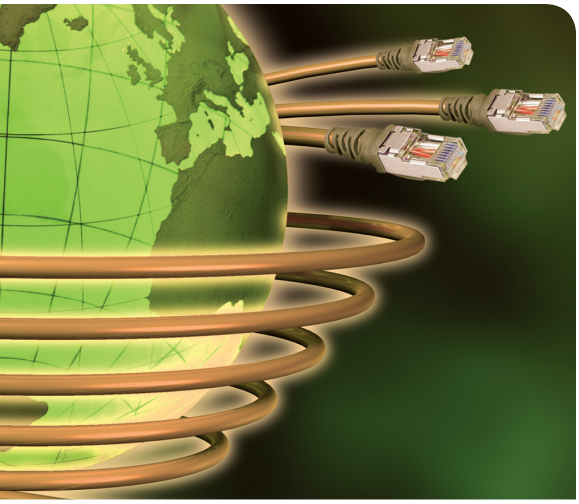


Guidelines for Designing an IT-Ready Machine

Best practices for machine builders on how to design information-enabled machines and integrate them into a plantwide network infrastructure.

Rockwell Automation and Cisco Four Key Initiatives:

- **Common Technology View:** A single system architecture, using open, industry standard networking technologies, such as Ethernet, is paramount for achieving the flexibility, visibility, and efficiency required in a competitive manufacturing environment.
- **Coverged Plantwide Ethernet Architectures:** These manufacturing focused reference architectures, comprised of the Rockwell Automation Integrated Architecture™ and Cisco's Industrial Intelligence, provide users with the foundation for success to deploy the latest technology by addressing topics relevant to both engineering and IT professionals.
- **Joint Product and Solution Collaboration:** Stratix 8000™ Industrial Ethernet switch incorporating the best of Cisco and the best of Rockwell Automation.
- **People and Process Optimization:** Education and services to facilitate Manufacturing and IT convergence and allow successful architecture deployment and efficient operations allowing critical resources to focus on increasing innovation and productivity.

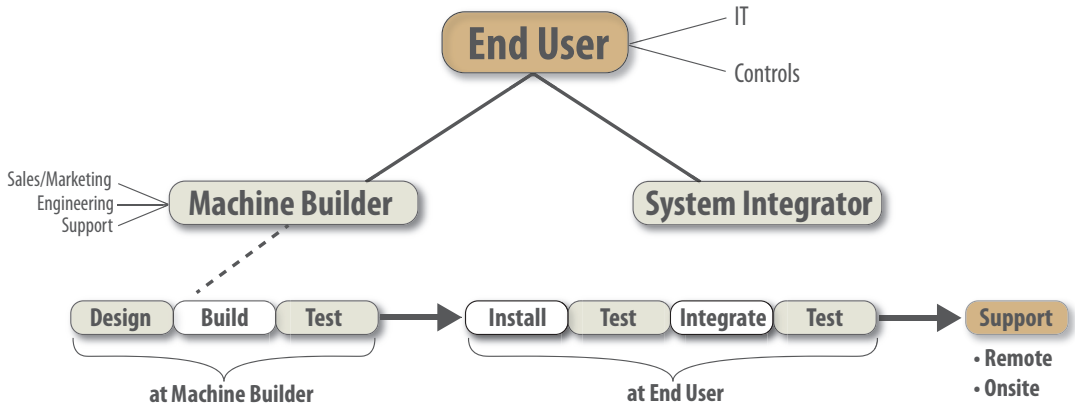
There is a paradigm shift occurring in manufacturing operations. For years, end users purchased purpose-built production lines based on their specifications. They controlled what machines went into the plants and the required level of networking. Often, that specification read "provide an Ethernet port for communications" with no indication of how they intended to use that communication.

Manufacturing companies can no longer think locally in this growing global economy. They now face new challenges, such as time to market and global competition, to name a few. Manufacturing operations have spread throughout the world, forcing many end users to reduce local engineering staffs. This shifted machine operation and performance responsibilities down to individual machine builders. These machine builders need to deliver defined OEE KPIs, take over more system responsibility and upgrade the networking ability of their machine.

Technology Convergence and Business Model Transformation

We have already seen the beginnings of technology convergence. Manufacturing companies are moving away from legacy proprietary networks in the controls systems and embracing open standard Ethernet, like EtherNet/IP. Corporate management has long desired a single network that would allow them to securely transfer data to where it needs to be. Timely information is now a key asset and companies realize the importance of investing in networks that facilitate business enterprise. The next stage of convergence calls for increased understanding and collaboration between a company's IT and controls organizations.

The graphic below reflects the many steps associated with building, installing and operating a machine. First, a machine is specified and built, generally at the machine builder location. Then, the machine is transported to the end user's location where it is installed, tested, integrated into the overall production facility and tested again so it can work seamlessly with other machines built by different vendors.



Machine builders in many industries are seeing dramatic changes to their business model as end users reduce control staff and, therefore, the time available to design, build and integrate a machine. Product life cycles are shortening while the global economy reacts to other market pressures. This requires many machine builders to react more quickly, reduce costs and provide more services to the end user. In some cases, machine builders take over more daily operations and warranty work because the end user or the systems integrator has reduced its engineering staff. These business model changes primarily occur in consumer-packaged goods and food and beverage industries, but are viable in heavy industries as well.

Over time, more and more things – sensors, actuators, human-machine interfaces (HMIs), controllers, tablets, computers, motors, pumps, and, yes, machines – will connect to the network. Devices and applications that join the network will need to integrate and collaborate in order to make the enterprise successful. This will lead to an Internet of Things where devices collaborate with each other as well as with their human counterparts. All of this will drive more integration to the enterprise.

It's now more critical than ever to build an "IT-ready" machine that easily integrates into a mixed environment controlled by both manufacturing and IT. In this environment, manufacturing focuses on how to build the end product, while IT focuses on the demand and supply components while maintaining call centers, sales portals and corporate email. Operations occur around the globe and a limited number of subject matter specialists are available to service and troubleshoot machines. As stated earlier, now machine builders need to understand what the next machine does, how it integrates and, potentially, what information flows from that other machine. This means IT and manufacturing operations and machine builders must effectively collaborate.

The IT-Ready Machine

Integrating a machine into an IT-controlled network requires an "IT-ready" machine that:

- Provides Ethernet connectivity
- Provides data that's relevant, timely and accurate so manufacturing companies can depend on it to make business decisions
- Does not compromise network security or breach existing policies
- Allows control traffic to co-exist with other types of network traffic and help ensure that this does not interfere with machine operation.

When designing a machine that integrates in an "IT-ready" scheme, machine builders need to be aware of some fundamental considerations:

- Aligning the machine's Industrial Ethernet configurations with their end customer's IT policies, a task simplified by using standard Ethernet and the TCP/IP protocol suite
- Using managed switches that provide network and security services
- Consistently using network services and follow IP addressing, subnetting and default gateway settings conventions
- Addressing Virtual LANs (VLANs), multicast management, Quality of Service (QoS) and resiliency
- Port security, access control lists and network access control, and aligning with emerging Industrial Control System security standards

Handling the IP configurations, the addressing unique to a machine or device, partially tackles these considerations. It is also increasingly important to provide remote access while adhering to an existing security policy. This calls for creating a managed environment, where the data types are known and controlled, and critical, real-time information is prioritized over video monitoring or email traffic. Setting up a secure and accessible environment enables the right people to access the right data at the right time, while blocking access to the wrong people. This environment should also enable users to quickly isolate and fix problems related to the network as well as individual pieces of equipment. Finally, users should have the ability to scale to new production or reporting requirements as well as incorporate new technology when it makes sense. This helps provide enhancements over the machine's life cycle while giving end users new efficiencies.

Why is designing an IT-ready machine important?

	End User	OEM/Systems Integrator
Security	Leverages existing security specialists and tools	Differentiates machines from competitors
Integration	Eases integration both physically (media) and logically (protocols and services)	Eases integration by using the right hardware
Maintenance	Increases data visibility to help with maintenance, operations and configuration	Enhances ability to maintain and troubleshoot
Compliance	Enables compliance with company standards and policies	Enables compliance with end-user policies and standards
Future-ready	Eases adoption of future technology	Eases adoption of future technology
Access	Enhances maintenance and troubleshooting once installed	Provides secure remote access and guest access

As Ethernet expands to lower-level devices on the factory floor, companies often want to leverage their security specialists, who typically work in the company's IT organization, to help protect their factory floor networks. But a machine builder can add value here by having secure access through the network, which gives the machine a competitive advantage over a similar machine that does not consider IT integration.

Integration onto the IT-controlled network allows machine builders to access their machine from anywhere to maintain it and gather production data. Improved visibility enables machine builders to more quickly and proactively respond to potential problems, helping to reduce downtime. In addition, both machine builders and end users can save money by reducing travel expenses and on-site engineering services.

Best Practices for Easing Network Integration

Follow Programming Best Practices

Machine builders can enable connectivity by using standard TCP/IP protocols and a defense-in-depth approach. Designing a machine that operates on standard Ethernet, like EtherNet/IP, provides the connectivity needed to interact with the business system at the end user location. EtherNet/IP is an industrial protocol that uses standard Ethernet and can easily integrate into the end user's network infrastructure without special switches or routers. Because it's standard Ethernet, EtherNet/IP can move data through a customer's existing network infrastructure and has the ability to co-exist on a network with other types of Ethernet traffic (e.g., HTTP, VoIP, SMTP, FTP).

Provide Ethernet Connectivity

Good programming enables machine builders to deliver data that's relevant, available and accurate. Best practices include:

- Using a UDT (user defined type), a named data type, to collect the data in the controller. This consolidates the data, improves performance and simplifies programming.
- Copying the data before moving it into the business system to increase reliability. Do not allow the business system to pull the data from the same memory location that the controller updates.
- Using programming to prioritize the copy process and prevent another process from interrupting it. Inappropriate settings can leave machine builders with incomplete data.
- Time-stamping data, so users can interpret it properly.

Discuss network address and security policies with IT

Machine builders also should take steps to provide a machine that will not compromise network security or go against existing security policies on the network. This can present a challenge to the machine builder, as every end user customer will have variations on these policies. The key to meeting this requirement is to design the machine with an Ethernet switch that provides flexibility in its feature set.

The chart below provides insight into how network policy typically differs between an IT-controlled network and a controls network.

Security Policies	IT Network	Controls Network
Focus	Help protect intellectual property and company assets	24/7 operations, high OEE
Priorities (in rank order)	1. Confidentiality 2. Integrity 3. Availability	1. Availability 2. Integrity 3. Confidentiality
Types of Data Traffic	Converged network of data, voice and video	Converged network of data, control, information, safety and motion
Access Control	Strict network authentication and access policies	Strict physical access, simple network device access
Implications of a Device Failure	Continues to operate	Could stop operation
Threat Protection	Enhances maintenance and troubleshooting once installed	Provides secure remote access and guest access
Upgrades	ASAP, during uptime	Scheduled, during downtime

Common Issues of Designing a Network-Enabled Machine

Network Addressing Scheme

When designing a machine that integrates into a larger network, the network addressing scheme is an important consideration. Each company has a different standard for addressing the automation system on the network. This often requires machine builders to re-work the controller and HMI programs to fit onto the customer's network address scheme.

End users are addressing this issue in many ways. Some write special script software that they can run in order to easily swap IP addressing in the programs. Others address this with network technology NAT (network address translation), which allows the user to assign a "private IP address" and a "public IP address" to the same node. NAT appliances, which can be a stand-alone device or a router, route all traffic coming to the "public" address to the private one. This allows the machine to keep the same IP address scheme and still communicate with the larger network. Yet another approach is to use hostnames when programming and rely on a DNS (Domain Name Server) on the end user's network to resolve the name to an IP address (e.g., www.google.com resolves to 66.102.1.99).

Switch Features

Network switches installed as part of the machine will likely be of great concern to IT. Many IT network policies are enforced through the network infrastructure, so it's important that devices can support these requirements. Some important switch features include:

- SNMP (simple network management protocol)
- VLAN (virtual local area network)
- IEEE 802.1x and NAC (network access control)
- IGMP (internet grouping management protocol) snooping
- QoS (Quality of Service)
- Network resiliency (spanning tree, rapid spanning tree, etc.)

Most network management software packages use SNMP. While users often implement proprietary protocols to enhance functionality, SNMP is an open standard that provides visibility into network configuration and diagnostics. Data gathered using the SNMP protocol can help manage configuration, perform diagnostics, manage administration of the network and justify new network equipment.

VLANs allow users to segment a network based on its purpose and independently of its physical location. It controls network traffic, which can be especially important on heavily loaded networks. It can also help enforce security policies and control network access. Once a user authenticates, they are given access to the network resources relevant to their job.

Both IEEE 802.1x and NAC enforce network security policies and prevent users from accessing network resources without first authenticating themselves or logging in as a guest. In addition to helping prevent unauthorized access, IEEE 802.1x and NAC also can track which resources were accessed and when.

IGMP and QoS enable tighter control of the network's bandwidth and have become increasingly important on a converged network with many types of network traffic co-mingling on the same wire. Both features give the network a deterministic quality important to control systems.

Network resiliency is often a required feature. Moving a cable creates the risk of plugging something into the wrong location, which causes a loop. Without resiliency, this could take down the whole network with a broadcast storm. In addition, when a cable gets broken or worn down, a resilient network finds an alternate path to help ensure continued availability of the network resources. Resiliency protocols vary from site to site, so it's important to select a switch that supports multiple protocols, including the most common, open protocols: STP, RSTP and MSTP.

Secure Remote Access

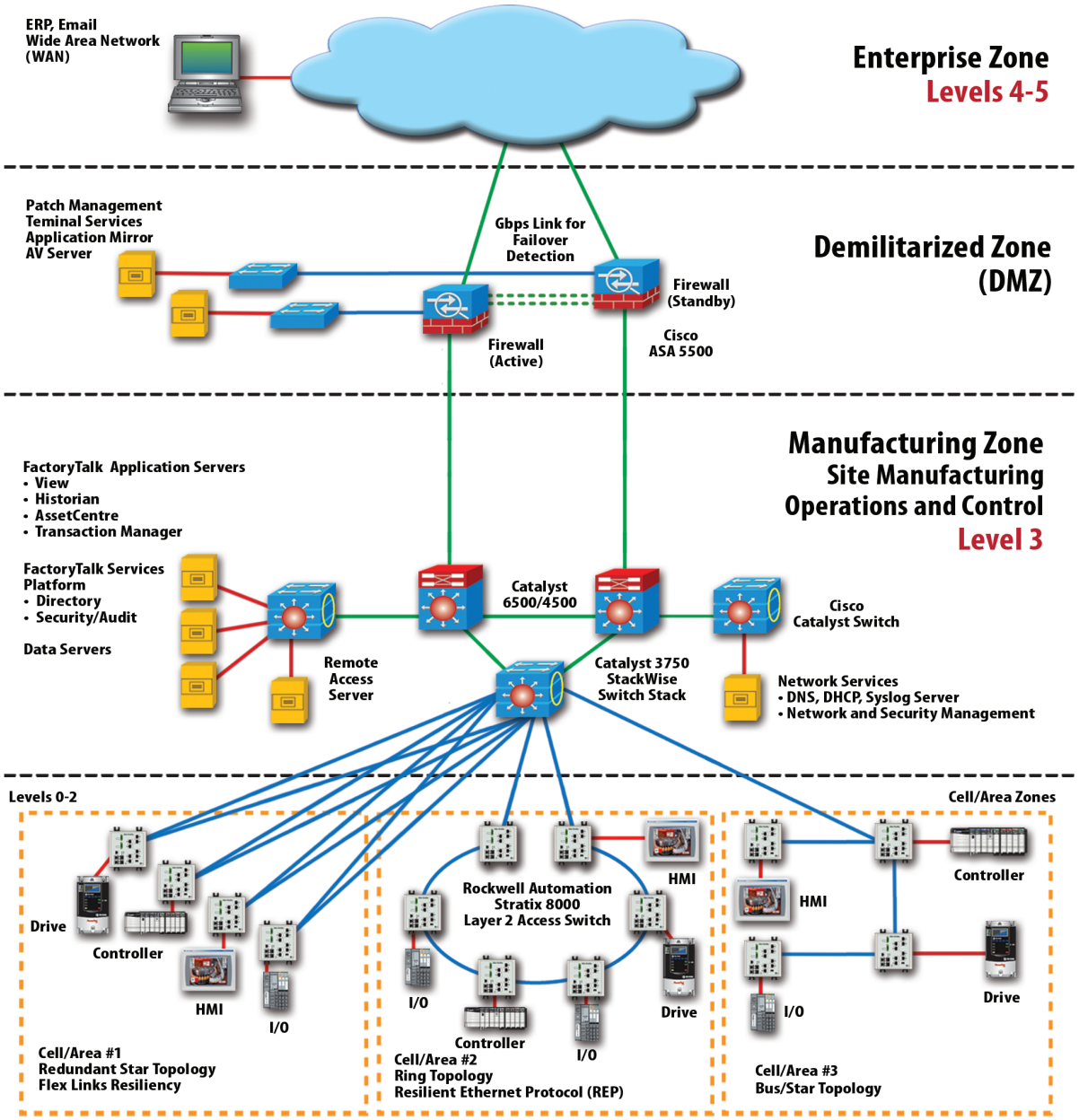
Secure remote access is less about the technology itself, and more about security policies and procedures. One size does not fit all. It is critical to find a scalable solution that fits the end user customer and the application. The following figure depicts an architectural approach to IT presence with defense-in-depth and alignment with industrial security standards.

With regard to remote access, machine builders should ask their customer's IT organization the following questions:

- Do you have an IT security policy?
- If so, do you have a remote access policy for employees and partners?
- If so, do you have a remote access policy for partners and suppliers, as well as the ability to manage partner access?
- What remote access technology and products do you use?
- Do you have a secure tunnel from your enterprise network to the industrial control system?

Converged Plantwide Ethernet Architectures

The graphic below illustrates the Converged Plantwide Ethernet (CPwE) architectures, a recommended practice that Rockwell Automation and Cisco Systems endorse together. This architecture model enables data flow, security, remote access and integration with a variety of devices. It demonstrates where the IT-ready machine integrates into a manufacturing operation, and how data flows into the enterprise business systems from production operations. Ultimately, it provides both end users and machine builders with an effective strategy that delivers the scalability and efficiency needed as the IT and control systems worlds continue to converge.



Imagining an IT-Ready Machine

An IT-ready machine is able to answer many questions.
Just imagine if your machine could tell you:

- I made 25 parts this past hour, five were rejected.
- I've been starving for product for the past 30 minutes.
- My drive system faulted.
- I took two minutes longer to reach temp, can you check this?
- I've had 22 parts jam in the past two days.
- I could run 15 percent faster if you kept my parts bin full.
- My current cost per part total = $27 (142 watts of electricity + 1.1 labor hours + 42 gallons of water + $3 of raw material).
- I could reduce energy by 5 percent by sleeping while I wait.

Who (or what) will your machines talk to? ERP, MES, OEMs, other machines? YOU?

Can you afford to ignore them?

To learn more about how Cisco and Rockwell Automation can help you, please visit:

www.rockwellautomation.com/partners/cisco.html
http://www.cisco.com/web/strategy/manufacturing/cisco-rockwell_automation.html

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at www.cisco.com. For ongoing news, please go to http://newsroom.cisco.com. Cisco equipment in Europe is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

www.cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Rockwell Automation is a leading provider of power, control and information solutions that enable customers to get products to market faster, reduce their total cost of ownership, better utilize plant assets, and minimize risks in their manufacturing environments.

www.rockwellautomation.com

Americas:
Rockwell Automation
1201 South Second Street
Milwaukee, WI 53204-2496 USA
Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Asia Pacific:
Rockwell Automation
Level 14, Core F, Cyberport 3
100 Cyberport Road, Hong Kong
Tel: (852) 2887 4788, Fax: (852) 2508 1846

Europe/Middle East/Africa:
Rockwell Automation
NV, Pegasus Park, De Kleetlaan 12a
1831 Diegem, Belgium
Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Publication ENET-WP024-EN-P — November 2011