CHAPTER 6

IACS Network Security and the Demilitarized Zone

Overview

This chapter focuses on network security for the IACS network protecting the systems, applications, infrastructure, and end-devices. As network security requires a holistic approach, many of the concepts and points are incorporated in previous sections. This chapter reviews many of those concepts to provide a complete overview of the security approach for IACS networks.

This chapter covers the following topics:

- Introduction to network security for IACS networks
- Background on network security
- IACS security overview
- Key network security features including the following:
  - Foundational network security considerations
  - Cell/Area zone network security
  - Manufacturing zone network security
  - Demilitarized Zone and the IACS firewalls
- Remote access to the IACS network

Introduction

As global manufacturing increasingly base its IACS applications on standard Ethernet and IP networking, manufacturers have been able to operate more efficiently and effectively. This new ability to integrate IACS and enterprise data enables real-time information sharing across the value chain, which increases data visibility, makes systems more available, assists rapid resolution of problems, and reduces operational and support costs.

Such powerful connectivity throughout the company and to outside partners has become indispensable for success. At the same time, it creates an environment where network security threats are a far greater concern. Because of the critical nature of IACS applications and the risks

associated with them, it is more important than ever for manufacturers to implement a comprehensive network security strategy that protects while it enables access and integration to achieve efficiencies and complete visibility.

The Cisco and Rockwell Automation CPwE solution helps manufacturers moving to IACS applications based on standard Ethernet and IP to connect, integrate, and secure their systems to help ensure consistent and reliable performance. The Cisco and Rockwell Automation recommended security model enables successful deployment of complex technologies in a manufacturing environment, meeting the needs of the IACS systems as well as enterprise business applications. This security model pulls from the best of Cisco security and Rockwell Automation security and approaches to deliver a cohesive and optimized security for IACS networks.

Cisco SAFE

The Cisco SAFE provides the design and implementation guidelines for building secure and reliable network infrastructures that are resilient to both well-known and new forms of attacks. Cisco SAFE takes a defense-in-depth approach, where multiple layers of protection are strategically located throughout the network, but under a unified strategy. Event and posture information is shared for greater visibility and response actions are coordinated under a common control strategy. The Cisco SAFE uses modular designs that accelerate deployment and that facilitate the implementation of new solutions and technologies as business needs evolve. This modularity extends the useful life of existing equipment, protecting capital investments. At the same time, the designs incorporate a set of tools to facilitate day-to-day operations, reducing overall operational expenditures.

This solution applies the SAFE model and many of the SAFE recommendations for the security of the IACS. This solution applies the relevant recommendations from “Chapter 2, Network Foundation Protection” and “Chapter 5, Enterprise Campus” of the Cisco SAFE Reference Guide (http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html). There are many other important guidelines in that document, but not necessarily relevant to the IACS network. For example, the section on the Corporate Access/DMZ are key considerations for the remote access capability outlined in this solution, but is usually the responsibility of the corporate IT organization.

Rockwell Automation Integrated Architecture

Protecting manufacturing assets requires a defense-in-depth security approach, as depicted in Figure 6-1, that addresses internal and external security threats. This approach uses 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 help protect high value assets. No single technology or methodology can fully secure IACS applications.

In achieving a defense-in-depth approach, an operational process is required to establish and maintain the security capability. A security operational process includes the following:

- Identify priorities (e.g., availability, integrity, and confidentiality)
- Establish requirements (e.g., remote access must not impact IACS network traffic, etc.)
- Identify assets
- Identify potential internal and external threats and risks
- Understand capabilities required

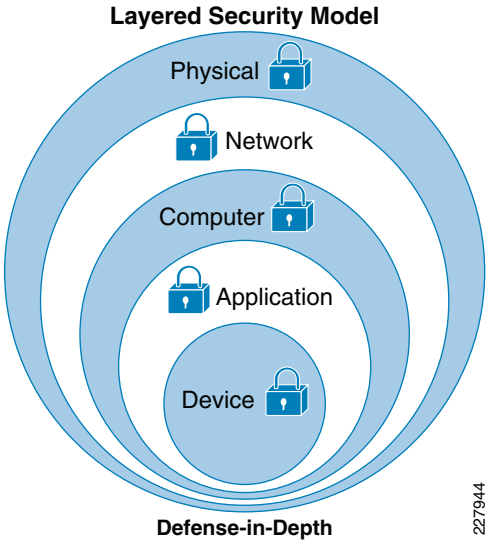
- Develop architecture
- Develop and implement manufacturing focused security policies

Designing and implementing a comprehensive manufacturing security model should serve as a natural extension to the manufacturing process. Manufacturers should not implement security as a bolt-on component to the manufacturing process.

In the Integrated Architecture approach, defense-in-depth layers for securing manufacturing assets include the following:

- *Physical Security*—This limits physical access of areas, control panels, devices, cabling, the control rooms and other locations to authorized personnel with provisions to escort and tracks visitors.
- *Network Security*—This includes the network infrastructure, such as firewalls with intrusion detection and intrusion prevention systems (IDS/IPS), and integrated protection of networking equipment such as switches and routers.
- *Computer Hardening*—This includes patch management and antivirus software as well as removal of unused applications, protocols and services.
- *Application Security*—This contains authentication, authorization and audit software.
- *Device Hardening*—This handles change management and restrictive access.

Figure 6-1 Rockwell Automation Security Defense-in-Depth Layered Security Model



Relevant Standards and Frameworks

ISA-99 Industrial Automation and Control System Security

The ISA-99 Committee establishes standards, recommended practices, technical reports, and related information that defines procedures for implementing electronically secure IACS applications and security practices and assessing electronic security performance. Guidance is directed towards those responsible for designing, implementing, or managing IACS applications and shall also apply to manufacturers, system integrators, machine builders, security practitioners, and IACS vendors.

The committee's focus is to improve the confidentiality, integrity, and availability of IACS networks and to provide criteria for procuring and implementing IACS applications. Compliance with the Committee's guidance will improve IACS electronic security, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising confidential information or causing IACS degradation or failure.

- ISA-99 published its Part 1 standard, ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems: Concepts, Terminology and Models, in late 2007.
- ISA-99 completed its Part 2 standard, ANSI/ISA-99.02.01-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program on 13 January 2009.

This *CPwE Design and Implementation Guide (DIG)* identifies some key security concepts that manufacturers should put in place, but are not necessarily covered in this document, such as Security Maturity Model and a process to evaluation and improve a “Security Level” of the IACS. These concepts are not covered in this CPwE solution.

The ISA-99 standards identifies a wide range of security concepts, definitions, models, as well as a process and guidance to develop cyber-security management systems for an IACS. This CPwE solution aligns with the process and guidance recommended. The key points of alignment include the following:

1. The clearly demarked network zones: Enterprise (CPwE and ISA 99) with Levels 4 &5, the DMZ and the Manufacturing (CPwE) or Control (ISA99) zone with Levels 0 - 3 as depicted in section ANSI/ISA-99.02.01-2009 section A.3.3.4.2 Figure A.8
2. Support for a Demilitarized zone (DMZ). As stated in ANSI/ISA-99.02.01-2009 section A.3.3.4.2 Network segments and zones:

   “For high risk IACS, the use of a DMZ in conjunction with a Control zone offers additional risk reduction opportunities between the low-security level Business zone and the high-security level Control zone. The security level for the DMZ is higher than the Business zone but less than the Control zone. The function of this zone is to eliminate or greatly reduce all direct communication between the Control zone and the Business/Enterprise zone.”

Additionally, the use cases where a DMZ is beneficial include the following:

- Minimize the number of people directly accessing control zone devices.

  Historian servers are often accessed by people located on the site LAN in the business zone. Rather than locating the historian server in the Control zone and allowing direct access to this device from the Business/Enterprise zone by a large number of users, the security level of the Control zone can be maintained at a higher level if the historian server is located in the DMZ. CPwE recommends the use of a historian mirror located within the DMZ to replicate historian data between the CPwE Manufacturing and Enterprise zones.
- Provide greater security for important IACS devices.

In the case of the historian server mentioned above, an option is to locate the historian on the site LAN where the majority of the users are located. This would reduce the number of people needing to access the PCN. However, since the business zone is a low-security level zone, the historian server would be subjected to a less secure environment. The potential for compromise of the server would be greater. The Cisco and Rockwell Automation CPwE does not recommend this approach.

- Compensate for patching delays.

  The DMZ offers additional security protection to important IACS devices that cannot be patched as quickly while waiting for patch compatibility testing results from the application vendor.

- Provide improved security for the Control zone by moving management devices to a higher security level.

  The DMZ is a good place to locate devices like anti-virus servers and patch management servers. These devices can be used to manage deployment of security modules to the control zone and DMZ devices in a more controlled manner without subjecting the high-security level control zone to direct connection to servers that may be communicating to hundreds of devices."

3. The implementation of a firewall to segment the Manufacturing or Control, DMZ and Enterprise zones from one another as noted in Figure 4-22. Although not specifically clarified, this CPwE solution recommends placing the Remote Access Server (CPwE name) or Remote Operator Console (ISA 99 name) and Historian servers in the Manufacturing or Control zone so as to keep the IACS communication contained to that zone.

The scope of this section is not to analyze and compare the ISA-99 material with the *CPwE DIG*, but nonetheless, Cisco and Rockwell Automation support the process and have tried to align this solution with concepts, ideas, and recommendations from ISA-99.

Background

This section is intended to give the reader some background and context to the security approach this CPwE solution promotes. As standard Ethernet and IP networking is still in a growth and adoption phase for many manufacturers, this background is intended to bring readers up to speed on key security concepts and considerations. Key topics include the following:

- Security principles maintained
- Challenges for network security specific to the IACS
- Key priorities for IACS security
- Review of the security requirements
- Description of IACS assets to be protected
- Overview of security threats to an IACS
- Impact considerations to determine level of IACS security

Principles

Defense-in-Depth

In the CPwE, security is embedded throughout the IACS network by following a defense-in-depth approach, and to ensure the availability, integrity, confidentiality and of data, IACS applications, IACS endpoints, the IACS network and the plant and its personnel. For enhanced visibility and control, a rich set of security technologies and capabilities are deployed in multiple layers, but under a common strategy.

Modularity and Flexibility

The CPwE design blueprints follow a modular design where all components are described by functional roles rather than point platforms. The overall IACS network infrastructure is divided into functional modules, each one representing a distinctive aspect such as the campus and the network foundation. Functional modules are then subdivided into more manageable and granular functional layers and blocks (for example, access layer, infrastructure device access), each serving a specific role in the network. The modular designs result in added flexibility when it comes to deployment, allowing a phased implementation of modules as it best fits the plant's needs. The fact components are described by functional roles rather than point platforms facilitates the selection of the best platforms for given roles and their eventual replacement as technology and business needs evolve. Finally, the modularity of the designs also accelerates the adoption of new services and roles, extending the useful life of existing equipment and protecting previous capital investment.

Service Availability and Resiliency

The CPwE design blueprints incorporate several layers of resiliency considerations and technologies and device/component redundancy to eliminate single points of failure and to maximize the availability of the IACS network infrastructure. A resilient and available network is inherently less susceptible to security threats. This includes the use of redundant interfaces, backup modules, standby devices, topologically redundant paths and application of network resiliency protocols. In addition, the designs also use a wide set of features destined to make the IACS network more resilient to attacks and network failures.

Auditable Implementations

The CPwE designs accommodate a set of tools to measure and verify the operation and the enforcement of safeguards across the IACS network, providing a current view of the security posture of the network, and helping assess compliance to security policies, standards, and regulations.

Challenges of Industrial Environments

Industrial environments are especially sensitive to security threats due to the fact that system downtime, loss of critical data, and other potential consequences can have a devastating impact on manufacturers. Even outages and performance degradation are unacceptable in these real-time, on-demand environments. Manufacturing business success depends on continuous, ongoing manufacturing, and downtime is incredibly expensive.

Today's movement toward commercial off-the-shelf (COTS) technologies—such as the Microsoft Windows operating system, Distributed Component Object Model, Ethernet and TCP/IP, and Internet-based applications—increases the risk. Ethernet and IP functionality provides great benefits in terms of visibility, efficiency, and cost-effectiveness, but it also exposes the manufacturer to a wider range of security threats, ranging from malicious code and attacks by hackers to performance issues due to unexpected traffic, network scans, or similar activities. Then too, as hackers become increasingly aggressive and sophisticated, and as disclosure of vulnerabilities occurs in real time, the time between the discovery and the exploitation of a COTS vulnerability is rapidly decreasing. While most security issues have been effectively managed in IT networks for several years, security has not typically been the focus of Control Engineers who design, deploy, and manage IACS networks.

The performance requirements of and IACS compound the challenge of securing IACS environments. To ensure consistent uptime and performance, these systems demand very low levels of latency, support of IACS network protocols, predictable performance, and high availability. At the same time, they often have patching limitations, and specialized network management considerations. Also, it is often important to provide guest and remote access to IACS applications and have visibility and integration of data between enterprise business and IACS applications. All these factors increase vulnerability and can affect the security tools that can be deployed.

Although it is tempting to conclude that IACS networks protected by a corporate firewall must be safe—and therefore immune to attacks on corporate mail and web servers—the situation is not that simple. Small security failures—an improperly secured wireless access point or a forgotten dial-up modem attached to a programmable automation controller for IACS applications, a personal computer, or even a remote access server directly connected to the IACS network—can provide access for a determined attacker. Intranet connections with business partners, suppliers, system integrators, or vendors within the plant can also provide ample opportunity for attackers to gain access without having to breach the Internet firewall or the firewall between the enterprise and IACS networks. Even IACS applications on their own isolated IACS network are at risk if users can access them. And once access is gained, attackers can find many familiar and largely vulnerable targets (namely, Windows-based workstations and servers) that can be compromised using existing tools and techniques.

These trends and issues are not unique to manufacturing. Organizations across many industries face similar challenges, particularly as hackers find new ways to exploit systems for financial gain. Manufacturing environments, like other embedded IACS applications, are especially at risk of attack since the cost of downtime is so high.

Priorities

The first step in developing an IACS network security approach is to define the secure environment's fundamental priorities, which will vary depending on the environment. This approach should be used for each security zone (such as an IACS network or a plant site IT network) across the enterprise to determine system needs and the best solution to support basic business requirements. These business necessities typically are availability, confidentiality, and integrity.

- *Availability*—The ability to preserve operational continuity. Information, data, services, networks, applications, and resources should be accessible in a timely manner when needed. It's essential to protect the availability of these assets from intentional or unintentional impact. Additionally, security services cannot impact the operational continuity as they execute.
- *Integrity*—The ability to preserve the authenticity of information, data, service, and configurations and to help ensure no unauthorized clients unexpectedly or covertly modifies any of these aspects.

- *Confidentiality*—The ability to maintain the privacy and confidential nature of potentially private or sensitive information, and to help ensure that only authorized entities have access to it. This applies both to data at rest and data in transit during communication.

A compromise in any of these three requirements carries the potential of serious impact or loss to a system. It is important, however, to understand the relative priorities between the requirements to make sure the security solution supports business demands. In a typical IACS, availability is the highest priority, followed by integrity of data, with confidentiality as the lowest priority. This may vary with the specific environment (if, for example, there are significant regulatory requirements), but confidentiality is rarely considered more important than availability or integrity. This differs from a manufacturer's traditional IT environment, in which confidentiality is often the highest priority (to protect information, batch recipes, or intellectual property), followed by integrity and availability.

System designs need to take into account these relative priorities to help ensure the appropriate security capabilities are implemented and aligned with policy. For example, if confidentiality is a priority, the IACS network may have very stringent access requirements or may incorporate security solutions that shut down access to the system when it detects unusual activity. Depending on how they are configured, these solutions can have a negative impact on availability and might not be appropriate in an IACS environment. Determining business priorities also helps to define the appropriate architecture for network services, such as Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and other critical network services.

Requirements

The IACS network should also be designed for a worst-case scenario to make sure systems remain available during unusual events, such as during alarms and notifications. If the IACS network is not designed to maintain high levels of performance, or if it shuts down access or reacts unpredictably to unusual activity, it will not achieve high availability and the security program will not have supported the business objectives.

The security tools implemented to support the above-mentioned high-level requirements must meet secure usability and manageability requirements:

- *Low end-user or end-device impact/High end-user transparency*—The measures used to protect the network environment should be chosen, designed, and deployed so as to minimize impact to IACS devices and applications, achieving a balance between security and end-device impact. Increased end-user impact and complexity also has the potential to affect the overall effectiveness of a security design, as it is human nature to try to avoid complexity.
- *Manageability*—A major aspect of delivering security services relies on increasing the overall visibility of the network and its transactions. It is imperative that manageability be considered when creating a security design, especially since online security is not typically an expertise found in manufacturing environments. Manageability includes being able to properly configure policy, rules, and parameters for the security system, but also involves key issues such as monitoring, feedback mechanisms, and telemetry data gathering.
- *Low performance impact*—The implementation of security measures in a network must take into account the underlying performance requirements to avoid affecting the overall performance of the system. Most IACS networks have unique performance considerations, including low latency and jitter.
- *Authentication, authorization, and auditing (AAA)*—The network solution should provide the ability to implement security services that provide the necessary control mechanisms to limit access to systems, applications, and network devices, as well as auditing mechanisms to track access, changes, and events.

- *Support Integration with Enterprise Applications and Remote Users*—The solution should support sharing of data and applications services between the Manufacturing and Enterprise zones where the DMZ is the "transfer" point. That includes making IACS data and applications securely accessible to remote engineers, control personnel and their partners and service providers.

Other security objectives that need to be considered when designing the architecture relate to the functional capabilities and access desired. The most important considerations include:

- *Guest access inside the facility*—Providing a mechanism for guests to access IACS applications and the Internet for third-party support personnel.
- *Shared access to data*—Allowing access to IACS data for efficient implementation in business systems and visibility of operational status.

The architectural design of CPwE accomplishes the above objectives in a manner consistent with these critical priorities and requirements. This highly secure, integrated network platform enables all these capabilities to be efficiently deployed as the need arises.

Assets to Protect

The second step in developing a security design is to identify the assets at risk or being targeted. The Cisco and Rockwell Automation approach is to identify the standard high-profile assets of potential value to an attacker or likely to have a significant impact on manufacturing operations in the event of an incident. The value typically associated with these assets is either direct (such as sensitive information) or indirect (such resulting fear, media coverage of a theft, revenue loss from an outage). They include the following:

- *IACS endpoints*—The devices or systems terminating an IP communications path and handing the data to the application layer. Endpoints may be interactive or standalone devices (laptops, desktops, servers, etc.). Endpoints considered include all the devices in Levels 0 to 3 and in the Demilitarized zone (DMZ) that are created as part of the architecture for the CPwE solution (see below).
- *Applications and services*—The higher-level processes relying on and using data being communicated or stored. Typically, the application or service uses network communications (and consequently the network infrastructure) to communicate with other applications or services residing on another endpoint.
- *Data in transit*—Data that is traversing the network infrastructure and is in transit between endpoints. Typically, active IP communications may use any subprotocol (UDP, TCP, RTP, etc.) to communicate information between applications on the endpoints. Of primary concern for protection of data in transit are IACS network protocols, such as CIP.
- *Stored data*—Information or data at rest in storage on an endpoint. The architecture designed to protect network access to endpoint systems should include protecting the stored data on those devices (e.g., Historian Server).
- *Network and Network Infrastructure*—The network elements that make up the transport structure moving communications between endpoints (switches, routers, security appliances, etc.) and the links interconnecting them may also be target of attacks such as theft of service, service abuse, denial-of-service (DoS), man-in-the-middle (MITM) and data loss to name a few

Protecting physical, non-network items such as material, products, resources, and people is also important to any overall security program. Protecting the networked assets noted above helps safeguard these items, but additional services may be needed to further defend physical assets. Capabilities such as physical security and location tracking are often important components of an overall security program. Many of these capabilities can be implemented using intelligent

networking technologies, such as integrated physical and virtual security and wireless location-based services. It is also important to include the appropriate policies, procedures, and training to protect all vital assets in a manufacturing facility.

Threats

After identifying priorities, basic requirements, and assets that need to be protected, the third step is to identify specific threats and attack vectors. As IACS applications move to more common computing and networking platforms, and become connected to enterprise systems, business partners, and the Internet, they are increasingly exposed to the same types of threats as traditional IT networks. These security threats include the following:

- Malicious code (malware)—The broad range of software designed to infiltrate or damage computing systems without user knowledge or consent. The most well-known forms of malware include:
  - *Viruses* manipulate legitimate users into bypassing authentication and access control mechanisms in order to execute malicious code. Virus attacks are often untargeted and can spread rapidly between vulnerable systems and users. They can damage systems and data, or decrease the availability of infected systems by consuming excessive processing power or network bandwidth.
  - A *worm* is a self-replicating program that uses the network to send copies of itself to other nodes without any involvement from a user. Worm infections are untargeted and often create availability problems for affected systems. They may also carry a malicious code to launch a distributed attack from all infected hosts.
  - The *Trojan* horse is a virus in which the malicious code is hidden behind a functionality desired by the end users. Trojan horse programs circumvent confidentiality or control objectives and can be used to gain remote access to systems, gather sensitive data, or damage systems and data.
- Distributed denial-of-service (DDoS) attack—A common type of attack used by network saboteurs. DDoS attacks have become notorious over the past few years by flooding the network resources (such as critical servers or routers) of several major retail websites, with the goal of consuming resources or obstructing communication to decrease the availability of critical systems. A similar attack can easily be mounted on a targeted IACS application, making it unusable for a critical period of time.
- Eavesdropping attacks—Used to violate the confidentiality of the communication by sniffing packets on the LAN or by intercepting wireless transmissions. Advanced eavesdropping attacks, also known as man-in-the-middle or path insertion attacks, are typically leveraged by an attacker as a follow-up to a network probe or protocol violation attack.
- Collateral damage—An unforeseen or unplanned side effect of techniques being used for the primary attack. An example is the impact that bulk scanning or probing traffic may have on link and bandwidth availability. IACS applications are especially sensitive to network latency and dropped packets. If a network is not properly configured, unintended traffic such as large downloads, streaming video, or penetration tests can consume excessive bandwidth and result in slowed performance and unacceptable levels of network jitter.
- Unauthorized access attacks—Attempts to access assets that the attacker is not privileged or authorized to use. This implies that the attacker has some form of limited or unlimited control over the asset.

- Unauthorized use of assets, resources, or information—Use of an asset, service, or data by someone authorized to use that particular asset, but not in the manner attempted.
- Reconnaissance attacks—Probing that enables the first stage of the attack lifecycle. This serves to provide a more focused attack cycle and improve the attacker's chances for success.

It is also important to understand where threats are coming from (threat vectors) when developing a security approach. As noted, security data related to IACS applications is limited, but you can see some consistent trends if you look at the data that does exist and traditional IT security issues.

According to the BCIT, the primary sources of attacks against IACS applications are the corporate WAN and business network, the Internet,[1] and trusted third-party connections (including guest laptops). While internal threats are still significant and one of the top areas of concern for plant managers, the data suggests that the threats increasingly originate from external sources. Prior to 2001, by contrast, the majority of attacks originated from internal sources. This mirrors the trend in traditional IT systems, where the threats have increasingly originated externally.

Internal threats can come from a number of sources, including attacks by disgruntled employees and contractors. Current or former employees and contractors often have detailed knowledge of target systems and can cause considerable damage. The IDC Security Survey of 2004 indicated that 31 percent of responding companies across multiple industries had terminated employees or contractors for violating their security policies. Therefore, it is important that security solutions and policies protect against potential insider attacks.

An internal threat can also be a device accessing the IACS network without the latest protection and unknowingly spreading a virus or attack. In addition to targeted threats, user error and unintentional incidents pose a significant risk and cause failure in manufacturing environments. A local or remote user might access the wrong systems and make changes, IT personnel can perform a network penetration test that degrades performance or renders systems inoperable, or a user may download or send large files over the network and impair IACS traffic performance. All these scenarios drive the need for comprehensive, multilayer security solutions and policies and should be considered when developing the system architecture.

External threats to information and automation systems are many and varied. They include accidental infection by a guest laptop; attacks by hackers seeking a thrill, fame, or money; corporate espionage; and even intrusion by terrorist organizations and foreign governments. Hackers use many of the techniques noted above and are an increasing source of threats to IACS applications. Today's hackers generally focus less on making trouble and more on making a profit, with groups looking for opportunities for extortion or theft that provide a quick payoff. Probably as a result, the number of attacks targeting specific organizations increased exponentially from 2005 to 2006. Such targeted intrusions are increasingly difficult to detect, which is a key reason for requiring complete visibility across the infrastructure. The faster a threat can be recognized, the more quickly it can be dealt with. Preventing the behavior of the attacks and intrusions once the hacker is inside is the key to security.

Hackers are developing new ways of penetrating a network every day, and their increasing sophistication has made it virtually impossible to prevent damage by traditional means. Numerous examples exist of means of attack that combine software vulnerability with human psychology. For example, a hacker may infect several USB keys with a Trojan horse designed to attack an internal system, setting them out in a parking lot in the hopes that an insider will use one and trigger the collection of a ransom. Cisco and Rockwell Automation has identified this and hundreds of other innovative techniques that hackers use to bypass traditional security controls.

1. Studies indicate that 80 percent of companies report employees abusing Internet privileges. Providing direct access to the Internet from manufacturing systems can significantly increase risks due to malicious code downloads, or may affect network performance due to the downloading of large files, videos, etc.

Software vendors regularly release patches to correct the vulnerabilities that hackers and viruses exploit. But a patch, by definition, is a response to an identified problem, not a proactive fix. Most patches are released three to six months after a vendor has identified a vulnerability—but large-scale outbreaks may occur just hours or days following a vendor announcement and continue causing incalculable damage until the patch is widely deployed. For example, in 2005 Microsoft identified and announced vulnerability in its Plug and Play service and issued a patch. Within seven days—before most companies could validate and deploy the patch—the Zotob worm struck, bringing down production for several manufacturers, including a number of large automakers and industrial equipment manufacturing plants[1].

Further complicating these issues are the difficulties in deploying patches and effectively implementing and maintaining antivirus protection on many systems in an IACS network. Patches typically need to be carefully qualified, sometimes by the automation vendor, and deployed during scheduled downtime. This increases the period of exposure to vulnerabilities and makes patch management a significant challenge for many manufacturers.

There are many other back doors and potential weak links in IACS networks, including incorrectly configured devices, undocumented connections, wireless networks without proper security configurations, and open ports on the plant floor. These weak links are vulnerable to a variety of threats and must be addressed as a part of any IACS network security architecture.

Impact

Once the requirements, priorities, and threats have been identified, it is important to estimate the impact of a security incident to establish the relative importance of protecting against various attacks. The implications of security incidents are often severe in manufacturing environments, as attacks may interrupt production and result in costly downtime and process startup time.

Security incidents can also result in the loss of critical data. Due to increasingly regulated manufacturing requirements, data from the manufacturing process usually needs to be gathered, stored, and integrated with business applications to maintain a detailed and accessible history of the manufacturing cycle. A related cost impact is the loss of proprietary information related to the manufacturing process, and contained in the IACS applications.

Attacks can have safety and environmental impacts, as well, caused by system availability concerns or deliberate attacks meant to sabotage systems.

Any one of these incidents may not only have a large, direct financial impact, but also can result in noncompliance penalties, a loss of customer satisfaction, and a decline in corporate image and public confidence.

Given the potentially significant impact of security incidents in manufacturing environments, a strong, adaptable security approach is highly recommended. Cisco and Rockwell Automation designed the architecture of the CPwE solution to address the significant implications of system failure and to minimize the risk of incidents while still meeting business objectives. With effective security solutions and procedures in place, many of the security incidents and associated losses described above are, in fact, preventable.

1. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, National Institute of Standards and Technology, special publication (SP) 800-82.

IACS Network Security Framework

This section briefly outlines and describes the key security concepts applied in this solution to maintain availability, integrity, and confidentiality of the plant, the IACS applications and the IACS network. These practices follow a defense-in-depth approach were a number of considerations, techniques and practices are applied within the overall system to protect the system and network. These practices are actually described in more detail in Chapter 5, "Implementing and Configuring the Cell/Area Zone," but are reviewed here to describe the overall security approach this solution endorses.

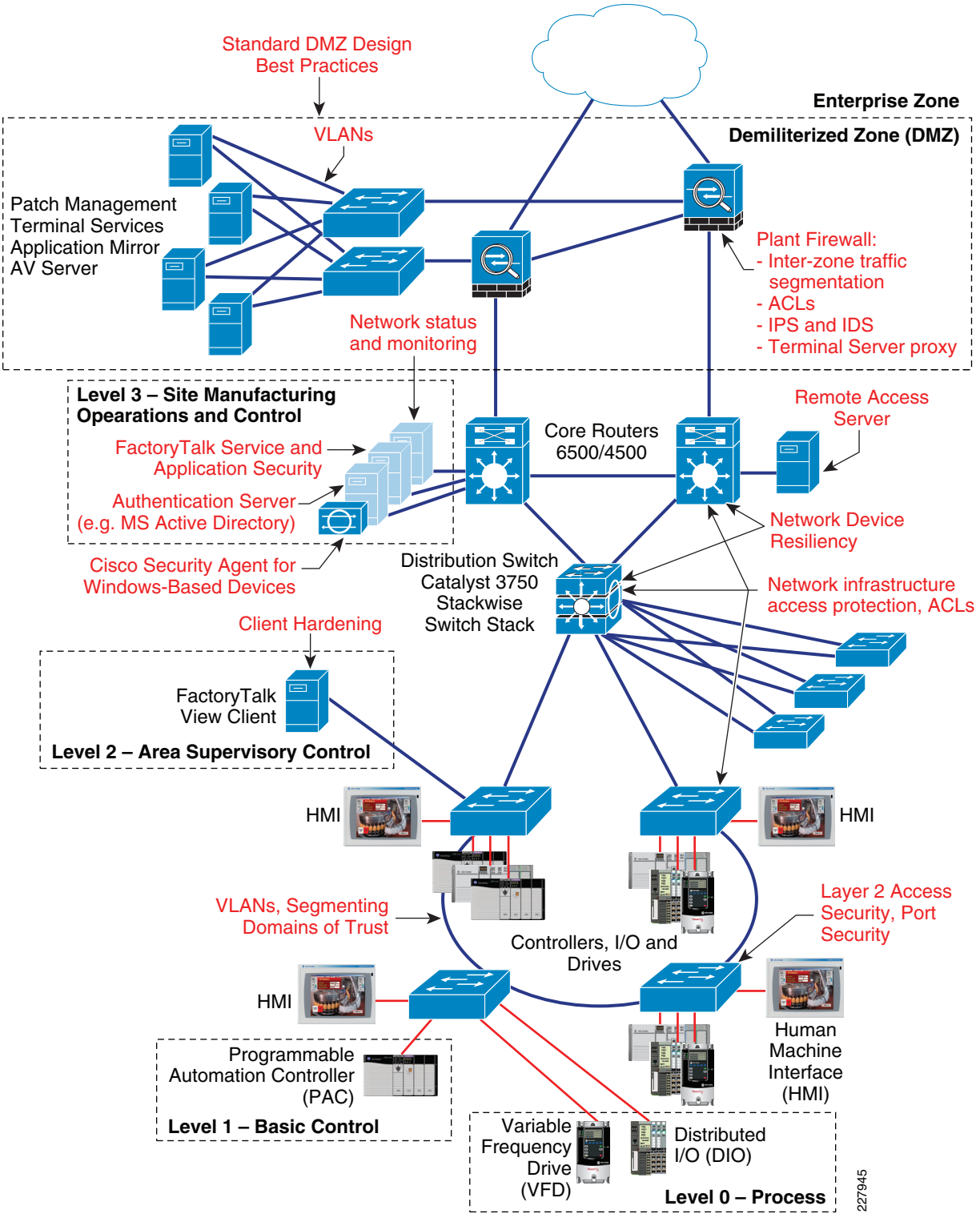
Overview

Security recommendations have been integrated into all recommendations provided in this *DIG*. Figure 6-2 depicts some of the major security recommendations and highlights the defense-in-depth approach.

The recommended IACS network security framework using defense-in- depth includes the following:

- *Manufacturing Security Policy*—This security policy roadmap identifies vulnerability mitigation. A multi-discipline team of operations, engineering, IT and safety should develop this manufacturing security policy.
- *Demilitarized Zone (DMZ)*—This buffer zone provides a barrier between the Manufacturing and Enterprise zones, while allowing users to securely share data and services. All network traffic from either side of the DMZ terminates in the DMZ. No traffic traverses the DMZ, which means that traffic does not directly travel between the Enterprise and Manufacturing zones.
- *Defending the manufacturing edge*—Users should deploy stateful packet inspection (SPI) firewalls (barriers) with intrusion detection/prevention systems (IDS/IPS) around and within the IACS network.
- *Protecting the Interior*—Users should implement access control lists (ACLs) and port security on network infrastructure devices such as switches and routers.
- *Endpoint Hardening*—This restricts access, prevents "walk up, plug in" access and uses change management to track access and changes.
- *Domains of Trust*—Users should segment the network into smaller areas based on function or access requirements.
- *Physical Security*—This restricts physical access to manufacturing assets and network infrastructure devices.
- *Security, Management, Analysis and Response System*—This monitors, identifies, isolates, and counters network security threats.
- *Remote Access Policy*—For employee and partner remote access, implement policies, procedures and infrastructure.

Figure 6-2 IACS Network Security Framework



Foundational Network Security Considerations

The concept of network security is about protecting the network infrastructure itself; protecting the network protocols used to establish and manage the networks functions. These key concepts are applied at all levels and zones of the solution. These steps help to protect the IACS network and IACS applications from a wide range of attacks. The following are the key areas of baseline security:

- *Infrastructure device access*—Securing the management access to the network infrastructure
- *Switching infrastructure*—Network access and Layer-2 design considerations
- *Routing infrastructure*—Protecting the Layer-3 routing function of the network from attack or mis-use
- *Device resiliency and survivability*—Preserve the resiliency and availability of the network
- *Network telemetry*—Monitor and analyze network activity and status to identify and react to issues or attacks

These practices are applied to various levels, zones, and network infrastructure where relevant. Earlier chapters describe the specific security best practices to be applied as well as resiliency and availability features that are designed to maintain high availability of the IACS network and the IACS applications that rely on the IACS network.

IACS Network Device Protection

This concept describes practices to secure the key IACS end-devices themselves, especially the controllers and computers. As these devices have key roles in the IACS, their security is of particular concern. These concepts are described in more detail in Chapter 3, "CPwE Solution Design—Cell/Area Zone," and include the following:

- *Physical security*—This limits physical access of areas, control panels, IACS devices, cabling and the control rooms and other locations to authorized personnel as well as provisions for escorting and tracking visitors and partners.
- *Computer hardening*—This includes patch management and antivirus software as well as removal of unused applications, protocols and services.
- *Application security*—This contains authentication, authorization and audit software such as FactoryTalk Security for IACS applications.
- *Controller hardening*—This handles change management and restrictive access.

Cell/Area IACS Network Security

Chapter 3, "CPwE Solution Design—Cell/Area Zone" covers a number of security topics for this zone. In addition, Chapter 5, "Implementing and Configuring the Cell/Area Zone" covers the implementation of these recommendations. The key security concepts applied to the Cell/Area zone include how to cover the following:

- Port security, password maintenance, administrative access for Cell/Area zone network infrastructure
- Redundancy and disabling un-necessary services
- Network system message logging, SNMP use, and network information to monitor
- Restricting broadcast domains, VLANs and protecting a variety of network protocols

- Computer and controller hardening

Manufacturing IACS Network Security

The Manufacturing zone design considerations and implementation are discussed in earlier sections, especially the key considerations from the Cell/Area zone. In addition to applying those considerations, the key security considerations for the Manufacturing zone include the following:

- Routing infrastructure best practices, covering routing protocol membership and routing information protection as well as routing status change logging.
- Network and security monitoring
- Server security covering end-point security
- FactoryTalk application security

Demilitarized Zone and the IACS Firewalls

The DMZ and plant firewalls are an essential aspect of protecting the IACS network and IACS applications. The combination of firewalls and a DMZ zone concept are key aspects of the defense-in-depth approach for IACS network security. The DMZ and plant firewall design and implementation guidance is provided in Chapter 4, "CPwE Solution Design—Manufacturing and Demilitarized Zones." The key features and functions include the following:

- Deploy plant firewalls to manage traffic between the Enterprise and Manufacturing zones. A plant firewall supplies the following:
  - Establishing traffic patterns between the network zones via assigned Security levels, for example establishing the DMZ
  - Stateful packet inspection of all traffic between the various zones, if allowed by the above
  - Enforce Authentication of users from one zone trying to access resources in another, for example from the Enterprise accessing DMZ services
  - Intrusion Protection Services (IPS) inspecting traffic between the zones designed to identify and potentially stop a variety of attacks.
- A DMZ zone where data and services between the zones can be securely shared

The firewall and DMZ concept also play an important role in allowing remote access to the IACS network. This role is described in more detail in the next section.

Remote Access to the IACS Network

Quick and effective response to issues on the plant floor often requires real-time access to information and status from IACS applications as well as the skills and knowledge to take corrective action or optimize the manufacturing process. Unfortunately, many manufacturers today do not always have key skilled and experienced personnel, such as Control Engineers, available at their global manufacturing facilities. Staffing constraints are often compounded by globalization and wider distribution of manufacturing facilities. Without these personnel readily available, manufacturers cannot quickly respond to events that occur in the manufacturing 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 manufacturing facilities offers a powerful means to help address the skill and resource gap experienced by many manufacturers. Secure remote access to manufacturing 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 Original Equipment Manufacturers (OEMs) and System Integrators (SIs), without needing someone onsite.

This section outlines a mechanism for providing secure remote access to the IACS network and the IACS applications that operate in the Manufacturing zone. This solution assumes that the recommendations in this *CPwE DIG* have been implemented and are in place, especially the plant firewalls and DMZ.

To deploy remote access, Cisco and Rockwell Automation recommend an approach to provide secure remote access based on network services and technology outside of the IACS network and Manufacturing zone, most likely provided by the enterprise IT organization. As such, it is not in the scope of this document to provide detailed design and implementation guidance for that aspect of the CPwE secure remote access solution.

This section discusses the following:

- Technical challenges to deploying remote access
- Guiding principles for establishing remote access
- Use cases considered
- Approach
- Implementation
- Organizational considerations

Technical Challenges

IACS applications have traditionally relied completely on onsite personnel to provide support for IACS applications, 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 IACS 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 IP-based Virtual Private Networks (VPNs), have been around for many years. While encryption and authentication are important components of any solution, successfully applying these technologies to provide effective remote access to IACS applications has been a challenge. This is due to the following reasons:

- IACS applications are often managed by plant personnel, while enterprise-level remote access solutions such as VPNs are the responsibility of the IT organization. Successful implementation of remote access to IACS applications requires collaboration between IT and manufacturing organizations.
- Remote access can expose critical IACS applications to viruses and malware that may be present on a remote or partner machine, potentially impacting manufacturing.
- 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.
- 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 IACS network. When VPN technology has been used, it has often been subject to the challenges identified above, 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. However, access needs to be limited to those individuals who are authorized to access systems, and their authorized actions need to be aligned to corporate and plant policies and procedures.

Guiding Principles for Implementing Remote Access

Several guiding principles should be maintained when allowing remote access to IACS data and resources. These principles were used to develop the Cisco and Rockwell Automation CPwE reference architecture and encapsulate the key concepts of strictly controlling the remote access of IACS 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 IACS data and resources should follow the enterprise's IT processes to grant and monitor access for local and remote users.

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

IACS Network Protocols Stay Home

A key principle outlined in the Cisco and Rockwell Automation CPwE is that "*IACS network protocols stay home*." IACS network protocols such as CIP, the Common Industrial Protocol, FactoryTalk® Live Data, OPC-DA, and Modbus TCP shall be contained to the Manufacturing zone. These protocols and the devices they run on have limited security capabilities compared to their IT counterparts. They also have a significant impact on the IACS and the plant processes as they are used to start, stop, and operate the industrial machinery. Therefore, the IACS network protocols should not leave the Manufacturing zone. In the Manufacturing zone, the IACS 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 IACS 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 IACS network traffic coming for devices outside of the Manufacturing zone. This requires 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, Cisco and Rockwell Automation recommend that the IACS network protocols "stay home."

Control the Applications

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

- Allows the plant to enforce change management, version control, and regulatory compliance of the applications 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 IACS network 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 IACS applications on a remote user's computer introduces significant risk to the IACS and should be avoided as a best practice.

No Direct Traffic

As indicated by the crossed circle in Figure 4-17, 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 IACS applications, because patches are typically validated in a test environment before being deployed into IACS applications. Remote access to devices on the IACS 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 IACS 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 4-17. This prevents worms like slammer to get through the upper firewall and infect a system in the DMZ from propagating into the Manufacturing 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 IACS applications rather than trusting that remote users are doing the right thing when accessing the IACS 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 IACS 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 CPwE solution focuses on deploying real-time access to IACS data and applications for users who are monitoring or problem-solving issues or activities in the manufacturing environment. The roles may be filled by either internal or external personnel, but it is assumed that they are identified in advance. This section of CPwE 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 CPwE is that users are known in advance and will typically have long-term or repeated access to IACS applications. 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.

Another use case is when plant personnel need to integrate an external expert who is not known before hand or is not established to access the Enterprise VPN. To enable remote access in this case, use of collaboration technology, such as Cisco's WebEx, could be used to share a desktop/laptop in the Manufacturing zone that is running a relevant application that the expert can use to help analyze and resolve plant floor issues. This mechanism does not per se violate any of the guiding principles, but it should be noted that the external expert is not authenticated to the enterprise network and does not access the enterprise network. This is a common solution used to provide remote access on an ad-hoc basis. This solution has not been included in this version of the *CPwE DIG*. For the purposes of this *DIG*, Cisco and Rockwell Automation do not make any recommendations on the use of this mechanism. Those using this adhoc solution should take caution as the external access is not audited and many of the security considerations included in the adhoc solution herein are performed by the collaboration technology, which may not apply the same level of encryption, authentication, audit and authorization.

Location

This CPwE solution 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.

CPwE 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. These methods may be used in conjunction with the specified techniques to provide remote access described in CPwE, 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 chapter.

Architectural Approach

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

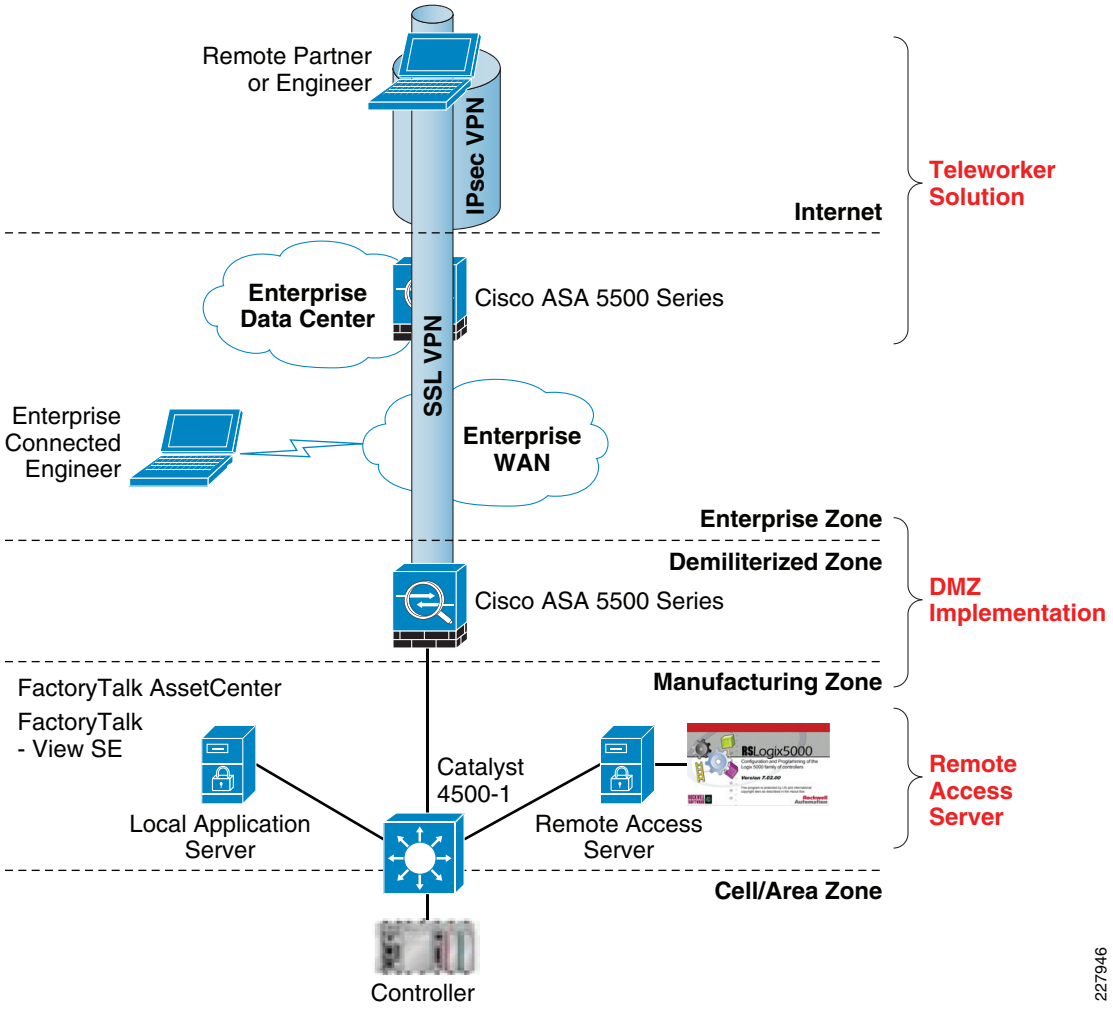
- Best-practice enterprise teleworker solutions implemented and operated by most IT organizations
- Cisco and Rockwell Automation Converged Plantwide Ethernet Architecture with implementation of a DMZ with modern firewalls managing and inspecting traffic into and out of the DMZ

When considering implementing remote access, the following questions 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 use?
- Do they have a "partner" remote access policy —the ability and process to add partners (OEM, SI, vendor, contractor)?
- For partners, is your solution ready to be integrated into your customer's IACS network infrastructure? Does your solution support remote access? Is your solution aligned with emerging IACS security standards such as ISA-99 and NIST 800-82.

With these capabilities and security policies in place, the key to implementing remote access to the IACS environment is the implementation and configuration of the remote access server. Figure 6-3 shows a simplified version of the remote access architecture.

Figure 6-3 Simplified Remote Access



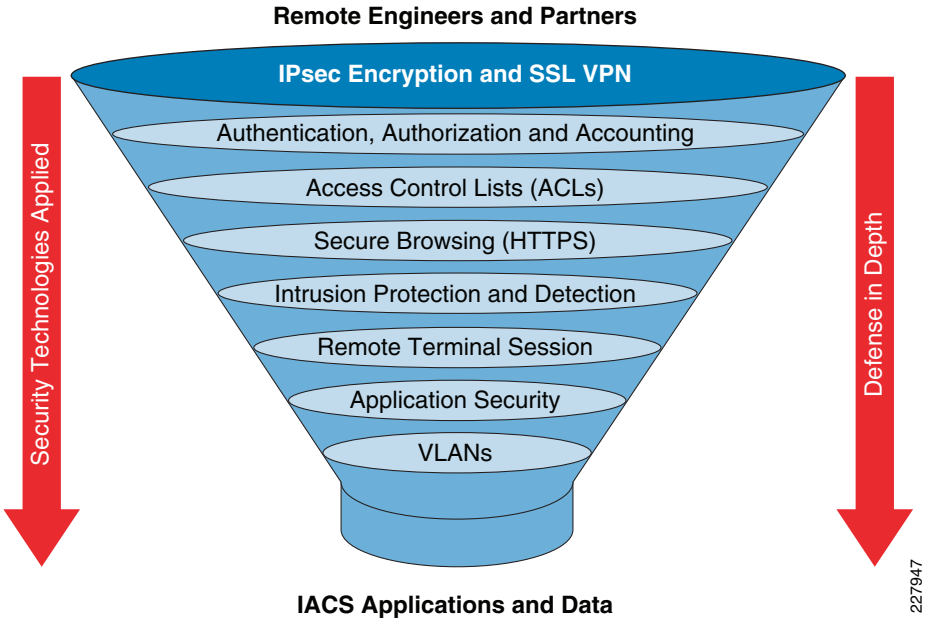
The DMZ is designed to allow sharing data and applications with users or applications not local to the manufacturing environment. A common means would be to replicate critical data onto a server in the DMZ to allow users/applications in the other zone to have visibility to that data. The DMZ is a proxy, 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 IACS 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 IACS applications on a dedicated remote access server in the Manufacturing zone. The recommended security mechanisms highlighted in this *CPwE DIG* 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 IACS applications 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 *CPwE DIG* 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 IACS applications 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 IACS applications is consistent with the existing IACS architecture and applies defense-in-depth concepts with a number of key security solutions. Although there is no single technology or methodology that fully secures IACS 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 6-4 depicts the security technologies that give remote engineers and partners access to IACS applications.

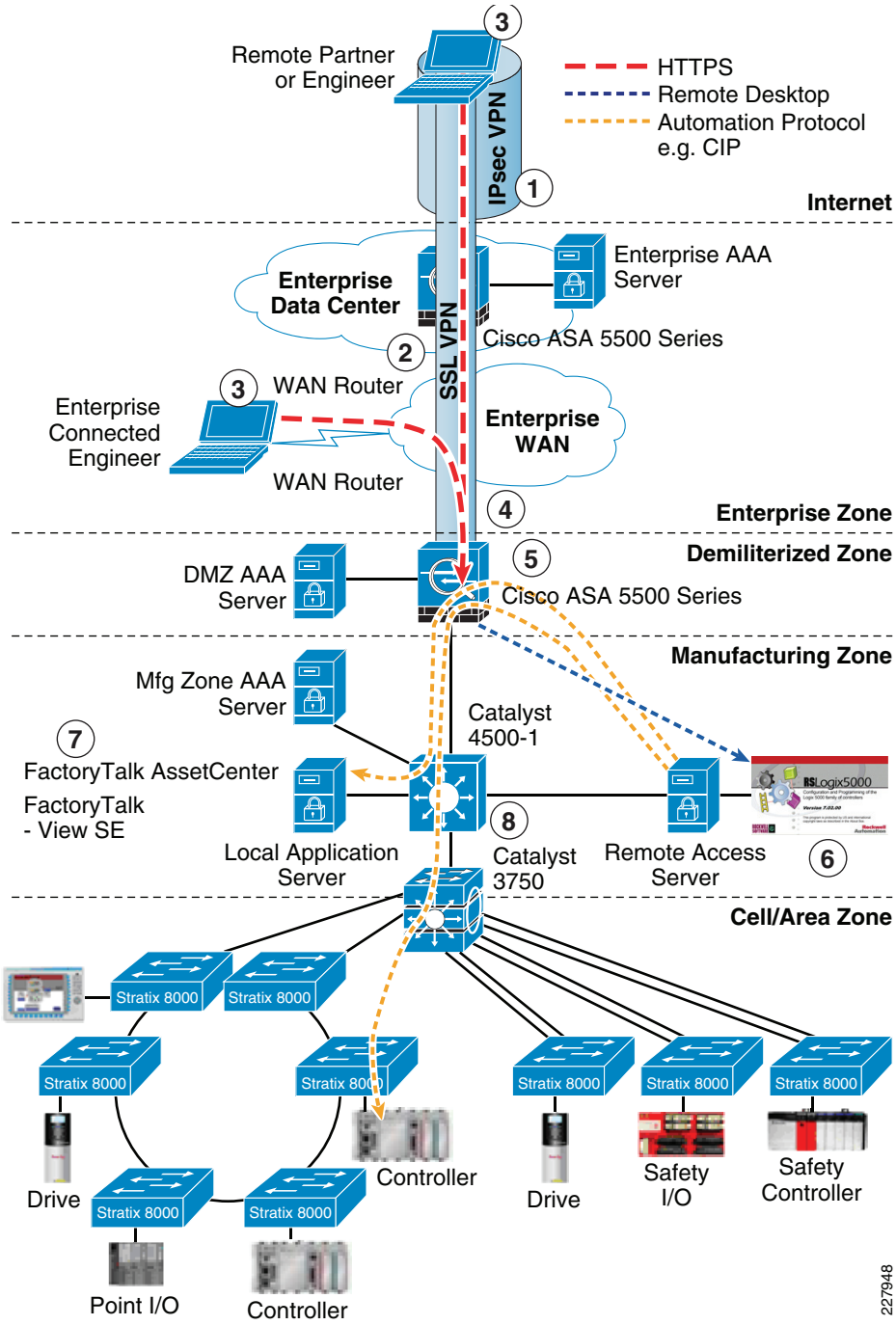
Figure 6-4 Defense-in-Depth Approach for Secure Remote Access



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 IACS applications and data in real time. This section discusses how the various security technologies are applied, the flow of traffic through the network infrastructure, and which network protocols make up that traffic. Figure 6-5 shows the steps to implement remote access to IACS applications.

Figure 6-5 Detailed View of Remote Access to Industrial Automation and Control Systems



The following steps provides the details for Figure 6-5:

Step 1 Use standard enterprise remote access solutions in the form of client-based, IPSec12 encryption VPN technology to connect to the enterprise edge and for confidentiality over the Internet. The establishment of a VPN requires RADIUS13 authentication of the remote person and is typically implemented and managed by the IT organization.

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

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

Step 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 session15 (e.g., Remote Desktop Protocol) over HTTPS.

Step 5 Use 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.

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

Step 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).

Step 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.

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).

The recommended architecture described in CPwE uses 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 used 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), often established with some type of a RADIUS server. In addition, enterprise IT organizations may even have established Network Access Control (NAC) 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 CPwE 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 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 6-5. These ACLs are usually managed and maintained by IT network operations or security teams.

Use Secure Web Browsers Supporting HTTPS

All interaction with 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.

Use of browsers suggests that client-based applications should not be used for remote access to IACS 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 further protects 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 is 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 CPwE 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.

Remote Terminal Session to Remote Access Server

Once secure browser connectivity has been established to the 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 prompts the user to authenticate using a RADIUS server before being authorized to access the remote access server. The plant firewall (such as Cisco's ASA 5500 Series Firewall Edition) should come 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.

IACS Applications on Remote Access Server

The remote access server hosts the approved IACS applications, such as FactoryTalk® View or RSLogix™ 5000. By executing applications on a secure, dedicated server, the plant floor personnel can strictly enforce change management, version control and regulatory compliance 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 users of the application server editing the registry or making themselves local windows administrators. Cisco and Rockwell Automation recommend following the guidelines in the *Securing Manufacturing Computing and Controller Assets* at the link below. These guidelines recommend that endpoint security such as antivirus and/or Cisco Security Agent be applied to the remote access server. For more information, refer to the following URL:

http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp005_-en-e.pdf

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 IACS VLANs, thereby further limiting a remote user's view of the Manufacturing zone.

Organizational Considerations

As with any IACS networking solution, successful implementation of remote access capabilities typically require a combination of IT and plant floor resources. It is important that both organizations agree on 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. In Table 6-1, the responsibilities are split between manufacturing and IT at the plant firewalls; IT is responsible for firewall configuration, especially the upper firewall instance. In many cases, as shown below, manufacturing and IT will collaborate on the design, implementation and operation of the DMZ. Manufacturing 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 manufacturing work together well, IT may take certain network design, implementation, and operational responsibilities in the Manufacturing zone.

Table 6-1 Example Breakdown of IT and Manufacturing Responsibilities

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

Figure 6-6 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 6-6 Example IT and Manufacturing Areas of Responsibility