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.
- **Converged Plantwide Ethernet Architectures:** These manufacturing focused reference architectures, comprised of the Rockwell Automation Integrated Architecture™ and Cisco's Ethernet to the Factory, 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.

Production Software Within Manufacturing Reference Architectures

Synopsis

Industry adoption of EtherNet/IP™ for control and information has driven the wide deployment of standard Ethernet for manufacturing networks. This deployment acts as the technology enabler for the convergence of manufacturing and enterprise networks. By gaining timely access to key performance indicators (KPIs) at the right levels by business and operation decision makers, Manufacturers now make business decisions from "real time" information. Information convergence between manufacturing and business systems within the enterprise allows greater business agility and opportunities for innovation.

To support and accelerate this network convergence, Rockwell Automation and Cisco collaborated to develop Converged Plantwide Ethernet Architectures, a set of manufacturing focused reference architectures. These resources, comprised of the Rockwell Automation Integrated Architecture™ and Cisco's Ethernet to the Factory, provide users with the foundation for success to deploy the latest technology by addressing topics relevant to both engineering and information technology (IT) professionals. Converged Plantwide Ethernet Architectures provides education, design guidance and recommendations to help establish a robust network infrastructure for manufacturing assets. One such manufacturing asset is the Rockwell Automation FactoryTalk® Integrated Production and Performance Suite, hereafter referred to as FactoryTalk.

This whitepaper outlines general recommendations for deploying production software, such as FactoryTalk, within the manufacturing reference architectures, as well as the use of FactoryTalk for convergence of manufacturing and enterprise information. At the end of this whitepaper is a listing of additional reference material; for additional information on manufacturing reference architectures, see notes 1, 2 and 3.

Converged Plantwide Ethernet Architectures

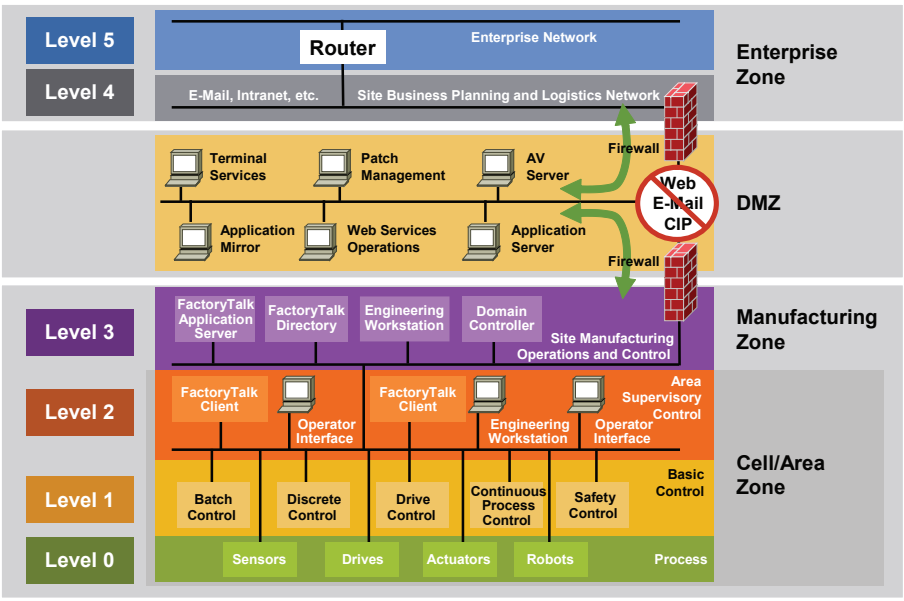
These manufacturing focused reference architectures are built on technology and manufacturing standards that are common to both IT and manufacturing. They include technology standards such as the IEEE 802.3 Ethernet standard, Internet Engineer Task Force (IETF) Internet Protocol (IP), and the ODVA Common Industrial Protocol (CIP™). For additional information about ODVA, see note 5. Additionally, Converged Plantwide Ethernet Architectures use manufacturing standards to establish a Manufacturing Framework as shown in Figure 1. These industry standards include ISA-95 Enterprise-Control System Integration, ISA-99 Manufacturing and Control Systems Security and the Purdue Reference Model for Control Hierarchy. The Cisco and Rockwell Automation framework establishes a foundation for key concepts such as

network segmentation for traffic management and policy enforcement, security, remote access, and quality of service (QoS). Following these concepts are important to ensure the optimal performance of manufacturing systems and applications, and to provide secure access and integration of FactoryTalk applications with the rest of the enterprise.

Throughout this paper and the Converged Plantwide Ethernet Architectures, terminology refers to "layers", "levels", and "zones". Layers are as defined in the Open Systems Interconnection (OSI) seven-layer reference model: Layer 1 for physical, Layer 2 for data link, Layer 3 for network, and so on. Layer 2 devices forward data and provide network services based on characteristics such as MAC addresses. Layer 3 devices forward data and provide network services based on IP. For additional information on the OSI network model, see note 5.

Both ISA-95 and the Purdue Reference Model for Control Hierarchy segment industrial control devices into hierarchical "levels" of operations within a manufacturing facility. Using "levels" as common terminology breaks down and determines plantwide information flow. For improved security and traffic management, ISA-99 segments levels into "zones". Zones establish domains of trust for security access and smaller LANs to shape and manage network traffic. For additional information about ISA, see note 6.

Figure 1 - Manufacturing Framework



The Manufacturing Framework groups levels into the following zones for specific functions:

- Enterprise Zone: Levels 4 and 5 include traditional enterprise IT networks, business applications such as email and enterprise resource planning (ERP), and wide area networks (WAN).

- Demilitarized Zone (DMZ): This buffer zone provides a barrier between the Manufacturing and Enterprise Zones, but allows for data to be shared securely. All network traffic from either side of the DMZ terminates in the DMZ; network

traffic does not directly traverse the DMZ. That is, no traffic directly travels between the Enterprise and Manufacturing Zones. Additionally, no primary services are permanently housed in the DMZ and the DMZ shall not permanently house data.

- Manufacturing Zone: Level 3 Site Manufacturing Operations and Control that addresses plantwide applications such as historian, asset management and facets of manufacturing execution systems (MES), and consists of multiple Cell/Area Zones.

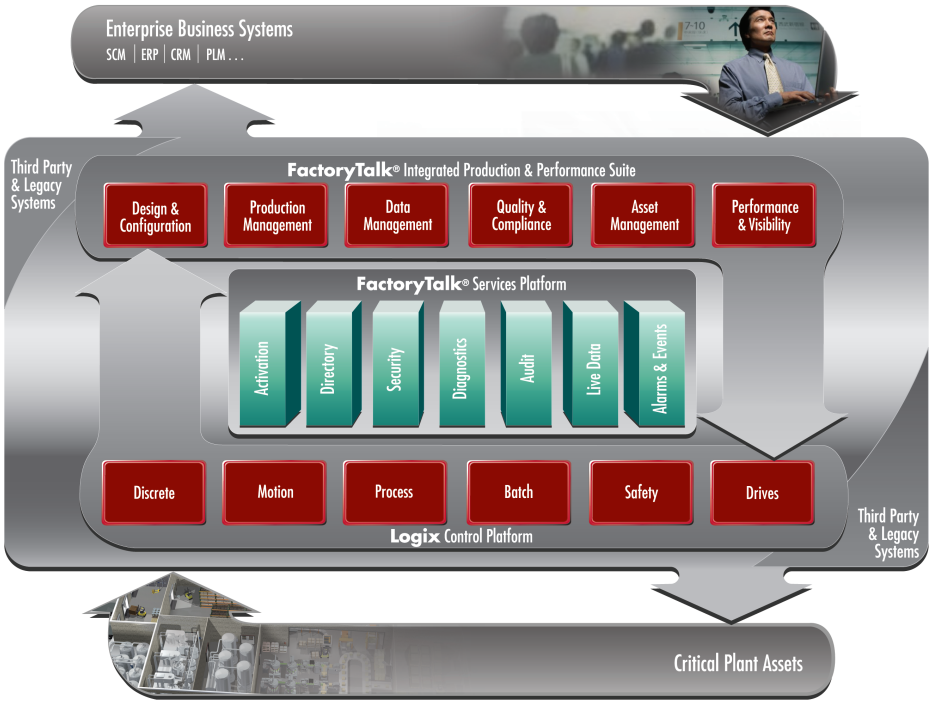
- Cell/Area Zone: Levels 0, 1 and 2 include industrial control devices such as controllers, drives, I/O and HMI, and multi-disciplined control applications such as drive, batch, continuous process and discrete.

FactoryTalk

FactoryTalk, shown in Figure 2, consists of a services platform and modular production disciplines (hereafter referred to as applications) that tightly integrate with the Rockwell Automation Logix Control Platform, helping to deliver a seamless flow of valuable manufacturing data. The Rockwell Automation Integrated Architecture is comprised of FactoryTalk and Logix, together providing both plantwide control and enterprise-wide information.
For additional information on Integrated Architecture, see note 1.

There are six distinct FactoryTalk applications that address today's diverse plant information needs, such as MES, asset management, historian and HMI/SCADA. The modular system design supports incremental solution deployments to help users maximize legacy technology investments, while improving the ability to incorporate new technologies. See notes 7 and 8 for additional information on FactoryTalk.

Figure 2 - FactoryTalk Integrated Production and Performance Suite



The FactoryTalk Services Platform is the foundation of the FactoryTalk applications. Comprised of a set of common software services that form a service-oriented architecture (SOA), FactoryTalk Services Platform allows applications to be developed that share common definitions, administration, real-time data, and so on. The FactoryTalk Services Platform is grouped by functionality.

- FactoryTalk Security allows centralized management of each user's rights and privileges based on their role and location.
- FactoryTalk Directory allows the sharing of common definitions such as users, tags, alarms or graphic displays.
- FactoryTalk Diagnostics and Audit provides common message formats, storage and viewing and also tracks the changes made in an application.
- FactoryTalk Live Data allows real-time communication between software applications as well as third-party OPC data servers.
- FactoryTalk Alarms and Events provide unified alarm definitions and common management between Logix programmable automation controllers (Logix PAC™) and software applications.

Manufacturing Zone

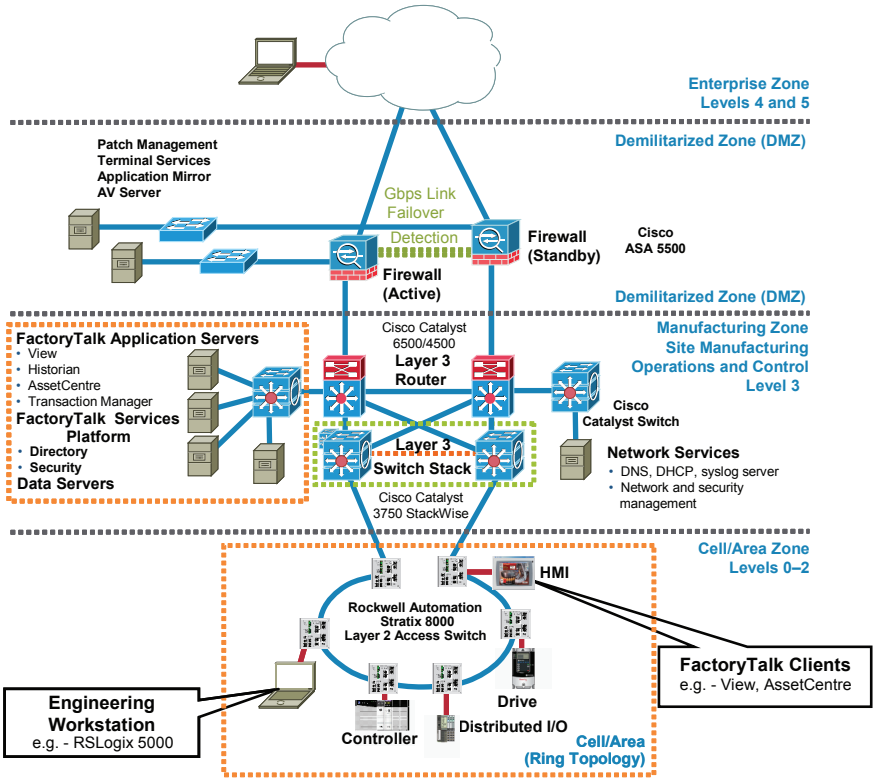
This zone includes Site Manufacturing Operations and Control functions (level 3) as well as multiple Cell/Area Zones (levels 0-2). The Manufacturing Zone contains all systems, devices and controllers critical to controlling and monitoring plantwide operations. To preserve smooth plantwide operations and functioning of the systems and network, this zone requires clear isolation and protection from the Enterprise Zone via security devices within the Demilitarized Zone (DMZ). This approach permits the Manufacturing Zone to function entirely on its own, irrespective of the connectivity status to the higher levels. A methodology and procedure should be deployed to buffer production data to and from the Enterprise Zone in the event of DMZ connectivity disruption.

All manufacturing assets required for the operation of the Manufacturing Zone should remain there. Assets include FactoryTalk as well as applications and services such as Active Directory, DNS and WINS. Figure 3 depicts the positioning of FactoryTalk within the Converged Plantwide Ethernet Architectures. See note 4 for additional information on deploying FactoryTalk within the Manufacturing Framework.

For clarity purposes, only content required to reflect the positioning of FactoryTalk within the Converged Plantwide Ethernet Architectures is reflected in Figure 3. See notes 1, 2, and 3 for additional information. The scope of this whitepaper is limited to manufacturing operations that exist within a single geographic site. This whitepaper does not address manufacturing operations which are distributed across multiple geographic locations.

Figure 3 depicts the multi-tier methodology defined by the Cisco and Rockwell Automation framework. To align with the Manufacturing Framework shown in Figure 1, Converged Plantwide Ethernet Architectures builds on the Campus Network Reference Model. Common with enterprise networks, this multi-tier model naturally segments traffic into three main tiers: core, distribution and access. This multi-tier model provides redundancy, rapid convergence, scalability and allows clear network segmentation, all of which are important in an industrial environment.

Figure 3 - Positioning of FactoryTalk within Converged Plantwide Ethernet Architectures



- Layer 2 access switches aggregate control devices within the Cell/Area Zones. Additionally, they provide layer 2 switching and network services such as resiliency via Spanning Tree Protocol (STP). Features such as IGMP Snooping, QoS, and Virtual LANs (VLANs) make sure that multicast traffic is managed, and critical control traffic is prioritized and properly segmented. This helps to restrict communications to the necessary network segments, and provides optimized communication performance for FactoryTalk applications.

- Multilayer (layers 2 and 3) distribution switches reside in the Manufacturing Zone (level 3), bringing together access switches from the Cell/Area Zones and providing network services. Services include layer 2 and 3 switching, routing, load balancing, resiliency via Hot Standby Routing Protocol (HSRP), QoS, IGMP Querier and security.

- The core switch aggregates distribution switches and provides high speed switching, and allows improved scalability and performance for large networks. Like Converged Plantwide Ethernet Architectures, IT professionals frequently use core/distribution/access as a common concept and tool within the enterprise.

The architecture depicted in Figure 3 will vary based on the size of the Manufacturing Zone to be supported, and requirements such as scalability, geographical dispersion and availability requirements. Examples of these scaleable architectures within the Converged Plantwide Ethernet Architectures are as follows:

- Small (Manufacturing Zone of up to 50 nodes)
  - collapsed core-distribution switch: multilayer switches with combined core and distribution functionality
- Medium (Manufacturing Zone of up to 200 nodes)
  - shown in Figure 3, separate core and distribution switches
- Large (Manufacturing Zone of more than 200 nodes)

Site Manufacturing Operations and Control (Level 3)

Site Manufacturing Operation and Control has a dedicated network segment within the Manufacturing Zone and contains the FactoryTalk application servers. Administrators should assign a unique IP subnet and Virtual LAN (VLAN) to this network segment.

The FactoryTalk application servers connect to a dedicated multilayer access switch, which aggregates into the layer 3 distribution switches. To provide redundant default gateways to the Cell/Area Zones, use Cisco Catalyst 3750 Stackwise layer 3 distribution switches. If stand-alone distribution switches are used, then use Gateway Load Balancing Protocol (GLBP) or Hot Standby Routing Protocol (HSRP) between the distribution switches. These protocols provide layer 3 failover and load balancing capabilities which are important to ensure the communications of FactoryTalk applications within level 3 to devices, controllers, and applications within the lower levels of the control system in the event of network disruption. FactoryTalk application server redundancy is the subject of a future whitepaper.

An example of software applications that would be deployed within the level 3 network segment include:

- FactoryTalk Services Platform
  - Directory
  - Activation
  - Security
  - Diagnostics
  - Audit
  - Live Data
  - Alarms and Events

- Application Servers

  - Factory Talk View SE
  - FactoryTalk AssetCentre
  - FactoryTalk Historian
  - FactoryTalk Transaction Manager

- Engineering Workstation

  - RSLogix™ 5000/500/5
  - RSNetWorx™

Manufacturing Zone implementations will also include additional applications and services which are recommended to be replicated within the level 3 network segment. This helps provide availability to manufacturing assets if connectivity to the Enterprise Zone is disrupted. Examples of these additional applications and services include:

- Active Directory
- DNS
- SQL Database
- File/Print Server

Area Supervisory Control (Level 2)

In addition to Site Manufacturing Operation and Control (level 3), the Manufacturing Zone consists of multiple Cell/Area Zones (levels 0-2). These layer 2 network segments should be assigned a unique IP subnet and VLAN per Cell/Area Zone. FactoryTalk application clients, engineering workstations, and maintenance tools used to configure and support the automation network are located within level 2. Examples of software applications positioned within level 2 include:

- Operator Interface

  - FactoryTalk View SE Client
  - FactoryTalk View SE Station

- Engineering Workstation

  - RSLogix 5000/500/5
  - RSNetWorx

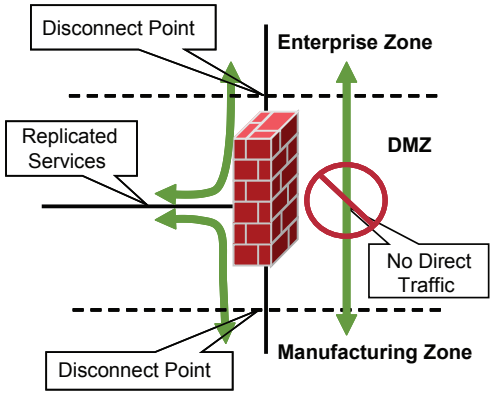
Information Convergence

Information convergence between manufacturing and business systems has provided Manufacturers with greater business agility and opportunities for innovation. With these opportunities, come challenges. Manufacturing computing and controller assets have become susceptible to the same security vulnerabilities as their enterprise counterparts due to this convergence. Securing manufacturing assets such as FactoryTalk requires a comprehensive security model based on a well-defined set of security policies.

Policies should identify both security risks and potential mitigation techniques to address these risks. Mitigation techniques include the use of a “defense-in-depth” security approach that addresses internal and external security threats. This approach utilizes multiple layers of defense (physical and electronic) at separate manufacturing levels by applying policies and procedures that address different types of threats. For example, multiple layers of network security protect networked assets, data, and end points, and multiple layers of physical security to protect high value assets. No single technology or methodology can fully secure industrial control systems. For additional details on defense-in-depth, see notes 10 and 13.

Given the different requirements, priorities, policies, and implications of incidents between the Enterprise Zone and the Manufacturing Zone, and the desire to share data, a DMZ should be used as a mitigation technique to provide a buffer zone between the Manufacturing and Enterprise Zones. The DMZ (Figure 4) can allow data that needs to be accessed by manufacturing and business systems to be shared securely, protecting information and accommodating the different security requirements of these zones.

Figure 4 - Demilitarized Zone (DMZ)

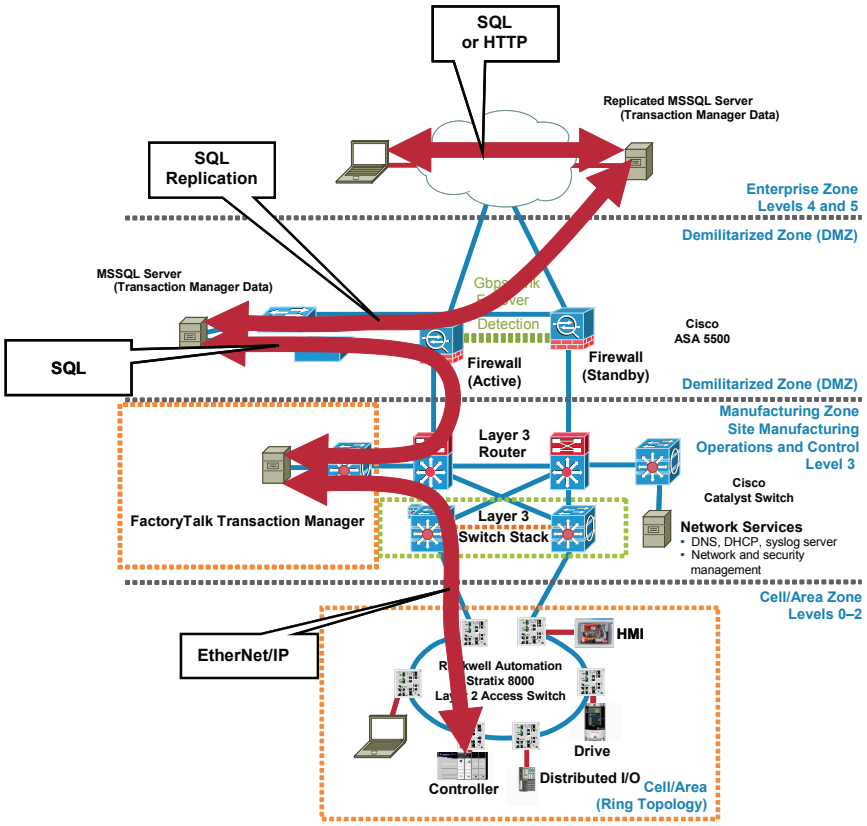


The methodology used to traverse information across the DMZ depends on the Manufacturers security policy, which will determine the acceptable approach and risk.

One example is to temporarily transfer Manufacturing Zone information into the DMZ, and then replicate this information up to the Enterprise Zone. This can be either unidirectional or bidirectional. This example is shown in Figure 5. This example uses FactoryTalk Transaction Manager to provide two-way data exchange between tags, such as Logix Controller or FactoryTalk View tags, and applications like an MSSQL server. These tags may contain key performance indicators (KPIs) or other important data that needs to be integrated into an enterprise application. In this specific example, production data is collected and transferred to a business system in the Enterprise Zone. The data is not stored nor used in the Manufacturing Zone, so DMZ connectivity disruption will not affect Manufacturing Zone operations. A methodology and procedure should be deployed to buffer production data to and from the Enterprise Zone in the event of DMZ connectivity disruption.

- The FactoryTalk Transaction Manager server (level 3) uses the RSLinx Data Server to read/write tags to controllers in level 1 utilizing EtherNet/IP.
- This same FactoryTalk Transaction Manager server is configured to read/write its SQL data to and from an MSSQL server located in the DMZ.
- This MSSQL server replicates the data to and from the Enterprise Zone MSSQL server.
- Business systems within the Enterprise Zone only access the enterprise MSSQL server.

Figure 5 - FactoryTalk Transaction Manager and MSSQL Server



In addition to information convergence, applications and personnel such as an engineer or partner may require remote access to manufacturing assets for the purpose of monitoring, management and configuration. This remote access to manufacturing assets can occur from either the enterprise or the internet. One example of remote access architecture is depicted in Figure 6.

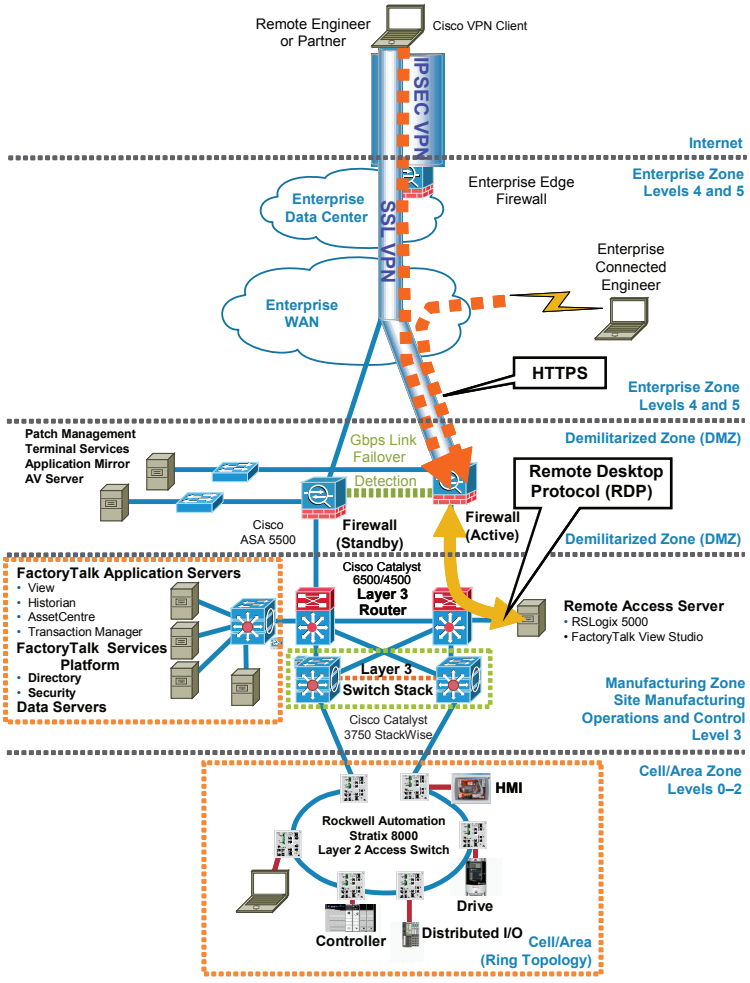
The heart of this remote access solution is the Cisco Adaptive Security Appliance (ASA) 5500 firewall located in the DMZ. This DMZ firewall hosts a secure web portal for web-based monitoring applications such as FactoryTalk ViewPoint and FactoryTalk VantagePoint. The DMZ firewall also initiates a remote desktop

protocol (RDP) connection to the remote access server (RAS) located in the Manufacturing Zone. The RAS hosts monitoring, management and configuration applications such as RSLogix 5000, FactoryTalk View Studio and RSLinx.

For this example, the internet client uses Cisco's VPN (virtual private network) Client to initiate a secure connection to the enterprise edge firewall via IPsec (IP security). A web browser (HTTPS) on the internet client is used to connect to the ASA web portal via SSL VPN (secure sockets layer). The firewall web portal establishes a link to the RAS server via RDP. From within the web browser on the internet client, the desktop of the RAS terminal server is accessed and applications such as RSLogix 5000 can be seen and interacted with. This minimizes the need to load manufacturing software on the remote clients, and the necessity to check the health status of the remote client itself (operating system patching and antivirus).

For additional information on Rockwell Automation software application use with terminal services see note 11. For additional information on secure remote access to plant floor applications and data see note 9.

Figure 6 - Remote Access Example



Summary

The convergence of manufacturing and enterprise networks has provided greater access to manufacturing data, which has led to greater agility in making business decisions for Manufacturers. The resulting agility has provided Manufacturers who have embraced the convergence trend with a competitive edge.

Network convergence has also exposed manufacturing assets to security threats that were traditionally found in the enterprise. Securing manufacturing assets such as FactoryTalk requires a comprehensive security model based on a well-defined set of security policies, and the use of a "defense-in-depth" security approach that addresses internal and external security threats. This approach utilizes multiple layers of defense (physical and electronic) at separate manufacturing levels by applying policies and procedures that address different types of threats.

General recommendations include:

- Establish a DMZ between the Enterprise and Manufacturing Zones.
- Keep FactoryTalk applications and Services Platform within the Manufacturing Zone.
- Keep replicated services such as Active Directory within the Manufacturing Zone.
- Utilize a team consisting of IT, operations and engineering professionals to define a security policy to address manufacturing needs:

  - DMZ information convergence - firewall and trust policies
  - Remote access for engineers and partners

- Use application data replication within the DMZ to converge Manufacturing and Enterprise Zone information.
- Utilize external network and security services (see note 12).

Additional Reference Material

Notes:

1) Converged Plantwide Ethernet Architectures Websites
http://www.ab.com/networks/architectures.html
http://www.cisco.com/web/strategy/manufacturing/cisco-rockwell_automation.html

2) Converged Plantwide Ethernet Architectures Whitepaper
http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp004_-en-e.pdf

3) Design and Implementation Guide (DIG)1.2
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

4) Ethernet Design Considerations for Control System Networks – ENET-SO001A-EN-E
http://literature.rockwellautomation.com/idc/groups/literature/documents/so/enet-so001_-en-e.pdf

5) Network Infrastructure for EtherNet/IP: Introduction and Considerations
http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf

6) ISA-99, Industrial Automation and Control System Security
http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

7) FactoryTalk Website
http://www.rockwellautomation.com/rockwellsoftware/factorytalk/

8) FactoryTalk Security Quick Start Guide
http://literature.rockwellautomation.com/idc/groups/literature/documents/qs/ftsec-qs001_-en-p.pdf

9) Secure, Remote Access to Plant Floor Applications and Data Whitepaper
http://www.ab.com/networks/architectures.html

10) Securing Manufacturing Computing and Controller Assets Whitepaper
http://www.ab.com/networks/architectures.html

11) Rockwell Automation Knowledgebase http://www.rockwellautomation.com/knowledgebase/

12) Rockwell Automation Network and Security Services
http://www.rockwellautomation.com/services/security/

13) Securing Today's Global Networks in Industrial Environments http://www.cisco.com/web/strategy/docs/manufacturing_self-defending_networks.pdf

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)
FactoryTalk, Integrated Architecture, RSLinx, Enterprise, RSLogix, RSNetWorx, are trademarks of Rockwell Automation, Inc.

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
Vorstlaan/Boulevard du Souverain 36
1170 Brussels, Belgium
Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.

Publication ENET-WP006A-EN-E — June 2009