrial Ethernet switches developed with the best of Cisco and Rockwell Automation technologies. The outer circle represents the capabilities and benefits of CPwE such as unified IT and industrial expertise.

Figure 1-1 CPwE Architecture


Converged Plantwide Ethernet
Built on Standards
Enables Secure Remote Access
Plant Specific Design and Implementation Guidance
Future Enabled Innovation Platform
Extensive System-level Validation Testing
United IT and Industrial Expertise
Industrial Ethernet Switches
CIP Integration via Native EtherNet/IP Support
Enhanced Ease of Use
CISCO Technology
AB QUALITY
Ethernet-to-the-Factory
Framework
Network Architecture
Security Architecture
CISCO
Integrated Architecture
FactoryTalk Platform
Logix Control Platform
Industrial Infastructure
Rockwell Automation
227634

CPwE is an architecture that provides standard network services to the applications, devices, and equipment found in modern IACS applications, and integrates them into the wider enterprise network. The CPwE architecture provides design and implementation guidance to achieve the real-time communication and deterministic requirements of the IACS as well as the reliability and resiliency required by those systems. By bringing the CPwE solution to market, Cisco and Rockwell Automation can help provide manufacturers the guidance needed to meet the challenges of a fully-integrated IACS and realize the business benefits standard networking offers.

Target Audience

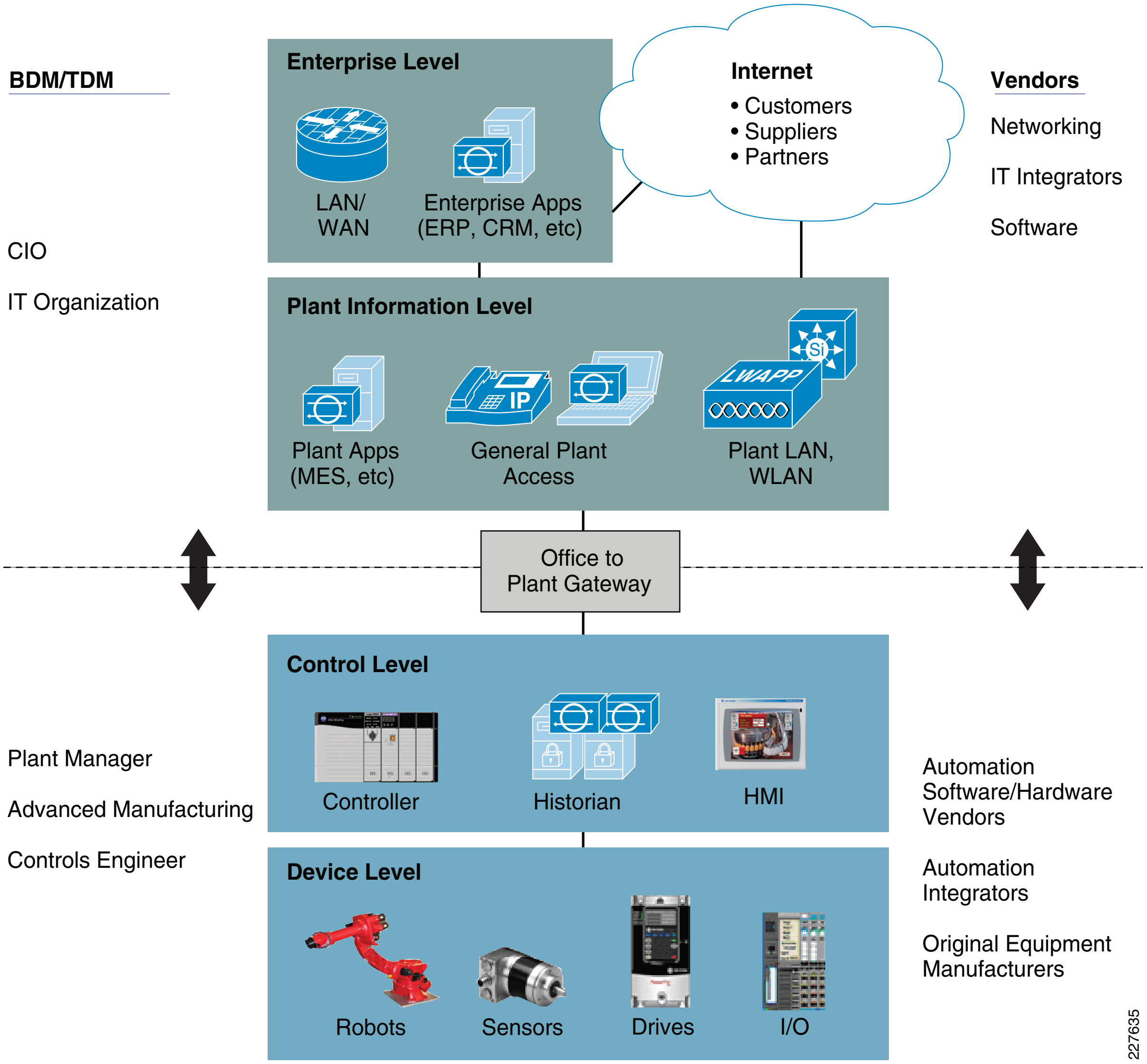
The CPwE solution is designed for industrial Ethernet applications. Although CPwE is applicable to multiple industries, this *DIG* focuses on the manufacturing industry, specifically manufacturers seeking to integrate or upgrade their IACS networks to standard Ethernet and IP networking technologies. These manufacturers are interested in the following:

- Lower the TCO of their current IACS network approach
- Integrate the IACS with the wider enterprise
- Take advantage of the networking innovations provided by using technologies employing industry standards

Decisions impacting IACS networks are typically driven by plant managers and Control Engineers, rather than the IT department. Additionally, the IACS vendor and support supply chain is different than those typically used by the IT department. This is driven by the different requirements of an IACS. That being said, the IT departments of manufacturers are increasingly engaging with plant managers and Control Engineers to leverage the knowledge and expertise in standard networking technologies for the benefit of plant operations.

The CPwE solution addresses the needs of and provides a common model for IT and manufacturing, such as plant managers and control engineers. Each camp has different perspectives and requirements for a successful CPwE implementation (see Figure 1-2).

Figure 1-2 Business/Technical Decision Makers—IT versus IACS



For the IT department, it is critical to understand the various IACS requirements and operating environment. For the plant managers and control engineers, a deeper knowledge of the capabilities and functioning of standard networking technologies is required. The CPwE 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 CPwE solution is developed and validated by Cisco and Rockwell Automation, leaders in their respective markets. The validated CPwE solution helps to increase success of manufacturers by more effectively addressing technical and business concerns of IT and Manufacturing organizations.

To summarize, the IACS and enterprise network convergence on which the CPwE solution is focused requires collaboration from both IT and manufacturing for successful implementation and operations. These organizations often have different objectives, ways of working and cultures that must be recognized. Each organization relies upon different partners, vendors and system integrators to implement and operate their solutions. IT may need its awareness levels raised concerning the differences and challenges posed by the manufacturing environment.

Plant Managers and Control Engineers

As mentioned above, plant management and control engineer are the key owners of the IACS that the CPwE solution targets.

Plant managers are business owners for the plant and are responsible for achieving manufacturing targets by ensuring plant reliability, uptime, and energy efficiency. Their performance is often measured by plant profitability, throughput, quality, OEE and return on assets. Technology decisions are made related to reliability, risk-free operation, environment fit, and company-wide standards.

Control Engineers are technical owners of the plant and are responsible for the design, implementation and operations of the IACS that operate the manufacturing facility. They are responsible for the IACS 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 management.

Key business drivers for plant managers and control engineers include the following:

- *Reliability*—The solution must support the operational availability of the manufacturing 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 employer or partner expertise in a secure manner.
- *Flexibility*—The ability to rely on commercial off-the-shelf (COTS) equipment, provided by a number of vendors and supported from a common expertise.

Key concerns for plan managers and control engineers include the following:

- *Performance*—Ability of the network infrastructure to meet the real-time communications requirements of the IACS.
- *Availability*—Both the ability to limit the impact on operations of upgrading or maintaining the IACS, and the reliability of the supported base network infrastructure features to handle outages with minimal impact.
- *Manageability*—Ease of configuring, maintaining, and repairing the IACS.
- *Compatibility*—How the network infrastructure supports various types of IACS communications (see the "IACS Communication Protocols" section on page 1-26) and the devices, controllers, human machine interfaces (HMIs), and applications already in use.

Both plant managers and control engineers typically rely on IACS vendors and partners with strong knowledge and track records in IACS. These vendors have varying degrees of capability and knowledge in deploying standard networking technologies and the relevant technical issues. Another objective of CPwE is to bring the relevant partners, such as system integrators and machine builders, up to speed on the availability and capabilities of industrial Ethernet and how to implement the technology in IACS environments.

CPwE enables the business drivers and addresses the key concerns relevant to plant managers, Control Engineers and the partner and vendor ecosystem that they rely upon for the IACS. The combination of Cisco and Rockwell Automation expertise, technologies, architectures, and validation work provides reliable reference architectures on which to base IACS network designs and implementations.

Manufacturing IT

Although IT managers are typically the owners of the enterprise network infrastructure, they are not typically the owners of the IACS network infrastructure for many reasons. However, they are increasing getting involved with plant to business integration at the application layer, convergence of the IACS and enterprise networks, deploying, and operating common network technologies in plants. In the past, they were 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 usually made decisions to focus on standardized solutions, to reuse whenever possible, and to reduce cost. There was 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 network convergence. To help overcome the cultural gap, the CPwE solution provides the following:

- Raises IT awareness of the particular challenges and requirements of IACS
- Outlines a solution and relevant design and implementation guidance that allows both plant and IT personnel to focus on a mutually-acceptable solution
- Develops a reference architecture standard on which to more quickly and assuredly deploy IACS networks
- Provides considerations for the use and deployment of common enterprise technology and tools whenever appropriate; for example, calling for standard IT external access technologies or applying standard network management tools and practices
- Addresses plant to enterprise network and application convergence, making it easier for IT to support wider business demands to be more aligned with manufacturing
- Pulls IT into the environment to deliver expertise and services based on their strength in standard Ethernet and IP networking technologies

Applications and Services Supported

The CPwE solution primarily supports IACS networks and their integration into the overall enterprise network. As noted earlier, IACS is a term that is meant to cover a large range of applications across multiple industries; Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), Programmable Automation and Logic Controllers (PACs and PLCs). There are other terms used for generally the same concept, for example Industrial Control System (ICS) is used in NIST and some ISA standards. IACS is used in ISA-99 Security standards. For the purpose of this *DIG*, Cisco and Rockwell Automation chose and standardized on IACS, but many other terms are used with similar meaning. IACS consists of the following:

- IACS devices, such as robots, sensors, actuator, and drives
- Human machine interfaces (HMIs) that provide visual status reports and control of the IACS
- 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 CPwE architecture focuses on the above items that support EtherNet/IP, which is driven by the Common Industrial Protocol (CIP) (see the "IACS Communication Protocols" section on page 1-26) and in particular are tested with Rockwell Automation devices, controllers, and applications.

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

- More alignment and focus on relevant aspects of deploying the IACS, for example the FactoryTalk™ integrated production and performance suite, the Logix multidiscipline Control Platform with RSLogix™ 5000™ and the IACS devices themselves
- 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 resiliency 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 Multiple Spanning Tree Protocol and Flex Links), and management of multicast traffic when multicast is chosen over unicast for IACS network traffic delivery
- IP address allocation, assigning, and related services (for example, DHCP, BootP, and DNS)
- Basic network management from both the IT and plant floor personnel's perspective, including the ease-of-use features available from the switch
- Network security for the IACS including Demilitarized Zone (DMZ), firewall, intrusion protection, endpoint security, and security monitoring, analysis, and response
- Secure remote access to the Cell/Area IACS network to improve service and support options and taking advantage of the interconnectivity that standard IT networking technologies allows.

These will be applied to network infrastructures with small (up to 50 Ethernet devices) to medium (up to 200 Ethernet devices) environments. Although larger environments will be addressed in future versions of this solution, the concepts and recommendations in this guide are envisioned to apply to those environments as well.

CPwE Solution Benefits

Manufacturers can realize the following operational benefits of the CPwE solution:

- Enables and simplifies convergence of the IACS network with enterprise networks to improve the flow and integration of manufacturing information into business systems.
- Enables remote access for engineers, partners, and IACS equipment vendors for diagnostics and maintenance. Increases efficiency and response time and enables IACS vendors to provide services to manufacturers that may have limited subject-matter expert (SME) resources.
- Help reduce risk, increase plant uptime and improve Overall Equipment Effectiveness (OEE) through validated reference architectures with a focus on network resiliency and application availability.
- Help reduce operating and capital costs by using open standards to eliminate the need to support multiple protocols in IACS networks and to provide manufacturing companies more options when purchasing IACS equipment.
- Integrates more quickly advances in networking technology that come from working with standard technologies (for example, voice, video, and security).

The integration of advanced technologies by leading vendors such as Cisco and Rockwell Automation provide 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 IACS and industrial networking expertise of Rockwell Automation.
- Providing architecture and terminology to support cultural and organizational convergence, as well as facilitate training and dialogue with IT and Control Engineers.
- Delivering end-to-end architecture with consistent technology, management tools, a common feature set, and software base making for stream-lined deployments and consistent management.
- Providing integrated security specifically configured for IACS networks to protect vital manufacturing assets, limit access to manufacturing 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 IACS network at the Cell/Area levels as the technology matures and the business requires.
- Simplifying deployment and helping to bridge the gap that often exists between IT and IACS networks by integrating and validating architectures with leading partners in the IACS 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 Rockwell Automation from vendors that have chosen to deploy solutions on the market that are not based on standard Ethernet and IP.

CPwE Solution Features

IACS 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 the IACS in general. In the move towards industrial Ethernet, many of these design features still apply, although the importance sometimes shifts. For example, with standard Ethernet and IP technology industrial networks, security is a pressing issue, particularly if there is no restricted segmentation between the IACS and the larger business system. This section defines the following seven key features that manufacturers expect as best practices:

- Industrial characteristics
- Interconnectivity and interoperability
- Real-time communication, determinism, and performance
- Availability
- Security
- Manageability
- Scalability

This DIG provides details on why and how to deploy these features. The manufacturing industry, and especially plant managers, Control Engineers, and their partners and vendors, are looking for simple guidelines and recommendations. Each chapter in this DIG highlights key recommendations and steps to follow when designing and implementing industrial Ethernet for and IACS application.

Industrial Characteristics

A key differentiator of the IACS from typical enterprise applications is the environment. The IACS end-devices and network infrastructure are located in harsh environments that require compliance to environmental specifications such as IEC529 (ingress protection) or National Electrical Manufacturers Association (NEMA) specifications. The IACS end-devices and network infrastructure may be located in physically disparate locations (up to miles away), and in non-controlled or even harsh conditions in terms of environmental considerations such as temperature, humidity, vibration, noise, explosiveness, or electronic interference.

The CPwE solution does not focus on environmental requirements and whether the IACS network infrastructure meets those requirements, outside of noting that this is an important consideration when choosing the network infrastructure. Additionally, the physical layer infrastructure is also driven by the physical requirements of the environment, with special consideration given to the potential for high noise. For physical layer considerations, refer to the ODVA's *EtherNet/IP Media Planning Guide* at the following URL:

http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf

This CPwE solution does focus on how the network infrastructure can support spatial challenges in an IACS network by supporting a number of topology options, thereby adapting to the industrial characteristics of the IACS.

The physical layout of the IACS equipment impacts the network topology for IACS networks. Unlike IT networks, which are largely redundant star topology networks, IACS networks have significant physical requirements that drive the use of topologies such as bus, linear, star and ring. In plants with long manufacturing lines, or equipment with long runs and interconnected operations (such as a printing press), 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. Given these cost considerations, many manufacturers choose to implement a ring topology rather than a redundant star topology where network resiliency is a requirement. In many cases, the IACS network utilizes a combination of topologies, with large rings connecting multiple star-based Cells/Areas.

Based on these considerations, the design guidelines provide information regarding the trade-offs between the various topologies to help manufacturers, system integrators and machine builders to make appropriate design decisions. Because of their significant use in manufacturing, bus topologies are discussed, as well as the associated trade-offs between linear, ring, and redundant star topologies (such as availability, and so on). Note that, although the linear topology is considered, Cisco and Rockwell Automation recommend ring or redundant star topologies for network infrastructure due to the resiliency they offer and therefore support higher availability and uptime.

For a summary of the advantages and disadvantages of each topology, see "Cell/Area Topology Comparison" section on page 3-27.

Figure 1-3 shows a redundant star topology.

Note 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 Redundant Star Topology

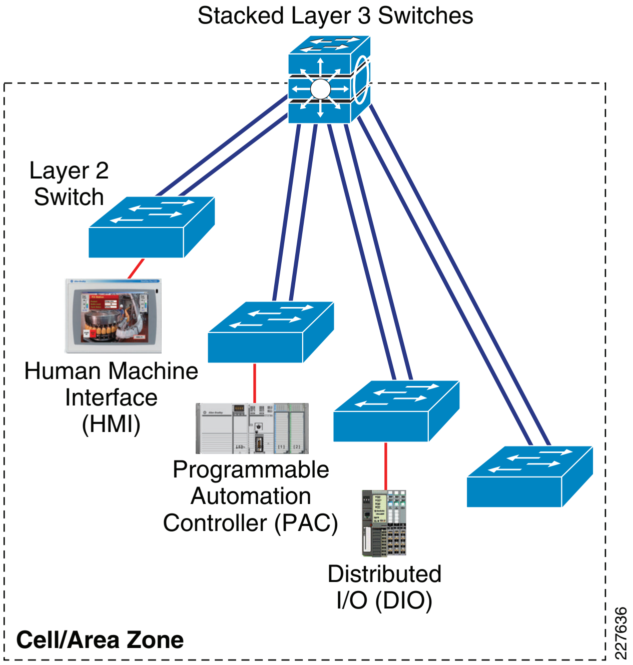


Figure 1-4 shows a ring topology.

Figure 1-4 Ring Topology

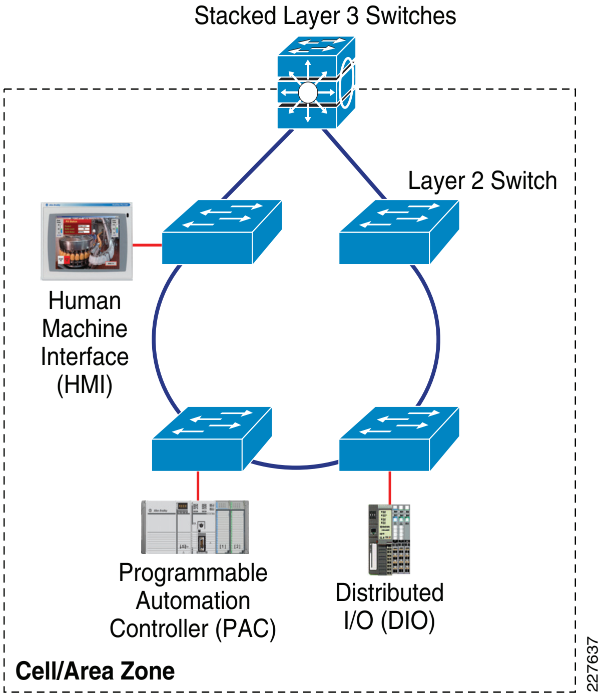
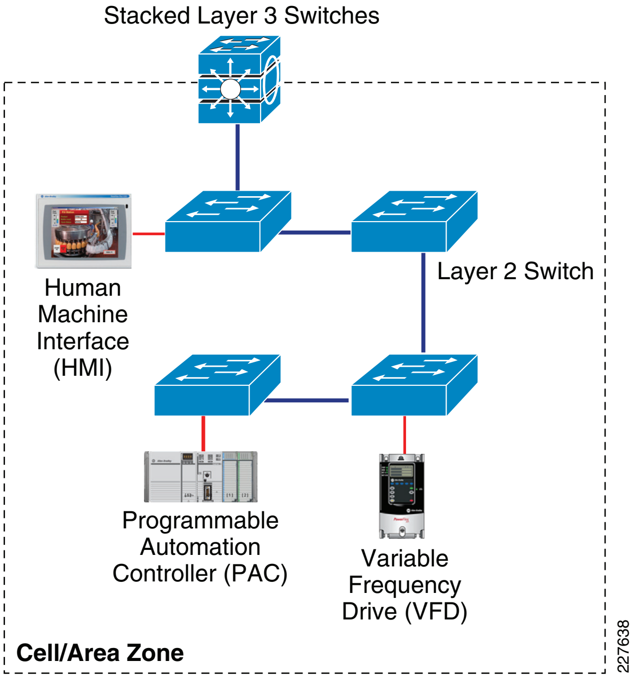


Figure 1-5 shows a bus topology.

Figure 1-5 Bus Topology


Stacked Layer 3 Switches
Layer 2 Switch
Human Machine Interface (HMI)
Programmable Automation Controller (PAC)
Variable Frequency Drive (VFD)
Cell/Area Zone
227638

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

- Choosing a topology that meets the performance, cost, and spatial requirements of the IACS 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, linear, trunk and drop topology, or a hybrid.
- Use ruggedized/hardened network devices in the plant environment where needed, but consider using non-industrial routers, switches, and firewalls where appropriate to reduce cost.
- The number of IACS 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.

Interconnectivity and Interoperability

The ability to interconnect and interoperate a wide range of IACS network devices and applications through a common, standard network infrastructure is a key goal for IACS networks. The interconnectivity and interoperability feature also applies to network infrastructure devices themselves. Standard Ethernet and IP network technologies offer the best opportunity to do such as the barriers for IACS vendors to integrate this into their product is low and the concepts and technology are widely available. This CPwE solution will focus on the use of standard Ethernet and IP networking technologies to deliver maximum interconnectivity and interoperability. Interconnectivity suggests that the IACS network devices can communicate using standard protocols at Layers 2, 3, and 4 (Ethernet, IP and TCP/UDP). Interoperability suggests that the IACS network devices can interoperate using standard, common protocols at Layer 7 (application). IACS network devices with different application layer protocols may not interoperate without some gateway device/service to perform an application layer translation. This CPwE solution is based upon the use of CIP as the common application layer protocol for IACS network interoperability employing EtherNet/IP as the IACS network.

The TCP/IP protocol suite with the CIP application layer protocol helps ensure that IACS devices from a variety of vendors will communicate and work together. Additionally, conformance testing from such organizations such as the ODVA certifies that EtherNet/IP devices from various vendors communicate and interoperate. The TCP/IP standards outline a wide range of features and functions. This solution will identify key features and functions from the TCP/IP suite and describe how they can be implemented with the products from Cisco and Rockwell Automation. Therefore, in theory, the concepts, recommendations and implementations CPwE specifies should be applicable in a wide range of other vendor's devices and solutions.

The key TCP/IP protocols relevant to this solution are described in Table 1-1. The 7-layer OSI model is used to segment the various protocols and standards.

Table 1-1 Key TCP/IP Protocols

Layer	Name	Function	Key Protocol
4	Transport	Reliable network communication between end nodes,	TCP, UDP
3	Network	Path determination, routing	Internet Protocol v4 (IPv4), Internet Group Management Protocol (IGMP), DSCP, Internet Protocol Security (IPsec), OSPF
2	Data Link	Physical addressing, network topology, line discipline, error notification, ordered delivery of frames, and flow control	MAC, Ethernet (IEEE802.3), Spanning Tree Protocol, Virtual Local Area Networks (VLAN), Link Aggregation Control Protocol (LACP)
1	Physical	Media, signal and transmission protocol	Ethernet (IEEE 802.3) including 10, 100 Mb and Gigabit Ethernet in copper and fiber varieties

Chapter 3, "CPwE Solution Design—Cell/Area Zone" and Chapter 4, "CPwE Solution Design—Manufacturing and Demilitarized Zones" of this DIG describes how and why these protocols and standards are applied. Note that there are a range of other protocols involved in standard networking that are not mentioned here as they are either not relevant or are transparent functions of the IACS network infrastructure and end-devices. For more information on a complete set of standard networking features and functions, see Cisco's technology support library at the following URL:

http://www.cisco.com/cisco/psn/web/psa/design.html?mode=tech

By definition, industrial Ethernet (IE) networks should operate on standard Ethernet and IP networking technologies and infrastructure, although some industrial Ethernet networks, not considered within this DIG, incorporate proprietary technologies so that common infrastructure may not be used. However, standard networking technologies have a wide range of service and configuration options that need to be considered to effectively support the IACS application. As well, various industrial Ethernet protocols specify various networking features that then must be available to operate at required performance levels, not all of which are based upon openly available standards. The "IACS Communication Protocols" section on page 1-26 lists the relevant general industrial protocols and the corresponding industrial Ethernet versions. This solution architecture focuses on CIP, the application layer protocol for EtherNet/IP. Other network protocols are referenced (see the subsections on traffic flows in the "Cell/Area Zone" section on page 2-3 and "Manufacturing Zone" section on page 2-5).

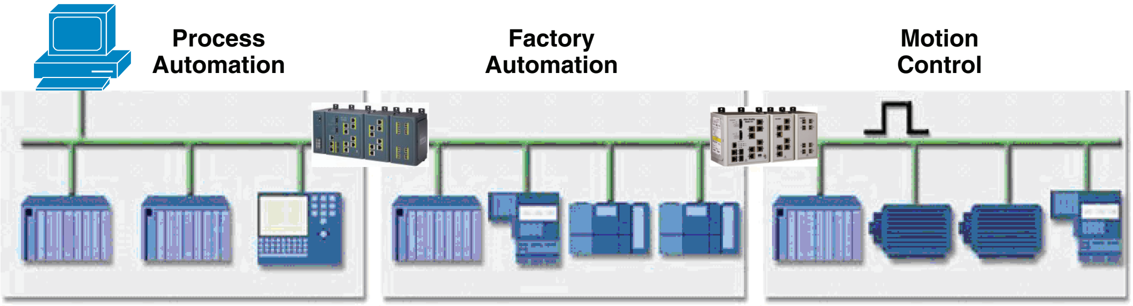
A key objective of the CPwE architecture is to interconnect standard EtherNet/IP IACS network devices and maintain interoperability with standard Ethernet and IP network technology infrastructure. This CPwE solution uses systems and infrastructure from Cisco and Rockwell Automation, but this solution could be applied using applications and infrastructure from other vendors.

Real-Time Communication, Determinism, and Performance

IACS networks differ significantly 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), significantly lower than typical Enterprise applications. Real-time communications help the IACS become more deterministic. Although the network plays a role in the deterministic nature of a system, a number of other factors, such as end-device latency and response time, are also involved. But the network has an important role, not just by sending packets quickly and consistently, but in the services it offers and supports, such as quality-of-service (QoS) and precision time. The capabilities of standard Ethernet and IP networks to support challenging real-time communications are described in this *DIG*.

IACS networks have different real-time communications requirements based on the type of application. Figure 1-6 represents examples of application requirements as developed by ARC Research in 2006. This is representative only. Figure 1-6 does not represent the testing and characterization results of the CPwE solution.

Figure 1-6 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 Application 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

227943

The CPwE solution provides design and implementation guidance to help achieve the real-time communications requirements of an IACS. Key considerations in achieving real-time communications include the following:

- Number of switches, routers, and amount of traffic in the Layer 2 network, all of which affects latency and jitter.
- Ratio of LAN switch ports to uplink switch ports based on traffic loads and patterns. Typically, this means using 10/100 Mbps for IACS 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 quality-of-service (QoS) parameters to meet the real-time requirements of various traffic flows.

Availability

Availability of the IACS has a direct correlation to the plant uptime and OEE of a manufacturing facility. Because the network is a key aspect of the overall system, these requirements translate directly to the IACS network. This CPwE solution outlines a number of features that not only maintain IACS network availability in the case of link-loss, device failure and other outages, but once an outage occurs, features that enable quick restoration of IACS network services to re-start manufacturing as quickly as possible. CPwE outlines a number of IACS network traffic or application types and what requirements they have for network resiliency. These network capabilities were then tested to validate that those requirements were met, with documented results and best practices to help determine what options are available for a variety of IACS application types.

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 quick enough and the cost associated with redundant wiring have often led to non-redundant topologies being implemented in IACS networking environments. The CPwE solution outlines the capabilities so as to let manufacturers, system integrators and machine builders make decisions on the level of network availability needed for the overall system.

High availability considerations are identified in each aspect of the CPwE 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 IACS network infrastructure, such as routers, switches, and firewalls.
- Using advanced network resiliency and convergence techniques to improve availability, such as EtherChannel/LACP, Multiple Spanning Tree Protocol (MSTP), Flex Links, and 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.
- Integration of the network device into the IACS application to better identify and diagnose issues when they do occur.
- Features and services to allow the quick replacement of failed devices with minimal or no configuration of the replacement device.

Security

IP networking facilitates interconnection of the IACS network with the enterprise network. Many industries have implemented enterprise applications for more efficient manufacturing, 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 IACS network to the enterprise network exposes the security risks of the Internet and enterprise network to the IACS application. Mitigating these risks may be more difficult and more critical than in the enterprise network because of the higher requirement for availability in an IACS and the sensitivity of these systems to different disruptions. Of the three security properties of confidentiality, integrity, and availability, IACS applications are primarily concerned with availability and integrity. Many of the applications that IACS networks support cannot be stopped or interrupted without serious physical damage or loss of productivity with measurable financial damage. On the other hand, confidentiality and integrity are the primary design considerations for enterprise networks. For example, it is preferable for an ecommerce 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 IACS applications. Building secure and reliable IACS networks utilizing Ethernet and IP has been a challenge.

Standards bodies such as ISA-99 and NIST are continually developing security design axioms, and there is an emerging consensus on what a secure IACS architecture should provide. This includes an IACS 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 CPwE architecture are as follows:

- Control data flows between different IACS levels (ACLs, firewall rules, etc).
- Prevent direct communication between IACS and enterprise applications.
- Restrict real-time manufacturing data to the IACS network.
- Restrict enterprise access to the mirror version or copies of IACS data to the DMZ.
- Authenticate and authorize user access based on the level within the IACS network and the role (read/read-write/local/remote/vendor/partner).
- Control rogue access to switches inside the IACS network (port level MAC-address controls, administratively shutdown unused ports, etc).
- Control which IACS 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 IACS network.
- Detect and mitigate malicious traffic originating from the corporate IT network.
- Secure connectivity for remote access to IACS 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.

This CPwE solution will incorporate these security best practices into the design and implementation guidance for IACS networks. A security risk assessment is recommended to determine the appropriate level of risk mitigation required for a specific situation. The CPwE solution incorporates design and implementation guidance to help secure remote access to the Cell/Area IACS network.

Manageability

Manageability is a key consideration for an IACS network. Individuals with a basic level of networking skills should be able to manage and monitor the network. On the other hand and with more regular occurrence, IT professionals are getting involved with maintaining and support IACS networks. The IACS networking solution needs to accommodate manageability via existing tools and procedures by plant personnel without deep networking expertise as well as manageability via enterprise-level network management tools and procedures by IT network experts.

Key manageability concerns include the following:

- Configuration of switches using IT tools such as the command-line interface (CLI) and IACS tools such as RSLogix™ 5000 and Device Manager.
- Single switch management utilizing a single GUI such as RSLogix 5000 and Device Manager, multiple switch management utilizing a single GUI such as Cisco Network Assistant.
- 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 IACS 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 IACS servers and clients.
- Standardizing hardware and software elements wherever possible.
- Driving the integration of basic network administration into the existing applications based on various IACS network protocols.

Scalability

An IACS may come in a wide range of sizes, from small machine builder solutions to the extremely large plant complexes (for example, an automotive plant). The IACS may include only a small number of network infrastructure devices (up to 50) to multiple 10,000s. The IACS solution architecture concepts and recommendations need to be applicable to that range, noting the considerations for various sizes.

This version of the CPwE 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 IACS sizes. Specific considerations for extremely small, pre-built systems (such as machine builders) or large to extra large implementations were left for future versions of the CPwE solution architecture. The basic concepts in this guide are applicable to the range of IACS.

Key scalability considerations include the following:

- Cost
- 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 CPwE Solution

This phase of the CPwE introduces basic network architectures based on standard technologies to provide services to an IACS through design and implementation guidance to implement an IACS network.

Key aspects of this phase of the CPwE solution include the following:

- Wired solutions for the IACS.
- The CPwE logical framework and solution are applicable for small to large IACS environments, but the testing and specific design recommendations were made based on small (less than 50) to medium (less than 200) network infrastructure devices.
- Key technical considerations such as the following:
  - Topology
  - Real-time communications
  - Networking functions of the OSI Layers 2 and 3 configuration including basic routing protocols
  - Insulation and segmentation including VLANs and DMZ design
  - Multicast traffic handling, including IGMP
  - Quality-of-service (QoS)
  - Redundancy and resiliency (including application of the standard MSTP EtherChannel/LACP, and Flex Links)

  - IP address allocation, assignment, and related services (for example, DHCP and DNS) in a manufacturing perspective
  - Basic network management
  - Network security for the IACS, including DMZ, firewall, intrusion protection, endpoint security, and security monitoring, analysis, and response
- Design and implementation is based on EtherNet/IP (driven by CIP application layer)

Phase 1—Ethernet-to-the-Factory (EttF)

Phase 1 (Versions 1.0 - 1.2) of EttF was the initial jointly developed IACS network architecture by Cisco and Rockwell Automation. The solution was mainly focused on network considerations and recommendations, albeit to support IACS applications. Phase 1 introduced the Six-Level logical Plant Architecture as the Reference Model for the solution. Phase 1 features of the solution, including:

- Key solution features (for example, real-time communication, availability, security) and described how they are supported by various aspects of the solution.
- Design and implementation guidance for key zones of the IACS network: Cell/Area, Manufacturing, and DMZ including the key network functions required.
- Test description and results to support recommendations and to be used as guidance for estimating performance of key network characteristics such as high availability and resiliency.

Phase 2—Converged Plantwide Ethernet (CPwE)

Phase 2, CPwE, builds upon and extends the Phase 1 EttF solution. CPwE represents further integration of the standard Ethernet and IP network infrastructure with the IACS applications as well as the convergence of IACS and enterprise networks. CPwE uses the same key structures and features as EttF, with modifications and additions. The CPwE solution will continue to focus on IACS applications using EtherNet/IP. The key areas of addition and extension include the following:

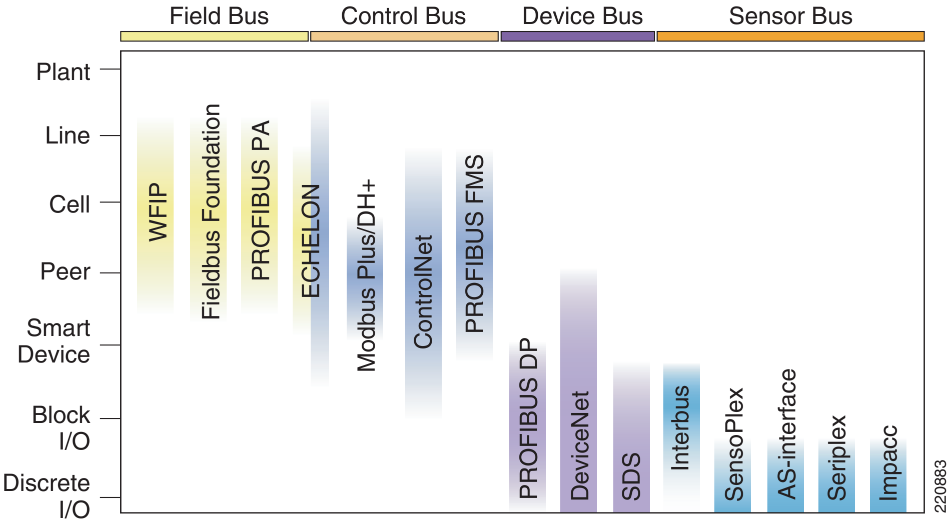
- Enhanced industrial Ethernet switching infrastructure. Replace the Cisco 2955 industrial switch with the Rockwell Automation Stratix 8000™ and highlight key new features including:
  - Additional configuration options, for example 6 to 26 port configurations with a mix of both fiber and copper ports.
  - Ease-of-use features such as pre-defined Smartports for easy setup and configuration and removable Compact Flash memory for easy switch replacement.
- Enhanced Cell/Area zone design options and detailed resiliency testing for both ring and redundant star topologies to support a variety of IACS applications including support for CIP Implicit I/O and CIP Explicit informational messaging.
- Design and implementation of secure remote access to Cell/Area IACS networks.
- Integrate the Rockwell Automation FactoryTalk production and performance suite into the solution design.
- Integration of the industrial Ethernet switches into the IACS application (e.g., FactoryTalk, RSLinx Data Servers and Logix control platform applications) via EtherNet/IP protocol support for enhanced manageability.

Industrial Automation and Control System (IACS)

History of IACS Networks

From the beginning, manufacturing environments have relied on numerous technologies to enable communication at the plant or Cell/Area levels. Typically, the technologies deployed were purpose-built and vendor-specific. Figure 1-7 provides a list of some of the types of protocols used in manufacturing environments. A wide range of protocols were developed for a variety of automation and control scenarios as well as types of devices.

Figure 1-7 Legacy Control Protocols Overview (Source: David Humphries, ARC)



IACS networks as a whole have been migrating 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 manufacturing reporting with legacy fieldbuses
- Expense of using vendor-specific IACS network technology
- Frustration in procuring IACS devices because of the confusion related to various fieldbus technologies
- Complexity of integrating various technologies into the overall IACS

Standard Ethernet and the IP protocol suite are now the defacto standard for many IACS protocols. 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.

IACS 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 dictate a complete physical media upgrade when migrating from one network 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/ST or LC connectors for fiber optic cables. Sealed connectors such as M12 are required for IP67 applications. The benefit of industrial Ethernet, once physically installed, is connectivity of IACS devices from multiple IACS vendors.

Cisco and Rockwell Automation recommend readers review the *ODVA's EtherNet/IP Media Planning Guide* (http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf).

Typical Ethernet speeds are 10Mbps, 100Mbps, and 1Gbps. 10 Gbps is mainly being deployed in enterprise-wide backbone networks. IACS installations rely upon 10Mbps or 100Mbps Ethernet for IACS devices while Gigabit Ethernet is appearing in industrial Ethernet backbones.

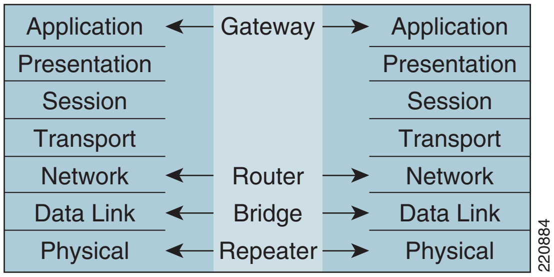
The physical layout and communication requirements of a manufacturing environment dictate how various standard Ethernet resources are physically connected. Typical Ethernet environments have full-duplex connection via a redundant star topology. Other options are possible such as ring, trunk and drop, and linear. Specific operating constraints when using Ethernet in these other models are discussed in Chapter 3, "CPwE Solution Design—Cell/Area Zone."

Networking Equipment

Note As IACS networks adopt standard Ethernet and IP technologies, they 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 layer communication protocol is in use. For example, Layer 3 refers to the Network layer of the OSI model, and in standard networking refers to the IP protocol.

Figure 1-8 shows, various types of devices working at different layers of the OSI model and common devices that perform representative interconnect functions.

Figure 1-8 Open System Interconnection (OSI) Reference Model



Many early IACS Ethernet networks used simple, inexpensive repeaters (also known as hubs) to connect IACS devices 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 IACS 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-controller communication or HMI polling)."*
>
> (Source:http://www.cisco.com/warp/public/779/smbiz/languide/p4.html)

The next advancement in IACS industrial Ethernet network design was the use of switches; a type of multi-port Layer-2 bridge. Switches can segment networks into virtual LANs (VLANs) to separate collision domains. Ethernet switches also typically have a fast internal backbone, which helps eliminate collisions among data packets. Collisions are eliminated for IACS network devices directly connected to switches in full-duplex mode. 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 and prioritization capabilities, meaning that the switch can provide more granular quality-of-service (QoS) for IACS networks. One example is the management of multicast traffic. Management of the multicast (rather than treating it as broadcasts as unmanaged switches do) significantly reduces the number of messages that end-devices and IACS network infrastructure must process, leading to better network and device performance. As another example, by assigning a priority to time-sensitive data, managed Ethernet switches can prioritize that traffic above lower-priority data. This ensures that high-priority IACS 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 IACS networks today. Both Cisco and Rockwell Automation highly recommend the use of managed switches. For further details on managed versus unmanaged switches, see the "Topology Options and Media Considerations" section on page 3-21.

In some cases, Layer-3 switches or routers are used in manufacturing environments. Layer-3 switches or routers forward information between different VLANs or subnets. They use information in the IP header (Layer 3) to do so. Regardless of the specific layer being connected, switches provide IACS networks with many of the safeguards that were realized by the natural separation inherent in existing IACS-optimized networks.

The specifics of how a Layer-2 switch is used compared to a Layer-3 switch, how to implement multicast management, and how QoS can be implemented are addressed in the "Cell/Area Zone" section on page 2-3.

IACS Network Devices

Many types of devices are used in IACS applications. Some are small, simple, single-function sensors or input/output devices (e.g., a light or on-off switch), while others are feature-rich, programmable automation controllers (PACs). The breadth and depth of available devices is driven primarily by IACS vendors and their partners and suppliers. Figure 1-9 shows some of the various types of devices connected to an IACS network.

Figure 1-9 Industrial Network Devices

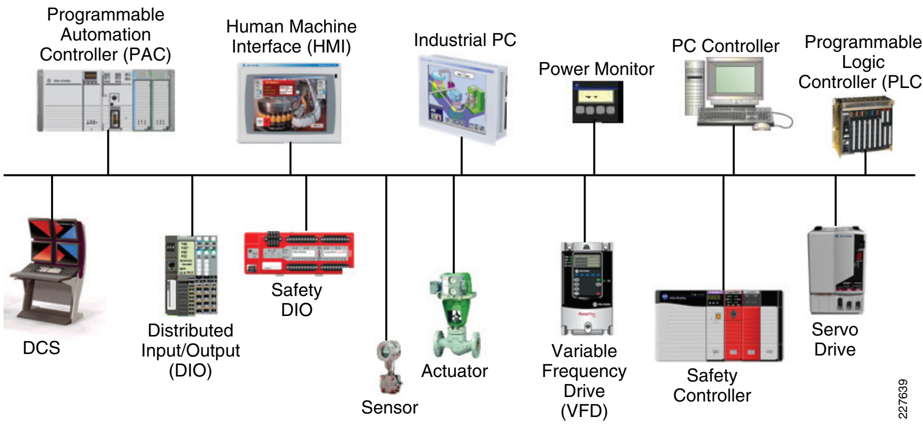

Programmable Automation Controller (PAC)
Human Machine Interface (HMI)
Industrial PC
Power Monitor
PC Controller
Programmable Logic Controller (PLC)
DCS
Distributed Input/Output (DIO)
Safety DIO
Sensor
Actuator
Variable Frequency Drive (VFD)
Safety Controller
Servo Drive
227639

Table 1-2 identifies the IACS and network infrastructure devices used within the architecture diagrams contained throughout this *DIG*, such as Figure 1-5.

Table 1-2 IACS Network Components

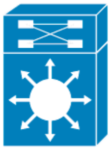
Device Icon	Description	Product/Platform
	Layer 2 Industrial Ethernet access switch	Allen-Bradley Stratix 8000 or Cisco IE 3000 Industrial Ethernet switch in a variety of port configurations Catalyst 2960 switch for non-industrial, rack mount environments, in a variety of port configurations
	Multilayer distribution switch	Catalyst 3750G in a variety of port configurations
	Router/Switch	Catalyst 4500 or 6500 in a variety of configurations
	Firewall	Adaptive Security Appliance (ASA) 5500 series
	Programmable Automation Controller (PAC)	Allen-Bradley ControlLogix System
	Safety Programmable Controller	Allen-Bradley GuardLogix System

Table 1-2 IACS Network Components (continued)

Device Icon	Description	Product/Platform
	Programmable Automation Controller (PAC)	Allen-Bradley CompactLogix System
	Programmable Automation Controller (PAC)	Allen-Bradley CompactLogix System
	Variable Frequency Drive (VFD)	Allen-Bradley PowerFlex Drive
	Human Machine Interface (HMI)	Allen-Bradley PanelView Plus
	Distributed Input/Output (DIO)	Allen-Bradley POINT I/O
	Safety Distributed Input/Output (DIO)	Allen-Bradley CompactBlock Guard I/O

Older lower-level IACS network devices tend to use specific IACS network protocols and are capable of only low data rates and volumes, albeit with deterministic characteristics. More advanced IACS devices have internal logic optimized for I/O control with the ability to support higher data rates and volumes. Many of these newer IACS network devices now come standard with more communication options including standard Ethernet and IP.

The trend with IACS network 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 IACS applications. 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. Regardless, there is and will continue to be a place for simple, low cost, and lower capability devices in IACS applications. 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 IACS network using high performance CPUs. By using fanless and diskless PCs with features such as 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, IACS 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 configuration environment both for vendors as well as manufacturers. This migration has coincided with the overall general trend in the software industry towards Internet browser-based technology. This offers IACS vendors the ability to embed web interfaces directly into IACS network 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 the IACS is discussed in *Chapter 2, "Converged Plantwide Ethernet Solution."*

IACS Communication Protocols

Communication Model

The communication messaging model in IACS environments has only loose ties to traditional client-server or peer-to-peer IT models. Unlike the typical IT environment, standard Ethernet and IP IACS network communications have different patterns, loads, and frequencies required by the manufacturing process they support. Standard IACS network communications are also driven by status polling between devices, cyclic data transfer, or change of state message patterns. The different requirements of the layers previously discussed have led key IACS 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 controllers (Levels 0-1) and information traffic within the upper level applications down to the controller (Level 1). This differentiation is made to meet the stringent requirements at these lower levels (see the "Industrial Automation and Control System Reference Model" section on page 2-1). However, the models can differ greatly at the Cell/Area levels. One example is the producer-consumer model applied in the ODVA Common Industrial Protocol (CIP). This model describes how devices "produce" data to be "consumed" by other devices; in particular, the controllers that take action on their data and control their behavior. These models are incorporated into the IACS 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-informational messages and Implicit I/O messages. In an Explicit message, the action is explicitly defined in the message; for example, read the value of a variable. Explicit messaging is a request/response, client/server-like protocol typically used for "information" and administrative messaging and is implemented over the Layer 4 TCP protocol. Explicit messages are information messages used for additional device configuration and acquisition of device diagnostics. Explicit messages are highly variable in both size and frequency based on configuration and application.

Implicit I/O messages are typically used for cyclic, input/output messages to/from controllers and devices. In Implicit I/O messages, the data is implied; the communicating parties inherently know how to parse the message content because of contextual knowledge. Implicit I/O messaging or real-time IACS messages are sent at requested packet intervals (RPI), and although the size can vary, it is consistent after the configuration is set and is generally smaller than Explicit messages. Implicit I/O messages contain IACS 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 I/O traffic, the UDP protocol is used (either unicast or multicast) to minimize processing resources and time on the end-device.

Network traffic in IACS 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 DIG, Cisco and Rockwell Automation has 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 IACS networks. For example, the CIP optional use of multicast traffic generates different network configuration considerations. However, these differences are focused on specific areas of an IACS network where the networking requirements are significantly different than standard IT networks. Chapter 2, "Converged Plantwide Ethernet Solution,"introduces a framework and model for IACS networks to clearly describe these areas and the network implications to be considered when designing and implementing the systems.

IACS Protocol Overview

IACS networks utilizing standard Ethernet and IP 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), and other standard protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and the Simple Network Management Protocol (SNMP). All these are established within IT and are being implemented to varying degrees, unchanged in IACS applications.

The goal of an Ethernet and IP IACS network is to ensure that the application layer protocol of choice, assuming it is based on standard Ethernet and IP is supported to meet the operating constraints of the IACS application.

Table 1-3 shows a list of some protocols that support or partially support standard networking.

Table 1-3 Key IACS Networks & Protocols

Fieldbus Protocol	Ethernet Implementation	Leading Vendors	Standards Body	Application
DeviceNet, ControlNet, CompoNet	EtherNet/IP (EIP)	Rockwell Automation, Cisco, Schneider (EIP), Omron, Eaton	ODVA	Industrial automation (process, discrete, safety) control, motion control
PROFIBUS DP, PA, and so on	PROFINET CBA, I/O, IRT, and so on	Siemens	PROFIBUS Foundation	Industrial automation process control
Modbus	PROFINET CBA, I/O, and IRT	Schneider	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
EtherCAT	EtherCAT		EtherCAT Technology Group	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 IACS networks. Of these protocols, EttF and now CPwE focuses 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 different messaging frameworks that dictate the type of traffic and traffic patterns found in the IACS network.

Table 1-4 outlines features of different industrial Ethernet protocols and briefly describes some of the key characteristics of the various protocols.

Table 1-4 Various Features of Different Industrial Ethernet Protocols

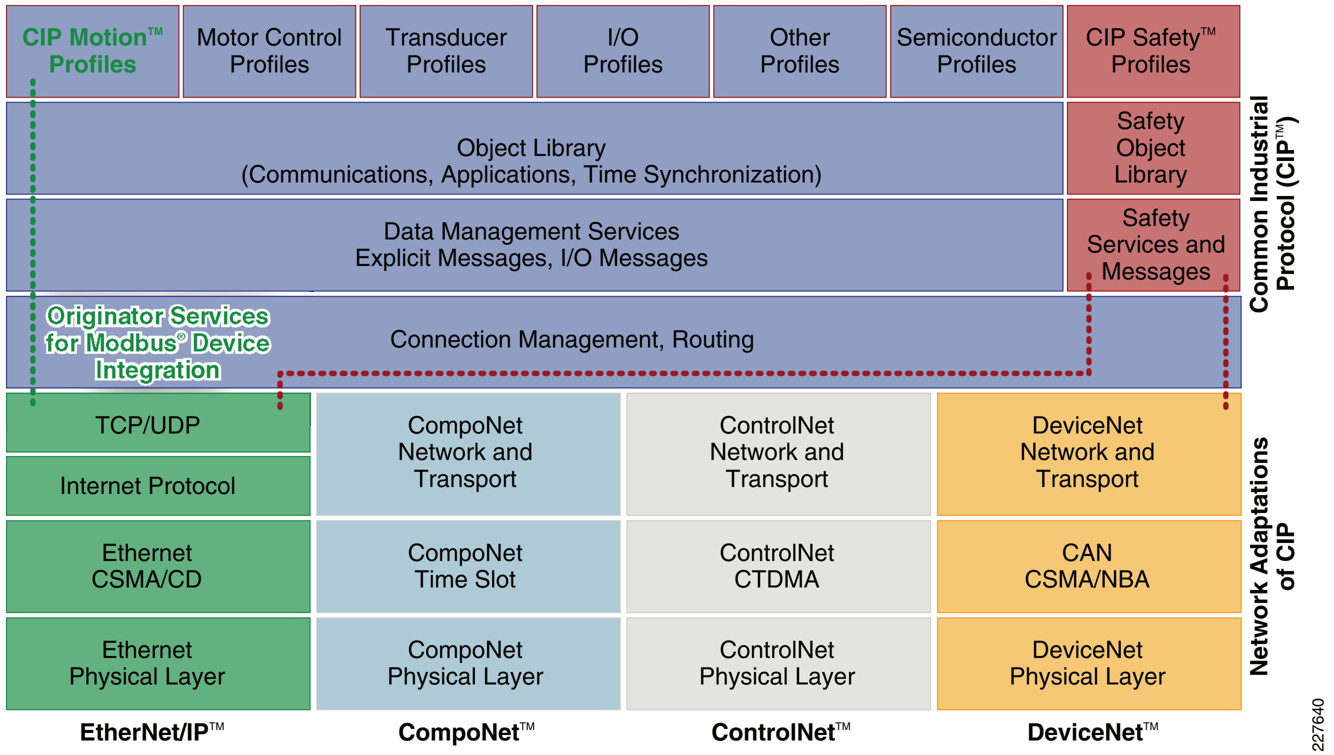
Industrial Ethernet Protocol	Encapsulated Telegram	TCP/IP UDP/IP	Port Usage	Profile/Object Support
EtherNet/IP	Common Industrial Protocol (CIP)	TCP/IP Explicit UDP/IP Implicit	44818 2222	Yes
Modbus/TCP	Modbus	TCP/IP	502	Yes
PROFINET CBA PROFINET I/O and IRT	Profibus Plus	TCP/IP Special Data link	Dynamic	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

In summary, a wide number of protocols operate in IACS networks. Design and implementation guidelines need to consider these protocols and their underlying communication models. This CPwE 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 IACS network.

Common Industrial Protocol Overview

CIP is a messaging protocol that defines how different IACS network devices, systems, and applications come together to form an IACS application, as shown in Figure 1-10. CIP is an application-layer protocol (OSI Layers 5 to 7). EtherNet/IP extends the application of Ethernet TCP/IP to the IACS for CIP applications.

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



CIP is a connection-based protocol and offers two main types of messaging: Explicit-informational and Implicit I/O. The protocol specifies a set of objects and services used to develop an IACS network. CIP is implemented at the application layer of four networks: CompoNet, DeviceNet, ControlNet, and EtherNet/IP. This *DIG* 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.

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.

Table 1-5 provides a brief overview of the CIP messaging types and their key networking characteristics.

Table 1-5 CIP Communication Overview

CIP mode	CIP message type	Description	Response Time Requirements	Layer 4 Type	Packet Size (Bytes)[1]	Port[2]
Unconnected	Unconnected	Temporarily used to open a CIP connection with another device.	Seconds	TCP	~500	44818

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

Table 1-5 CIP Communication Overview (continued)

CIP mode	CIP message type	Description	Response Time Requirements	Layer 4 Type	Packet Size (Bytes)[1]	Port[2]
Connected	Explicit Messages	Non-time-critical information data. For example, between a controller and a manufacturing historian application.	100s of milliseconds to seconds	TCP	~500	44818
	Implicit 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 (controller to device) or between controllers (controller-to-controller).	< Millisecond to 10s of milliseconds	UDP (IP) multicast and unicast	100 - 200	2222

[1] These are typical numbers, although depending on the application, the byte size can vary.

[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. Where multicast is chosen for use, Cisco, Rockwell Automation and the ODVA recommend the application of IGMP to manage the multicast traffic flow.
- EtherNet/IP implementations have traditionally been unable to route multicast traffic since the time-to-live field in the IP packet is set to 1. Although updated CIP EtherNet/IP specifications (CIP Specifications version 1.3, Volume 2 EtherNet/IP Adaptation of CIP, December 2006) call for this limit to be removed, this *DIG* is based on the implementation of TTL=1 because the routing of multicast traffic requires a more complex set of protocols and considerations to be applied.
- By the current EtherNet/IP standard, a multicast group is created for each EtherNet/IP 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 CPwE solution.
- Depending on the device producer, options may be enabled to configure whether the traffic generated by the device is unicast or multicast. This allows more flexibility in Cell/Area zone design and provides a means to manage the number of multicast groups within a Cell/Area zone.