Achieving Secure, Remote Access to Plant-Floor Applications and Data

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.

Abstract

To increase the flexibility and efficiency of production operations, manufacturers are adopting open networking standards for their industrial automation and control systems. Among the key benefits of open-standard networks is the ability to remotely access automation systems and share plant data, applications, and resources with engineering personnel and external partners, regardless of physical location. This flexibility is becoming even more critical in today's manufacturing environment, as increasing globalization and a shrinking skilled workforce make it very challenging to share information and quickly respond to production issues. This white paper outlines the means to enable highly secure remote access to plant-based applications and data.

Overview

Quick and effective response to issues on the production floor often requires real-time access to information and status from industrial automation and control systems as well as the skills and knowledge to take corrective action or optimize the production process. Unfortunately, many manufacturers today do not always have key skilled and experienced personnel, such as control and manufacturing process engineers, available at their global production facilities. Staffing constraints are often compounded by globalization and wider distribution of production facilities. Without these personnel readily available, manufacturers cannot quickly respond to events that occur in the production process or optimize their processes and operations. The resulting impact on operational efficiency and potential increase in downtime directly impact order fulfillment and revenue generation.

The adoption of standard networking technologies in production facilities offers a powerful means to help address the skill and resource gap experienced by many manufacturers. Secure remote access to production assets, data, and applications, along with the latest collaboration tools, provides manufacturers with the ability to apply the right skills and resources at the right time, independent of their physical location. Manufacturers effectively become free to deploy their internal experts or the skills and resources of trusted partners and service providers, such as OEMs and Sis, without needing someone onsite.

This paper describes how to provide highly secure remote access to industrial automation and control systems at production facilities. This paper is based on and extends the Cisco and Rockwell Automation joint Converged Plantwide Ethernet reference architecture. The Converged Plantwide Ethernet reference architecture is the integration of Cisco's Ethernet to the Factory (ETTF) and the Rockwell Automation Integrated Architecture™, and is part of an ongoing collaboration between Rockwell Automation and Cisco to provide customer education and network design guidance to help manufacturers successfully achieve the benefits of converging automation and business systems. This paper was written for Manufacturers looking to take advantage of standard networking technology in their plants. OEMs and SIs involved in plant design, implementation and operations that are looking to provide additional valuable services based on secure remote access to the plant floor may want to refer to this paper as a guideline on which those services can be deployed.

Technical Challenges

Automation systems have traditionally relied completely on onsite personnel to provide support for industrial automation and control systems, or used methods such as dial-up access and separate dedicated networks for remote support. These remote access methods have limited bandwidth and capabilities and are therefore limited to very basic monitoring and updating functionality. At the same time, they often circumvent perimeter security defenses and don't have the visibility and support of the Information Technology (IT) organization. This creates the threat of "back doors" into the manufacturing system and can represent a significant security risk. As manufacturers and partners want to provide more service and support remotely, and respond to issues in real time, these methods are no longer sufficient.

Another challenge is the need to keep local expertise onsite. While onsite support from both employees and partners is often an important element of an overall service and support plan, it can become expensive to have full-time support from IT, internal manufacturing resources, or related partners, especially if the plant is running multiple shifts or operating 24 hours a day. Even when personnel are available, there may be a limited number of subject-matter experts who can provide the expertise and knowledge needed to solve complex problems. The subject-matter expert may be at home, traveling, at a remote office, or solving the issue may require collaboration between a team of individuals from multiple locations and organizations.

Technologies for remote access to traditional enterprise networks, such as Internet-Protocol (IP) based Virtual Private Networks[1] (VPNs), have been around for quite some time. While encryption and authentication are important components of any solution, successfully applying these technologies to provide effective remote access to industrial automation and control systems has been a challenge. This is due to a number of challenges:

- Industrial automation and control systems are often managed by manufacturing organizations, while enterprise-level remote access solutions such as VPNs are the responsibility of the IT organization. Successful implementation of remote access to automation systems requires collaboration between IT and manufacturing organizations.

- Remote access can expose critical manufacturing systems to viruses and malware that may be present on a remote or partner machine, potentially impacting production.

- It is challenging to ensure that the end device (computer) being used for remote access is secure and has the appropriate versions of the applications needed for remote access and control.

[1] See Glossary

- Limiting the capabilities of the remote user to those functions that are appropriate for remote users, and do not require local presence due to line-of-sight or other similar requirements can be difficult.
- Manufacturers are often unable to limit a partner or remote employee's access to only specific machines, applications, or parts of the network for which they are responsible and have authorization.

As a result, remote access solutions, while widely deployed in the enterprise network, have not been as widely adopted to support the industrial automation network. When VPN technology has been used, it has often been subject to the previously mentioned challenges, and therefore limited to employees only (not partners), and can still result in some security risks, including viruses and unauthorized access, if not properly implemented.

To truly achieve collaborative manufacturing, thus leveraging the full value of a converged manufacturing enterprise, access needs to be scalable, regardless of location or company, and it needs to be done securely and in combination with the necessary communication tools – whether they are voice, video, and/or data – to effectively communicate, diagnose problems, and implement corrective actions. Access of course needs to be limited to those individuals that are authorized to access systems, and their authorized actions need to be aligned to corporate and plant policies and procedures.

Converged Plantwide Ethernet Reference Architecture

The Converged Plantwide Ethernet reference architecture developed by Rockwell Automation and Cisco outlines the key framework as well as detailed design and implementation guidance for applying standard networking technologies such as Ethernet[2], IP, and TCP/UDP[3] to the automation and control applications of a production facility. Adding remote access capabilities to the solution assumes the key tenants of the architecture are already in place, including:

- Security policy and procedures are in place, including consideration of remote access and the intended users.
- Well-defined zones are established, specifically the manufacturing zone, enterprise zone, and cell/area zones.
- Core industrial automation and control systems, applications, and devices reside in the manufacturing zone.
- A demilitarized zone[4] (DMZ) based on modern network firewall appliances protects the access to data and resources between the manufacturing and enterprise network zones.
- No direct traffic is allowed between the manufacturing and enterprise zone.
- The manufacturing zone is properly segmented into various cell/area zones with the application of Virtual LANs[5] (VLANs).
- Proper security and network management processes and applications are in place to monitor and manage the firewalls and manufacturing zone.

[2] See Glossary
[3] See Glossary or for more on IP, TCP and UDP, see Internetworking Technology Handbook-Internet Protocols: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html
[4] See Glossary
[5] See Glossary

- Properly secured controller and manufacturing zone computers, with proper patch management, are in place.

- Change management procedures to track what, when, and by whom changes are made.

Framework Overview

The Cisco and Rockwell Automation Converged Plantwide Ethernet reference architecture is aligned with emerging guidelines and standards that advocate differentiated zones and multiple layers of defense to ensure system and data integrity and availability. This security framework is based on the widely accepted Purdue Model referenced in standards such as ISA-99[6], 95[7], and NIST SP 800-82. Remote access capabilities are based on the security approach and recommendations outlined in this framework. This section will review the key tenants of the security approach in this architecture as a background and foundation for remote access.

The architecture developed by Cisco and Rockwell Automation specifies separate, protected zones for industrial automation and control systems and for the rest of the enterprise. A "zone" is defined as an aggregation of resources with similar access requirements, potential vulnerabilities, change-management processes, and provisions for the same consequences of security incidents. The concept of well-defined zones is especially important to help ensure that appropriate policies and capabilities are applied and security and performance requirements met in the different areas. The architecture is based on the principle that security must not compromise operations of the manufacturing control zone or the performance required by control I/O and real-time traffic. Zones typically encompass compatible content and frequent, clearly defined communication patterns. The zones are directly relevant to implementing remote access.

There are four zones in the Cisco and Rockwell Automation reference architecture. The two primary zones are the enterprise zone and the manufacturing zone. The cell or area zone is considered a subzone within the manufacturing zone.

- The **enterprise zone** comprises the site (plant) and enterprise IT environments, and includes corporate data centers, general access LANs and WANs, email systems, and business applications.

- The **demilitarized zone (DMZ)** is a buffer zone between the enterprise and manufacturing zones where data and services, such as remote access, are deployed.

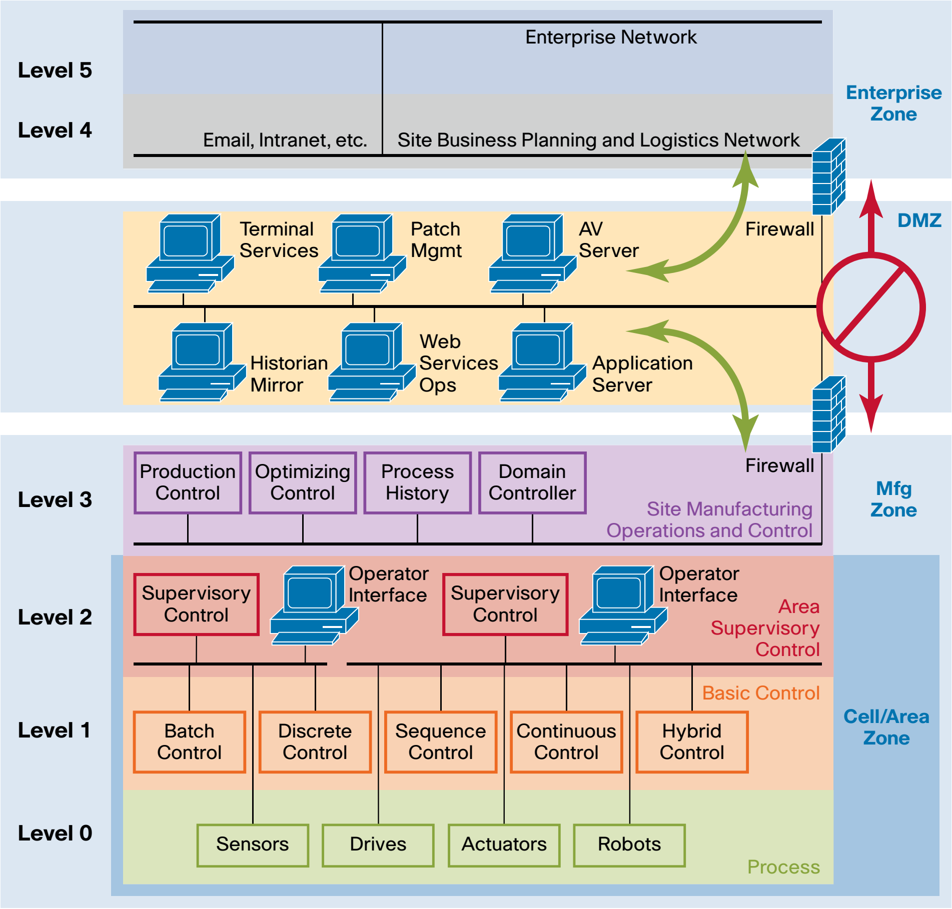
- The **manufacturing zone** consists of the different cell/area zones within a specific site and the application, systems, and services required for ongoing manufacturing operations.

- The **cell/area zone**, a subzone within the manufacturing zone, typically consists of systems that need to interoperate and communicate on a frequent or real-time basis. A cell/area zone may consist of multiple programmable automation controllers (PACs), robotic devices, and the human-machine interfaces (HMIs); either standalone or distributed associated with related or interdependent steps in the manufacturing process.

Figure 1 depicts the four zones.

[6] See Glossary
[7] See Glossary

Figure 1 Six-Level Plant Framework with DMZ



The DMZ and the "three-legged" firewall deployment is a key concept upon which remote access is built. A "three-legged" firewall configuration allows traffic from two different zones to a third, the DMZ, but no direct traffic flows between the other two zones (as depicted in Figure 3). This can be implemented with a single firewall running multiple firewall instances or in separate firewall appliances. The DMZ provides a highly important buffer between the manufacturing and enterprise zones, permitting highly secure, shared access to data and systems. The addition of remote access capabilities maintains these recommendations and uses key capabilities of the modern firewall (combined with a built-in VPN concentrator) to enable remote access to engineers and partners.

Strict policies in the DMZ help prevent cross-layer communication and infection, and include signature identification and intrusion protection through the deployment of intrusion prevention systems[8] (IPSs) to inspect and secure traffic coming from the enterprise and external networks. Signature identification is a mechanism modern security solutions incorporate to monitor the network packets and detect and respond to known network-borne threats. The DMZ can be split into functional subzones, divided by a firewall and an IPS (logically partitioned) to limit access to authorized individuals and traffic types.

Some of the key security components in the manufacturing zone include the use of VLANs to segment the traffic of specific devices and ports.[9] .As shown if Figure 2,

[8] See Glossary
[9] See Glossary

different cells/areas in Levels 0–2 can be grouped into different VLANs and then integrated at Level 3 in the manufacturing zone to enable communication between cells/areas. Access control lists[10] (ACLs) prevent unauthorized users and traffic types from gaining access, while port security prevents users from plugging in unauthorized devices. These concepts are also important for implementing remote access.

The Cisco and Rockwell Automation reference architecture specifies other relevant security and network design recommendations critical to efficient plant operations. More information on the Converged Plantwide Ethernet reference architecture is available at: http://www.ab.com/networks/architectures.html

Guiding Principles for Implementing Remote Access

Several guiding principles should be maintained when allowing remote access to plant data and resources. These principles were used to develop the Cisco and Rockwell Automation reference architecture and encapsulate the key concepts of strictly controlling the remote access of automation and control applications.

Use IT-Approved User Access and Authentication Policies and Procedures

Access to enterprise resources and services should be monitored and logged. Every user must be a known entity to the organization and use a unique account. Each network access by a user is then authenticated and given appropriate authorization within the enterprise network. Access is then tracked and logged for audit purposes. Granting access to plant floor data and resources should follow the enterprise's IT processes to grant and monitor access for local and remote users.

Use of backdoor solutions (such as modems, phone lines, and direct Internet access) to give partners, remote engineers, or vendors access to the plant floor and the manufacturing zone may pose a risk to plant and enterprise networks unless these solutions follow IT policies and procedures.

Automation and Control Protocols Stay Home

A key principle outlined in the Cisco and Rockwell Automation reference architecture is that "CIP Stays Home." CIP, the Common Industrial Protocol, and all other core automation and control protocols, including FactoryTalk® Live Data, OPC-DA, Modbus TCP, shall be contained to the manufacturing zone. These protocols and the devices they run on have limited security capabilities. They also have a significant impact on the industrial automation and control systems and the plant processes as they are used to start, stop, and operate the automation machinery. Therefore, the automation and control protocols should not leave the manufacturing zone. In the manufacturing zone, the automation and control devices are in a well-known physical boundary and are installed, operated, and maintained by trained personnel. Limiting the protocols to this zone ensures that the automation and control devices are communicating with known devices and applications (including versions). As well, the users of those devices and applications are authenticated and have authorization appropriate for their role.

This guideline may be reconsidered in the future when security devices (such as firewalls) exist that can strictly police the automation and control traffic coming for devices outside of the manufacturing zone. This will require that these "application" firewalls have an appropriate level of application or protocol awareness to fully inspect the data portion and the network portion of the packets being communicated and establish that the device is known and trusted. Until that technology is available on modern enterprise class firewalls, we recommend that the automation and control protocols "stay home."

[10] See Glossary

Control the Applications

A major consideration for plant floor applications is controlling the application used by the remote partner or engineer. As a best practice, partners and remote engineers should use versions of automation and control applications (such as FactoryTalk® View or RSLogix™ 5000) on controlled application servers when accessing the plant floor remotely for the following reasons:

- Allows the plant to strictly control the version/revision update of the application being used.
- Controls the level of access and authority of remote personnel. Using an application (such as FactoryTalk® View) installed on the remote system makes it more difficult to differentiate whether the user is local or remote and potentially requires allowing the automation and control protocols to leave the manufacturing zone.
- Prevents viruses or other compromises on the remote system from affecting the manufacturing zone applications and systems.

The use of automation and control applications on a remote user's computer introduces significant risk to the automation and control and should be avoided as a best practice.

No Direct Traffic

As indicated by the crossed circle in Figure 1, no direct traffic is permitted between the enterprise zone (including the Internet) and the manufacturing zone. Operations such as application or deployment of qualified patches must be a two-step process, with patches first being downloaded to a patch server in the DMZ and then deployed from there to manufacturing zone devices.

Deploying patches in two stages is desirable for control systems, because patches are typically validated in a test environment before being deployed into production systems. Remote access to devices on the control network requires logging into, or at least proxying through a server. The remote access server serves as a choke point where remote access can be further authenticated, logged, and filtered beyond what authentication and authorization are required to reach that server. This provides deeper accountability.

In this architecture, the plant firewall will act as a proxy between remote users and specifically implemented automation and control applications in the manufacturing zone, as well as strictly policing the traffic into and out of each zone, and therefore maintains this best practice.

No Common Protocols or Ports

No protocols that traverse one firewall (or firewall instance) are allowed to traverse the other firewall (or firewall instance) on the same port (as defined earlier) at the same time, see Figure 1. This prevents worms like Slammer to get through the upper firewall and infect a system in the isolation zone from propagating into the control zone.

Only One Path In or Out

The path from the DMZ through the lower firewall (or firewall instance) into the manufacturing zone should be the only path in or out of the manufacturing zone. The path from the enterprise LAN through the upper firewall into the DMZ should be the only path connecting the two zones.

These guiding principles encapsulate the key concepts of strictly controlling the remote access of automation and control applications rather than trusting that remote users are doing the right thing when accessing the plant applications.

Remote Access Use Cases

It is important to consider the use cases for remote access as they impact the solution used to support those requirements. The use cases for allowing remote access to the manufacturing plant floor have a range of characteristics, including who the user is (role – including internal employees, partners, and suppliers) and where the user is located (physical and network location). These use cases have different considerations and requirements.

Role

This paper focuses on deploying real-time access to plant floor data and applications for users who are monitoring or problem-solving issues or activities in the production environment. The roles may be filled by either internal or external personnel, but it is assumed that they are identified in advance. The paper does not describe a means to provide continuous data to Enterprise ERP applications, although the solution described does not preclude or inhibit such a mechanism.

A key consideration for the remote access approach identified by this paper is that users are known in advance and will typically have long-term or repeated access to industrial automation and control systems. This is a requirement as the process to deploy access to remote users, particularly external users such as partners or suppliers, often takes time given the need for the request for access to be initiated, approved, and then processed by the IT organization. Existing corporate policies should be already defined for differentiated roles and their access into the network.

Location

This paper focuses on remote users located in the enterprise network (external to the manufacturing zone) and external to the enterprise network altogether. Enterprise-based users may not have to apply all the technologies outlined below (such as establishing VPN to the enterprise) because they may already conform to existing corporate security policies.

This paper does not describe how to provide guest access for partners or third parties when they are physically located on the plant premises. There are a number of technologies available for guest access, including wireless guest access or network admission control, which provides generic Internet access for web browsing .[11] These methods may be used in conjunction with the specified techniques to provide remote access described in this paper, by essentially tunneling guests from outside of the manufacturing zone and then allowing them access to the manufacturing zone using the approach outlined in this paper.

Architectural Approach

With the principles of the Cisco and Rockwell Automation reference architecture in place, implementation of highly secure remote access to plant floor applications and data becomes relatively straightforward. The remote access capabilities are based primarily on the following existing architectures:

- Best-practice enterprise teleworker solutions implemented and operated by most IT organizations
- Cisco and Rockwell Automation Converged Plantwide Ethernet reference architecture with implementation of a DMZ with modern firewalls managing and inspecting traffic into and out of the DMZ

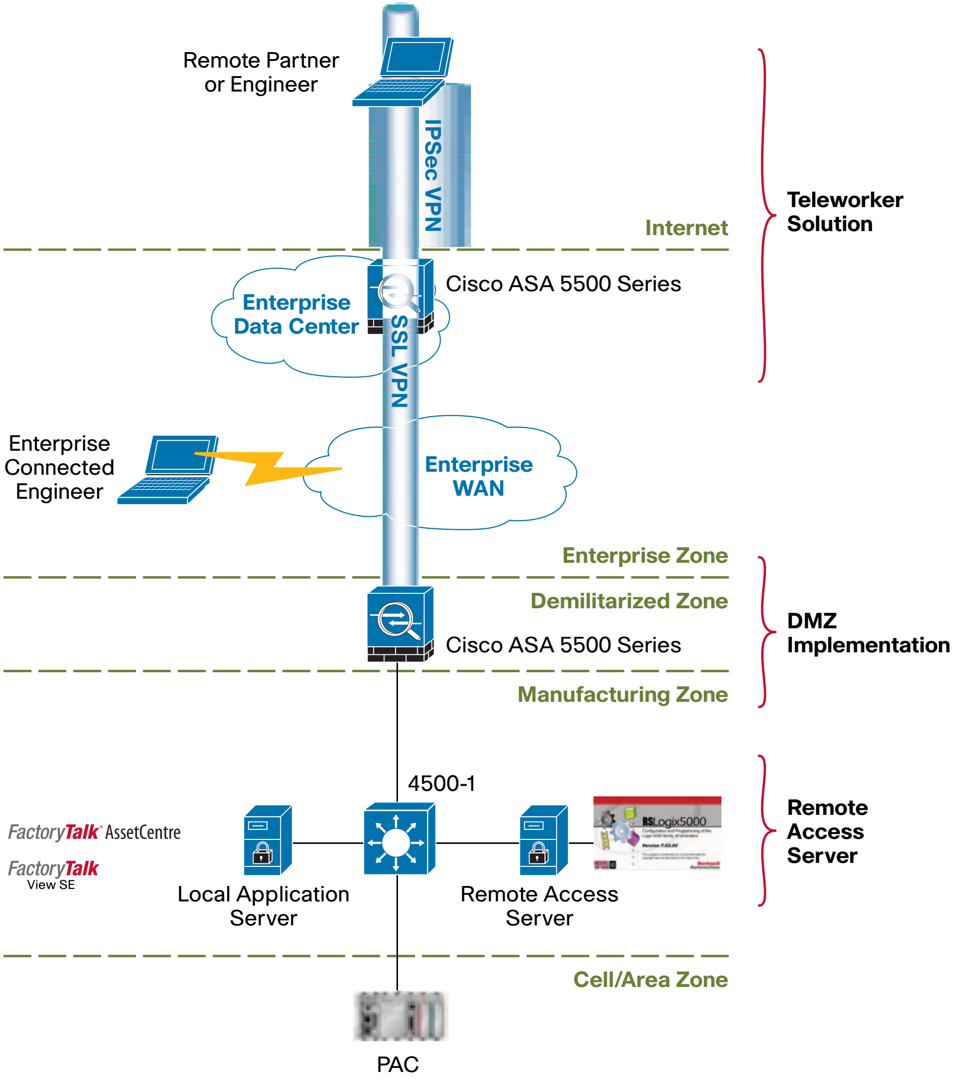
[11] For Cisco Validated Designs for guest access, please visit: http://www.cisco.com/en/US/netsol/ns815/networking_solutions_program_home.html

When considering implementing remote access, the following questions will help identify the organization's level of readiness:

- Do they have an IT security policy?
- Do they have a remote access policy for employees and the infrastructure to support? What VPN technology/products do they utilize?
- Do they have a "partner" remote access policy - the ability and process to add partners (OEM, SI, vendor, contractor)?

With these capabilities and security policies in place, the key to implementing remote access to the industrial environment is the implementation and configuration of the remote access server. Figure 2 shows a simplified version of the remote access architecture.

Figure 2 Simplified Remote Access Architecture



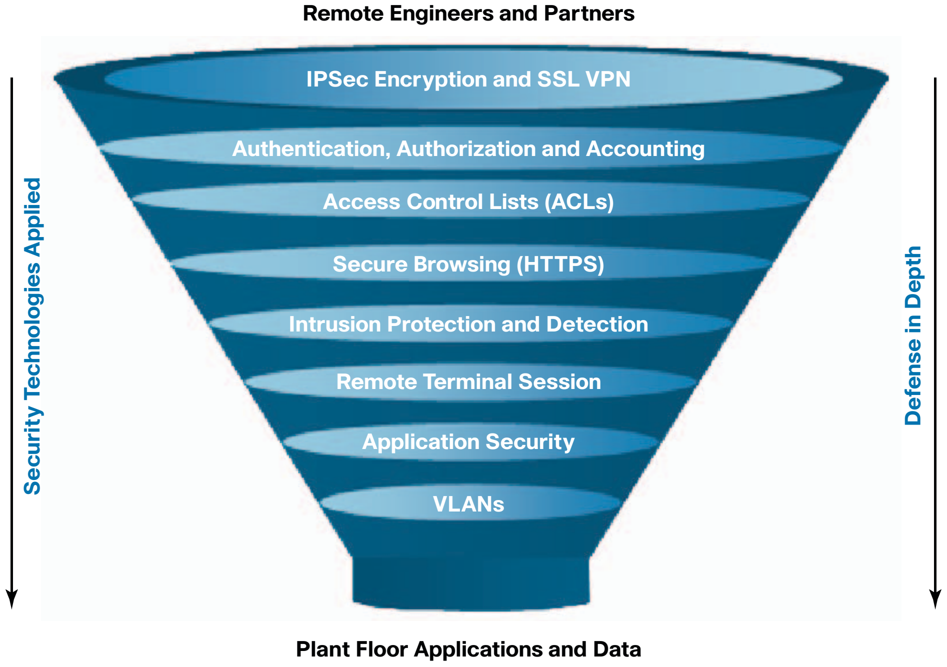
The DMZ was designed to allow sharing data and applications with users or applications not local to the production environment. A common means would be to replicate critical data onto a server in the DMZ to allow users/applications in the other zone to have visibility to that data. The DMZ is a proxy, allowing other users to make indirect network connections to data and applications residing in other network zones.

While replicating data into the DMZ enables quick and efficient data transfer between the manufacturing and enterprise zones, there are times when real-time access to the actual production systems and applications is needed to resolve issues, gather real-time information, or make adjustments to the process. The addition of remote access capabilities addresses this scenario by using terminal services in the DMZ as the proxy to real-time access to automation and control applications on a dedicated remote access server in the manufacturing zone. The recommended security mechanisms highlighted in this paper make that access highly secure for enterprise as well as external users, even when accessing externally from the enterprise network.

Remote users (partners or employees) can also access industrial automation and control systems through the remote access server via the Internet. Remote users often are in locations that may not offer high-bandwidth, low-latency network connectivity. This paper outlines the use of browser and terminal services, similar to thin clients, which perform relatively well in low-bandwidth and high-latency network environments. It does not, however, identify any network bandwidth or latency requirements nor does it explore any need to manage or monitor application performance in low-bandwidth, high-latency network connections differently.

Given the critical nature of industrial automation and control systems and the unique security considerations associated with them, it is important to ensure that remote access is implemented in a highly secure manner. This is achieved through a multilayer security approach that addresses the different potential security threats that could occur in a remote access scenario. The Cisco and Rockwell Automation recommended approach to securely grant access to plant floor applications is consistent with the existing plant architecture and applies "defense in depth" concepts with a number of key security solutions. Although there is no single technology nor methodology that fully secures industrial networks, combining these technologies forms a strong deterrent to most known types of threats and security breaches, while limiting the impact of any compromise. Figure 3 depicts the security technologies that give remote engineers and partners access to plant floor applications.

Figure 3 Defense-in-Depth Approach for Secure Remote Access


Remote Engineers and Partners
IPSec Encryption and SSL VPN
Authentication, Authorization and Accounting
Access Control Lists (ACLs)
Secure Browsing (HTTPS)
Intrusion Protection and Detection
Remote Terminal Session
Application Security
VLANs
Security Technologies Applied
Defense in Depth
Plant Floor Applications and Data

Implementation Details

This section describes how the various technologies are applied to enable highly secure remote access. It details the steps needed to give a remote user access to plant applications and data in real time. Other sections will briefly describe the implementation and operational considerations associated with implementing remote access to industrial applications. These sections discuss how the various security technologies are applied, the flow of traffic through the network infrastructure, and which network protocols make up that traffic.

The steps to implement remote access to industrial applications are as follows. (Details are depicted in Figure 4 and described in more detail in the following section.)

1. Use standard enterprise remote access solutions in the form of client-based, IPsec[12] encryption VPN technology to connect to the enterprise edge and for confidentiality over the Internet. The establishment of a VPN requires RADIUS[13] authentication of the remote person and is typically implemented and managed by the IT organization.

2. Limit access of remote partners connecting via IPsec to plant floor DMZ/firewalls using ACLs. Connect to the plant floor DMZ through a secure browser Hypertext Transfer Protocol Secure (HTTPS) only.

3. Access a secure browser (HTTPS) portal application running on the DMZ/firewalls. This requires an additional login/authentication.

4. Use a Secure Socket Layer (SSL)[14] VPN session between the remote client and the plant DMZ firewall and restrict application usage to a remote terminal session[15] (e.g. Remote Desktop Protocol) over HTTPS.

5. Utilize intrusion detection and prevention systems (IPSs/IDSs) on the firewall to inspect traffic to and from the remote access server for attacks and threats, and appropriately stop them. This is important to prevent viruses and other security threats from remote machines from traversing the firewall and impacting the remote access server.

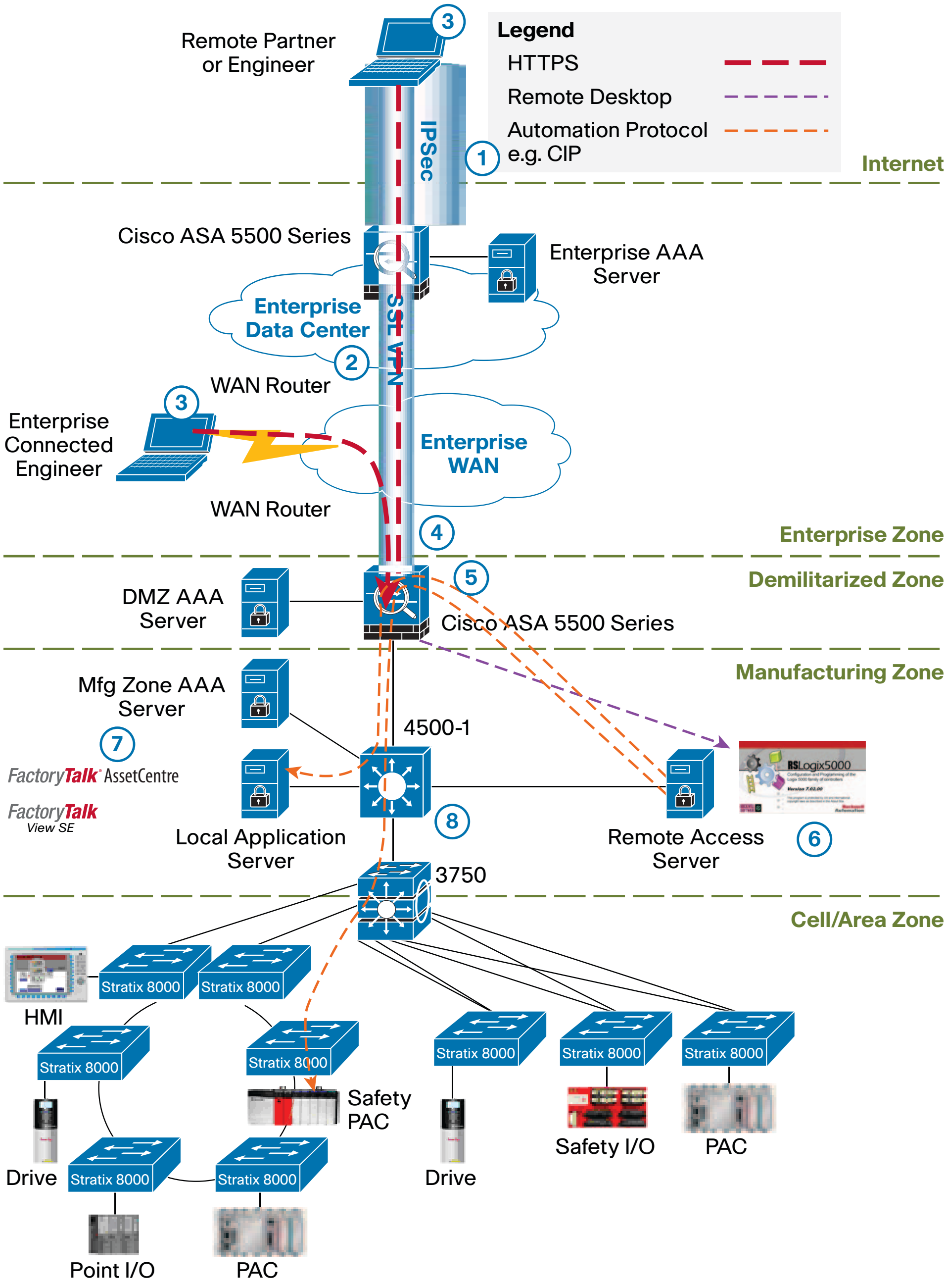
6. Allow the remote user to execute, via the terminal session, a selected set of automation and control applications that reside on the remote access server. Application-level login/authentication is required.

7. Implement application security that restricts users from the remote access server to a limited set of application functions (such as read-only, non-line-of-site functions).

8. Segment the remote access server on a separate VLAN and have all traffic between the remote access server and the manufacturing zone go back through the firewall. Apply intrusion protection and detection services to this traffic to protect the manufacturing zone from attacks, worms, and viruses.

[12] See Glossary
[13] See Glossary
[14] See Glossary
[15] See Glossary

Figure 4 Detailed View of Remote Access to Industrial Automation and Control Systems



Use of Standard IT-Based Remote Enterprise Access – IPsec VPN

Most enterprise security guidelines and regulations maintain that all access to corporate networks should be tightly managed. Therefore, any access to the corporate network for remote partners or employees should be granted and deployed using standard IT-based remote enterprise access solutions.

These solutions typically involve establishing an account and authorization for the end user and providing a VPN connection to the corporate network from wherever the end user has network access. VPN technologies include IPsec and Secure Sockets Layer (SSL). IPsec-based VPNs are the most widely deployed remote-access technology used by most enterprises today. IPsec VPN technology does, however, require software to be loaded on the remote user's computer. SSL-based VPNs are becoming more popular as they can be deployed in a clientless manner (the client system only requires a web browser).[16]

The recommended architecture described in this paper utilizes IPsec-based VPN for the teleworker access to the enterprise network. The installation of the software client on a remote user's computer to support IPsec VPN can sometimes be a challenge for external users such as partners or suppliers, depending on their corporate policies and technologies utilized. At this time, however, given the wide deployment of IPsec VPN solutions for enterprise-level access and technical considerations regarding the capabilities and interaction of SSL and IPsec VPN technologies, it is recommended that IPsec VPN solutions be utilized for access to the enterprise-level network. Additional options to implement remote access capabilities without the use of an end-user software client may be possible as technology and market adoption evolve.

Access to enterprise networks normally requires authentication, authorization, and accounting (AAA)[17], often established with some type of a RADIUS server. In addition, enterprise IT organizations may even have established Network Access Control (NAC)[18] for remote users to verify that the external systems are running a certain level of code and have certain security precautions (often referred to as posture) in place. Although this paper does not specifically discuss NAC, some corporate polices may require that any remote users have their posture verified through NAC. NAC brings advantages such as protecting the other infrastructure (such as a remote access server) from possibly getting infected or impacted by any existing viruses, keystroke loggers, spyware, or worms that remote users may unknowingly have on their remote systems.

The establishment of a remote account for a remote partner is usually not a temporary or instant service. It may require a certain amount of time to establish initially, so may not address situations where ad-hoc or unknown user access is required. Once established, however, it is typically readily available, supported, and in place for a specified amount of time and is therefore an appropriate solution for internal employees and key partners with known users.

Permissions Limiting Access of Remote Partners

Once access to the enterprise network has been established, remote partners should be given explicitly limited access to corporate resources. Remote employees/engineers have access as defined by their corporate account. Strict access control lists (ACLs) should be established for remote partners to limit access to the resources and applications they need via a limited set of IP addresses and transport-layer port numbers. In this case, access should be limited to the plant DMZ firewalls and the use of HTTPS protocols (port number 443). Remote partners should not have access to all other non-required IP addresses and port numbers to maintain corporate security.

These restrictions can be applied using ACLs in the corporate network infrastructure, such as the Internet edge firewall in Figure 4. These ACLs are usually managed and maintained by IT network operations or security teams.

Use Secure Web Browsers Supporting HTTPS

All interaction with plant floor data and applications for remote engineers and partners should be performed using web browsers supporting HTTPS. HTTPS supplies additional encryption and authentication and is commonly used for Internet applications.

[16] For a more detailed description of these VPN technologies, please visit: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/prod_brochure09186a00801f0a72_ns125_Networking_Solutions_Brochure.html

[17] See Glossary

[18] See Glossary

Use of browsers suggests that client-based applications should not be used for remote access to plant floor applications.

Establish SSL VPN Session to Plant DMZ Firewall

Once secure browser connectivity to the firewall is established, the firewall will establish an SSL VPN session to the remote user for an additional level of protection. The session will further protect the traffic between the end client and the plant firewall. The remote user once again authenticates to verify which services/account on the remote access server are required.

Additionally, the plant firewalls ensure that all remote users are authenticated and authorized to use the remote access services.

Intrusion Protection/Detection

Once a user has established a session, the firewall's intrusion detection and protection services come into play to inspect traffic into and out of the firewall for various types of network-born threats. IDS/IPS was specified as part of plant architecture (Ethernet to the Factory, revision 1.2) to inspect all traffic passing through the firewalls. IDS/IPS provides an additional level of security to stop threats or attacks that may originate from the remote system and prevents these threats from impacting systems in the DMZ or the manufacturing zone by dropping malicious traffic at the source.

Although NAC also reduces threats from remote systems, the two technologies are complementary in that NAC focuses on the posture of the remote system (what versions and protection are installed) and IPS/IDS inspects the traffic for threats and attacks that may not be eliminated by NAC. Again, an in-depth approach is applied to develop a highly secure service.

Remote Terminal Session to Remote Access Server

Once secure browser connectivity has been established to the plant DMZ, the firewall can allow the user to access the remote access server through a terminal session. This can be established using Remote Desktop Protocol (RDP), Citrix, Virtual Network Computing (VNC), or other terminal session technologies. The firewall will prompt the user to authenticate using a RADIUS server before being authorized to access the Remote Access Server. The Cisco ASA 5500 Series Firewall Edition comes with Java plug-ins that natively support terminal session technologies within the SSL VPN portal. The remote desktop session is then hosted by the firewall using SSL VPN (provided by the Java plug-in) allowing the remote user to view and operate approved applications (based on their RADIUS authorization) on a dedicated server in the manufacturing zone.

By only allowing remote terminal protocols, the potential for viruses or attacks through the remote session is significantly reduced, and the plant can audit and record the actions taken by a remote engineer or partner.

Automation and Control Applications on Remote Access Server

The remote access server hosts the approved automation and control applications, such as FactoryTalk® View or RSLogix™ 5000. By executing applications on a secure, dedicated server, the plant floor personnel can strictly control the version of the applications, limit the actions that can be performed – for example by allowing read-only actions – and even limit the types of devices that can be accessed, only allowing vendors to see their relevant devices, for example.

The remote access server setup and configuration should also be carefully considered. Users authenticating to the remote access server should not be able to change their rights on either an application level or system level. For example: you do not want user's of the application server editing the registry or making themselves local windows administrators. We suggest following the guidelines for "Securing Manufacturing Computing and Controller Assets". These guidelines recommend that endpoint security such as antivirus and/or Cisco Security Agent be applied to the remote access server.

Segment and Inspect Traffic to and from the Remote Access Server

In order to strictly control the traffic to and from the remote access server, the server should be segmented onto a specific VLAN, while traffic is inspected by the firewall. The firewall can route traffic to and from the remote access VLAN. If more than one remote access server is available, each server can be on a different VLAN and each VLAN can have access to a specific set of other manufacturing VLANs, thereby further limiting a remote user's view of the manufacturing zone.

Organizational Considerations

As with any plant networking solution, the successful implementation of remote access capabilities typically require a combination of IT and plant floor resources. It is important that both organizations agree upon the architecture and split the responsibilities throughout the lifecycle (design, implementation, management, etc.) based on each group's skills, capabilities, and resources.

The breakdown of responsibilities will depend on the level of interaction and cooperation between IT and the plant floor resources. For Table 1, we assumed that responsibilities are split between production and IT at the plant firewalls; IT is responsible for firewall configuration, especially the upper firewall instance. In many cases, as shown below, production and IT will collaborate on the design, implementation and operation of the DMZ. Production is typically responsible for setup and configuration of the manufacturing zone. This division of responsibility is highly dependent on each organization's skills and capabilities. When IT and production work together well, IT may take certain network design, implementation, and operational responsibilities in the manufacturing zone.

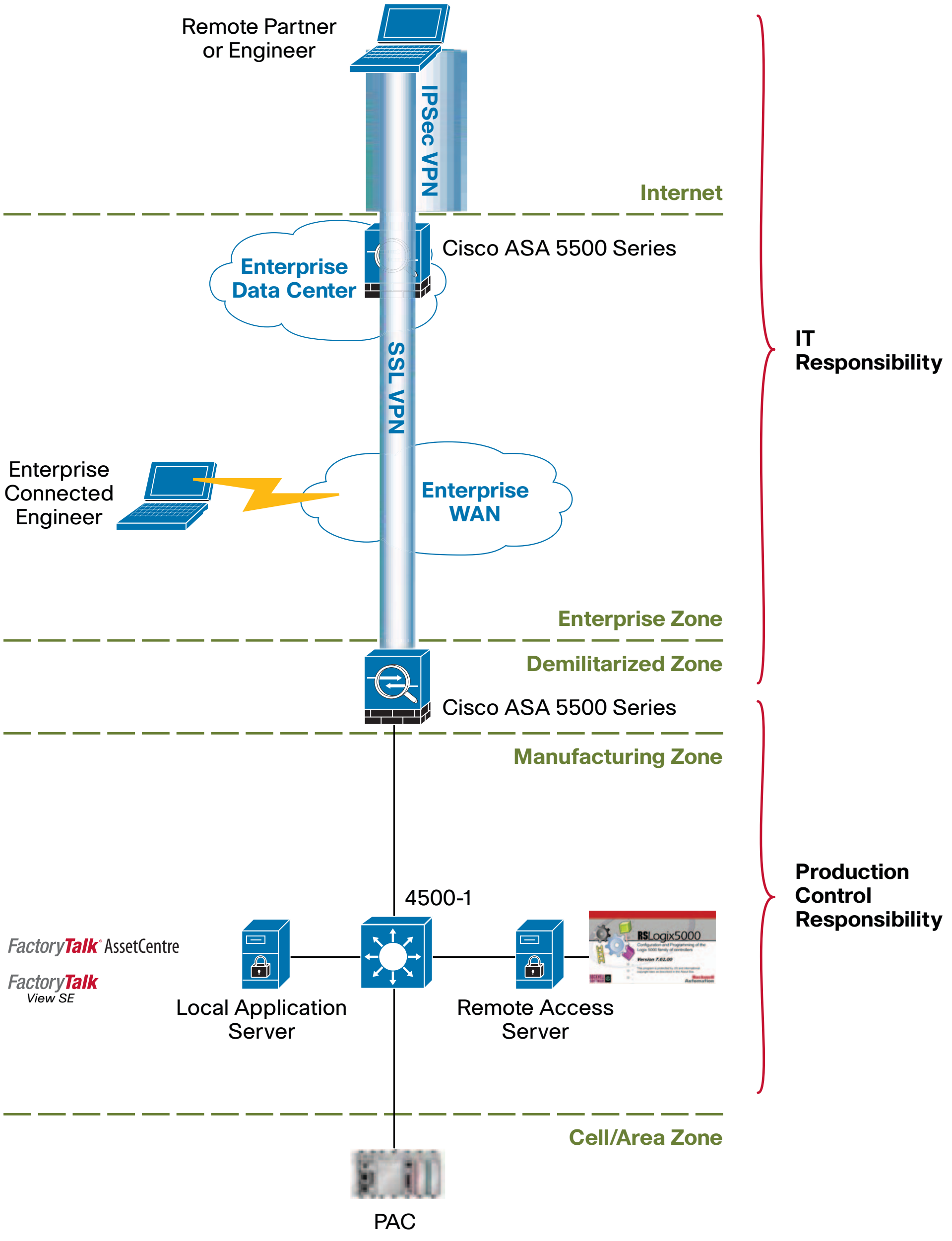
Table 1 Example Breakdown of IT and Production Responsibilities

Step	IT	Production
1. Establish VPN to enterprise including VPN client installation and enterprise authentication	X	
2. Limit access to production firewalls	X	
3. Secure browser	X	
4. Set up SSL VPN to plant firewall	X	X
5. Set up IPS/IDS on plant firewall	X	X
6. Set up and configure remote access server		X
7. Automate and control application security		X
8. Segment remote access server		X

Many organizations rely on partners and suppliers to provide services throughout the system lifecycle, ranging from design to implementation and operation. These services can complement the organization's available skill sets to shorten implementation times and ensure the system architecture design meets the requirements of the applications. It's important to find partners that have the necessary range of services and skills for both IT and production areas of responsibilities. Cisco and Rockwell Automation both offer services that can help address some of these challenges and, between the two companies, can often meet the needs of both IT and production organizations.

Figure 5 highlights how these responsibilities break down in the context of a remote access architecture. Note, this diagram is a simplification of the networking infrastructure normally in place and is meant to highlight the key infrastructure needed for remote access.

Figure 5 Example IT and Production Areas of Responsibility



Specific Components

The Cisco and Rockwell Automation Converged Plantwide Ethernet reference architecture includes the following components:

- **Adaptive security appliances:** Cisco ASA 5500 Series Adaptive Security Appliances provide critical perimeter defense, including defining and protecting the DMZ. The security appliances can perform a number of advanced functions, including firewall capabilities such as stateful packet inspection and application-level firewall and protocol inspection. The Cisco ASA 5500 Series can also incorporate additional advanced functionality, such as intrusion detection and prevention and VPN capabilities. Implementing a strong perimeter defense with adaptive and multifunctional firewalls is an important step to achieving prevention objectives.

- **Intrusion prevention system (IPS):** Deployed between the enterprise and manufacturing networks, the IPS can detect and block attacks, including worms, viruses, and other malware, through inline intrusion prevention, innovative technology, and identification of malicious network activity. This stops threats before they reach industrial automation and control systems, helping to ensure availability and integrity of manufacturing data and equipment. These capabilities can be integrated into Cisco ASA 5500 Series devices identified as the plant firewall.

- **Secure infrastructure:** A secure network platform supports the consistent use of integrated security features important to both the manufacturing zone and the enterprise zone, such as VLANs, ACLs, port security features, and network protection features.

- **Remote access server:** The remote access server deployed in the manufacturing zone houses only the automation and control applications that remote engineers and partners need to access. The remote access server is a dedicated physical server with appropriate endpoint security. As a dedicated server, it can be configured on a dedicated remote access VLAN to more finely manage the traffic to and from the server.

- **Production Control and Information:** Designed to provide a common control and information platform for plantwide production control systems, the Rockwell Automation Integrated Architecture is a control and information architecture consisting of the Logix Control Platform and the FactoryTalk® integrated production and performance suite, featuring EtherNet/IP and other enabling technologies. FactoryTalk® consists of modular production disciplines and a services platform that tightly integrate with the Logix Control Platform via EtherNet/IP. Logix programmable automation controllers provide a single control architecture for discrete, drives, motion, continuous process and batch production control systems.

- **Stratix 8000™ Modular Managed Switches, with Cisco Technology:** Providing the best of Rockwell Automation and the best of Cisco, this Rockwell Automation industrial Ethernet switch uses the current Cisco Catalyst® operating system, providing features and user interface familiar to IT professionals, while at the same time providing ease of set-up and comprehensive diagnostic information from within the Rockwell Automation Integrated Architecture.

The solution was designed and tested with the latest Cisco and Rockwell Automation components. Manufacturers may use older or other components, but may not have all the functionality identified here and therefore the solution may not be able to achieve the same level of “Defense in Depth”. Therefore, we always recommend that a Security Policy be defined and in place that outlines the technical security functions required to meet a Manufacturer’s security requirements.

Summary

The adoption of open networking standards for industrial automation and control systems has created new opportunities for manufacturing companies to improve productivity and respond more quickly to events that impact the production process. By connecting automation and control systems with standard networking technologies such as Ethernet and TCP/IP, manufacturers can share plant data, applications, and resources in real time with remote engineering personnel and external partners. These capabilities are increasingly important as manufacturing operations become more complex and globally distributed while the availability of skilled workers to support systems onsite on a 24-hour basis is decreasing. The remote access capabilities of the Cisco and Rockwell Automation Converged Plantwide Ethernet reference architecture give manufacturers the ability to apply the right skills and resources at the right time, independent of their physical location. This allows for higher efficiency, less downtime, and lower cost for production operations.

Given the critical nature of production control systems, however, it's important that any remote access solution provides the appropriate levels of security. Cisco and Rockwell Automation have worked together to develop an architecture that meets these requirements and provides secure access for both remote enterprise and external partners located away from the plant.

Solution References

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

Enterprise Class Teleworker
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/guide_c07_458724.html

Cisco IPsec and SSL VPN Solutions Portfolio
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/prod_brochure09186a00801f0a72.html

Cisco Ethernet-to-the-Factory Solution
http://www.cisco.com/web/strategy/manufacturing/ettf_overview.html

Rockwell Automation Reference Architectures for Manufacturing
http://www.ab.com/networks/architectures.html

Glossary

AAA

Authentication, authorization, and accounting. Pronounced "triple a."

For more on Authentication Protocols, see: http://www.cisco.com/en/US/tech/tk59/tsd_technology_support_protocol_home.html

ACL

Access Control Lists are used for purposes filtering IP traffic generally for security reasons.

For more on ACLs, see IP Addressing Services – Access Lists: http://www.cisco.com/en/US/tech/tk648/tk361/tk821/tsd_technology_support_sub-protocol_home.html

CSMA/CD

Carrier sense multiple access collision detect. Media-access mechanism wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period of time, a device can transmit. If two devices transmit at once, a collision occurs and is detected by all colliding devices. This collision subsequently delays retransmissions from those devices for some random length of time. Ethernet and IEEE 802.3 use CSMA/CD access.

DMZ, Demilitiarized Zone

Refers to a buffer or network segment between 2 network zones. A DMZ is commonly found between a corporate network and the internet where data and services can be shared/accessed from users in either the internet or corporate networks. A DMZ is typically established with network firewalls to manage and secure the traffic from either zone.

For an example of a network DMZ, see Scenario: DMZ Configuration: http://www.cisco.com/en/US/docs/security/pix/pix72/quick/guide/dmz_p.html

Ethernet

Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps. Ethernet is similar to the IEEE 802.3 series of standards.

For more on Ethernet, see Ethernet – Introduction : http://www.cisco.com/en/US/tech/tk389/tk214/tsd_technology_support_protocol_home.html & Internetworking Technology Handbook-Ethernet: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Ethernet.html

IKE

Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.

IP

Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

For more on IP, TCP and UDP, see Internetworking Technology Handbook-Internet Protocols: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html

IPS

Intrustion Prevention Systems is a network security device that monitors network activity for malicious or unwanted behavior.

See more on Intrusion Prevention Systems at widpedia: http://en.wikipedia.org/wiki/Intrusion-prevention_system or Cisco IPS: http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html

IPSec

IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE (See above) to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

For a more in-depth understanding of IPsec, see the following URL: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094203.shtml.

ISA-99

ISA-99 focuses on security for industrial automation and control systems, For more, see http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

ISA-95

The standard for the integration of enterprise and control systems , see http://www.isa.org/Template.cfm?Section=Find_Standards&Template=/Customsource/ISA/Standards/TaggedStandardsCommittee.cfm&id=2360

NAC

Network Access Control is a security approach that allows only compliant and trusted endpoint devices, such as PCs, servers, and PDAs, onto the network, restricting the access of noncompliant devices, and thereby limiting the potential damage from emerging security threats and risks.

For more on Network Admission Control, see: http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

Port

A port can refer to two things in networking.

1. Physical Interface on an internetworking device (such as a router).

2. In IP terminology, an upper-layer process that receives information from lower layers. Port is an application-specific or process-specific software construct serving as a communications endpoint used by Transport Layer protocols of the Internet Protocol Suite such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Ports are numbered (a port number), and each numbered port is associated with a specific process. For example, SMTP is associated with port 25. A port number is also called a well-known address. For a list of official port numbers see The Internet Assigned Numbers Authority (IANA). http://www.iana.org/assignments/port-numbers.

For the purpose of this document, port refers to the second meaning.

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized access, authorization and accounting management for pe.ople or computers to connect and use a network service. When a person or device connects to a network often “RADIUS” authentication is required.

Remote Terminal Session

Remote Terminal Session of Remote Desktop refers to a set of protocols and software that enable one computer or user to remotely access and control another computer through graphical Terminal Emulation. Software that makes it appear to a remote host as a directly attached terminal, including Microsoft’s RDP, Remote Desktop Protocol and VNC Virtual Network Computing.

SSL

Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

TCP

Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

For more on IP, TCP and UDP, see Internetworking Technology Handbook-Internet Protocols: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html

UDP

User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by the application or other protocols. UDP is defined in RFC 768.

For more on IP, TCP and UDP, see Internetworking Technology Handbook-Internet Protocols: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html

VLAN

virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

For more on VLANs, see Internetworking Technology Handbook-Lan Switching http://www.cisco.com/en/US/docs/internetworking/technology/handbook/LAN-Switching.html

VPN

Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

For more on VPNs, see "How VPNs work": http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094865.shtml or "IPSec VPN WAN Design Overview" http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html#wp1006588

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

Cisco: C11-519880-02—July 2009
Rockwell Automation: ENET-WP009A-EN-E—August 2009