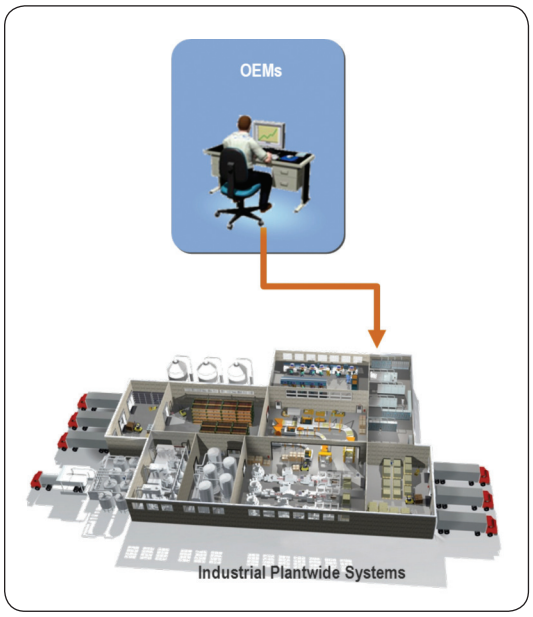
Scalable Secure Remote Access Solutions for OEMs



Introduction

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. OEMs are looking to reduce costs, add more value to their manufacturing customers and differentiate themselves from their competitors. This paper outlines the means to enable secure remote access to plant-based applications & data and can be used as guidance for OEMs to collaborate with their customers when designing a secure remote access

Technical Challenges

OEMs have traditionally relied on deploying onsite personnel to provide support for industrial automation and control systems (IACS), or used methods such as standalone dial-up access without using a firewall. This method of Remote Access often circumvents perimeter security, creates the threat of a "back door" into the manufacturing system and can represent a significant security risk. As OEMs want to provide secure support remotely, and respond to issues in real time, this method is no longer sufficient.

Technologies for remote access to traditional enterprise networks have been around for quite some time, such as Virtual Private Networks (VPNs). However, successfully applying technologies to provide effective remote access to IACS has been a challenge.

This is due to a number of reasons:

- IACS is 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 IACS 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 computer, 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.
- 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.
- One size does not fit all. An IACS remote access solution that works for one customer may not be sufficient for another. An IACS remote access solution that is required by one customer may be too burdensome or even impractical for another. As noted below, a viable remote access solution is dependent upon industry requirements, customer requirements (security policies and procedures), customer size and their support infrastructure.

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 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, access needs to be scalable, regardless of location or company. Access needs to be secure to effectively communicate, diagnose problems, and implement corrective actions. Access needs to be limited to those individuals that are authorized to access systems, and their authorized actions need to be aligned with corporate and plant policies and procedures.

When collaborating with your customer to implement remote access to your IACS solutions (e.g. machine), the following questions will help identify the organization's level of readiness:

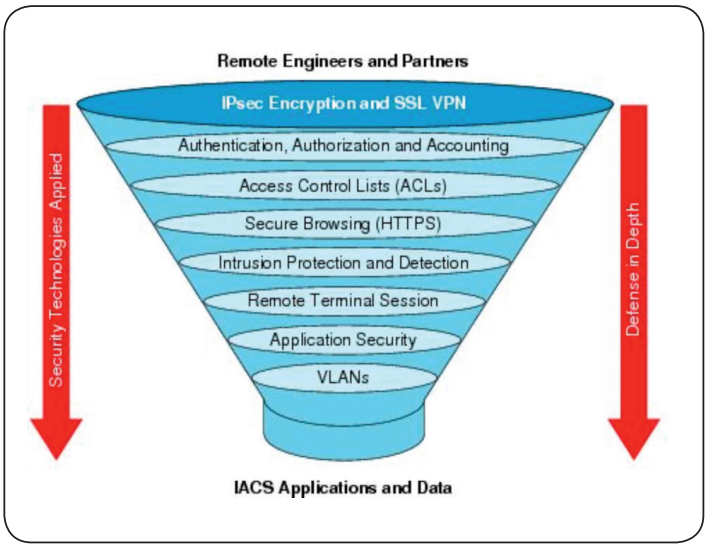
- Do they have an IT security policy?
- Do they have an IACS security policy?
- Do they have a remote access policy for employees and the infrastructure to support? What VPN technology/products do they utilize?
- Do they have a "partner" remote access policy - the ability and process to add partners (OEM, SI, automation 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 established IACS security standards such as ISA-99 and NIST 800-82?

Some other key considerations include:

- Monitoring and auditing activities of remote users to identify misuse
- Determine if there are any "line of site" (visual requirements) or other restrictions that need to be identified prior to allowing certain remote access capabilities
- Define what software tools are allowed for remote access

Principals of Secure Remote Access

When designing a Secure Remote Access solution, a "Defense-In-Depth" approach should be implemented. This approach creates multiple security layers that address the different potential threats that could occur in a remote access scenario. Although there is no single technology or methodology that fully secures IACS networks, combining multiple security technologies forms a strong deterrent to most known types of threats and security breaches, while limiting the impact of any compromise. To ensure a comprehensive "Defense-In-Depth" security program, companies need to rely on multiple types of controls.



These controls can be categorized as:

- Administrative
  - Mostly security policies and procedures.
  - Examples include: password policy, security awareness training, etc.
- Technical
  - Also called "logical" controls and consist of hardware, software and electronics to monitor and control access to information systems.
  - Examples include: firewalls, IPS/IDS, smartcards, etc.
- Physical
  - Mostly mechanical controls to monitor and control physical access
  - Examples include: locks, security guards, security cameras, etc.

Its important to remember that its not just about the technical controls and that a complete security program includes Administrative, Technical, and Physical controls. The diagram above is an example of technical controls that can be implemented to create a "Defense-In-Depth" strategy.

Approach

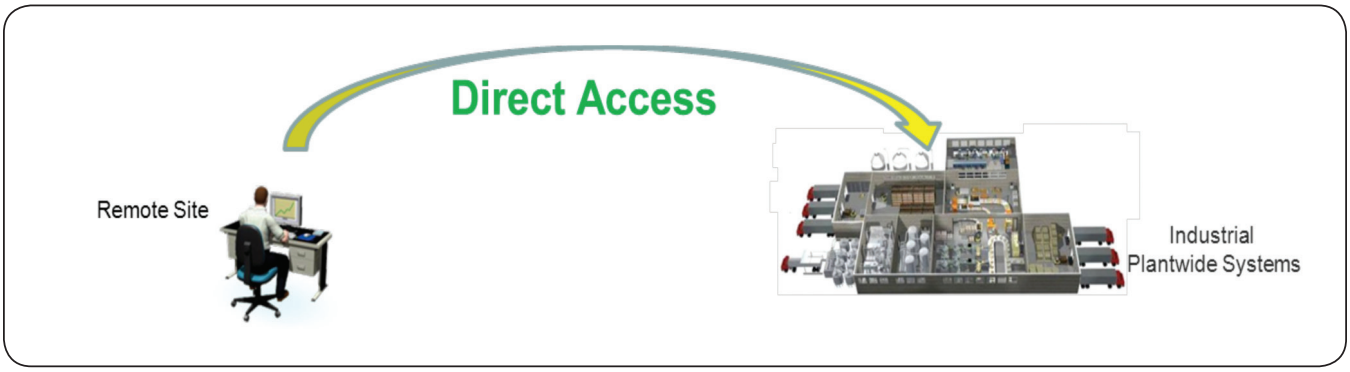
There are several approaches to providing Secure Remote Access to an IACS, two of which are Direct and Indirect Access. The choice of these approaches is dependent upon the criteria previously noted such as customer security policies and procedures. Each approach has several design considerations that could impact the proper operation of the IACS and should be accounted for in the design and implementation of an IACS remote access solution.

Direct Access

Direct Access allows the remote user to establish a secure connection "directly" to the IACS. After creating a secure VPN tunnel, the software on the remote user's computer, initiates communication directly with the IACS.

- **Design Considerations – how will these be enforced?**
  - Network and application authentication and authorization
  - Change management, version control, regulatory compliance, and software license management
  - Health management of the remote client (computer)
  - Alignment with established IACS security standards

NOTE: Though little to no IT support is required when following this approach, best security practices should be in alignment with established IACS Security Standards.

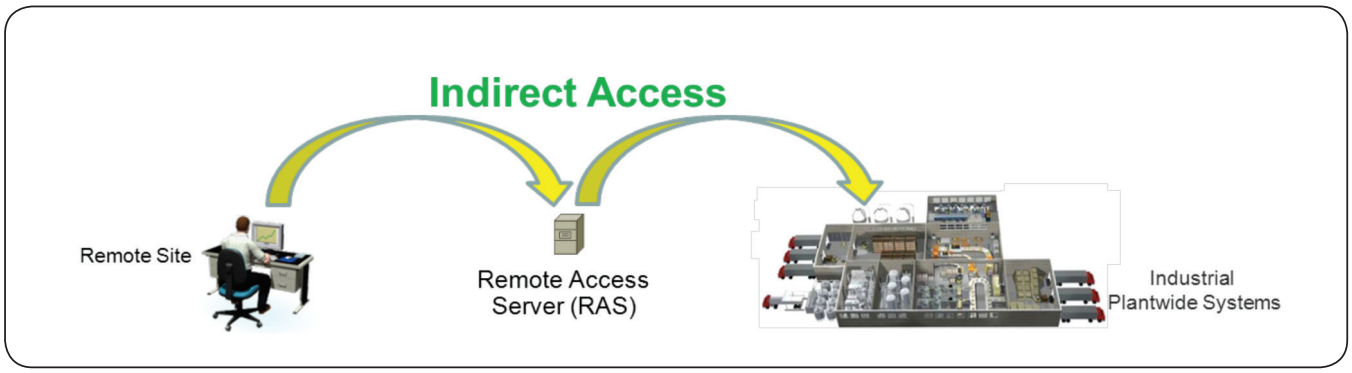


Indirect Access

Indirect Access allows the remote user to establish a secure connection to the IACS through an intermediary server usually residing in the DMZ (Demilitarized Zone) providing remote gateway access to a Remote Access Server (RAS) in the IACS. The remote client uses either a thin client software application or a web browser to establish a connection to the RAS once the VPN session has been established.

- **Design Considerations**
  - Multiple layers of network authentication and authorization
  - Simplified asset management – change management, version control, regulatory compliance, and software license management
  - Simplified health management of the remote client
  - Greater alignment with established IACS security standards

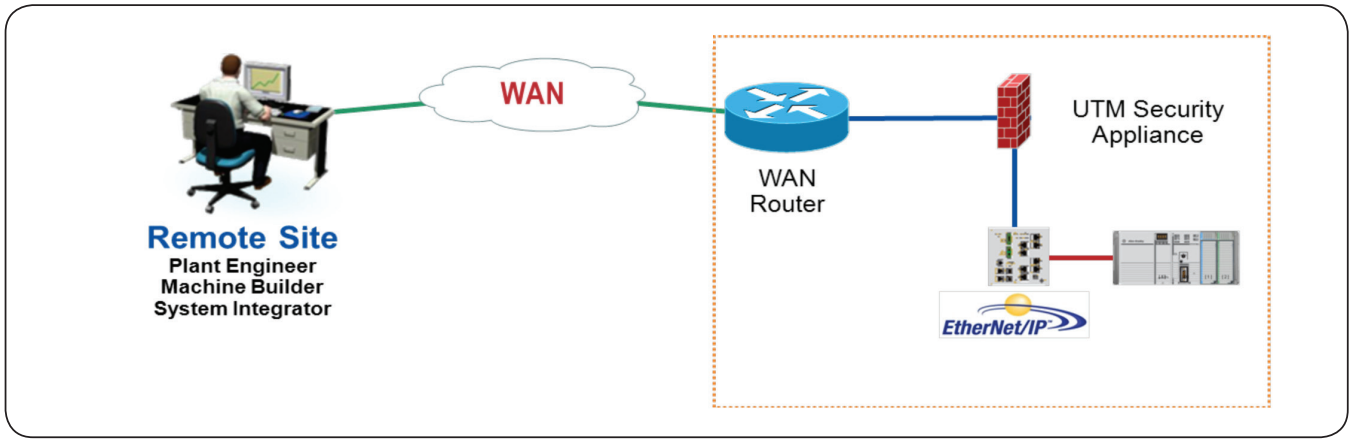
NOTE: Indirect Access is the preferred approach due to greater alignment with established IACS security standards. As such this is the approach recommended by the Cisco and Rockwell Automation Converged Plantwide Ethernet (CPwE) architect team.



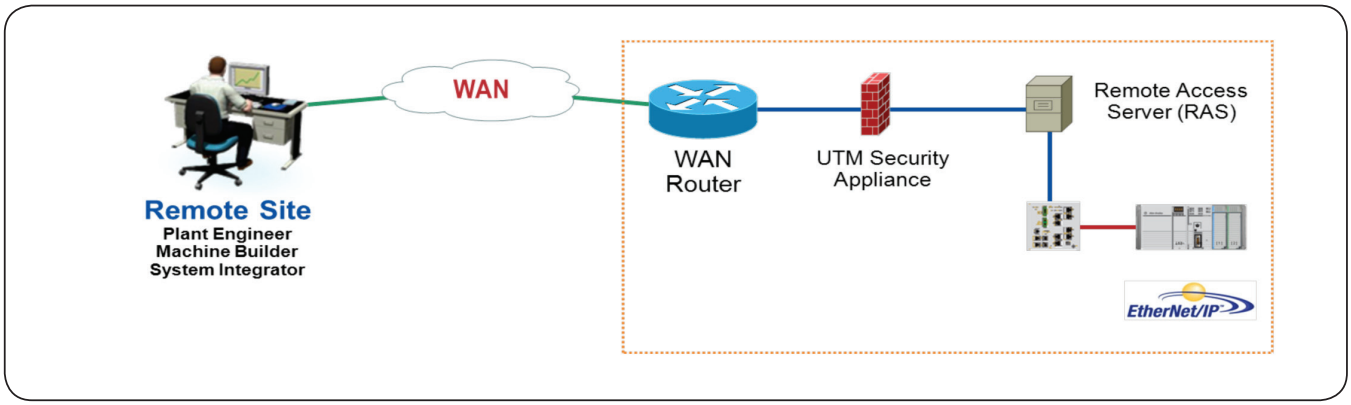
When analyzing Secure Remote Access solutions you must be determine whether the type of system(s) that needs to be accessed, are stand-alone isolated IACS or an enterprise integrated IACS.

- **Stand-alone Isolated IACS Representative Example**
  - Small manufacturing plant, could be small single-operator shops, remote location (not enterprise-integrated), with few automated machines
  - Little to no IT support with minimal to no security policies
  - Little to no alignment with established IACS security standards
- **Enterprise-Integrated IACS Representative Example**
  - Larger manufacturing plant
  - Industrial network interfaces with the enterprise network
  - Strong IT presence with defense-in-depth security policies
  - Alignment with established IACS security standards

Example: Direct Access for Stand-alone IACS

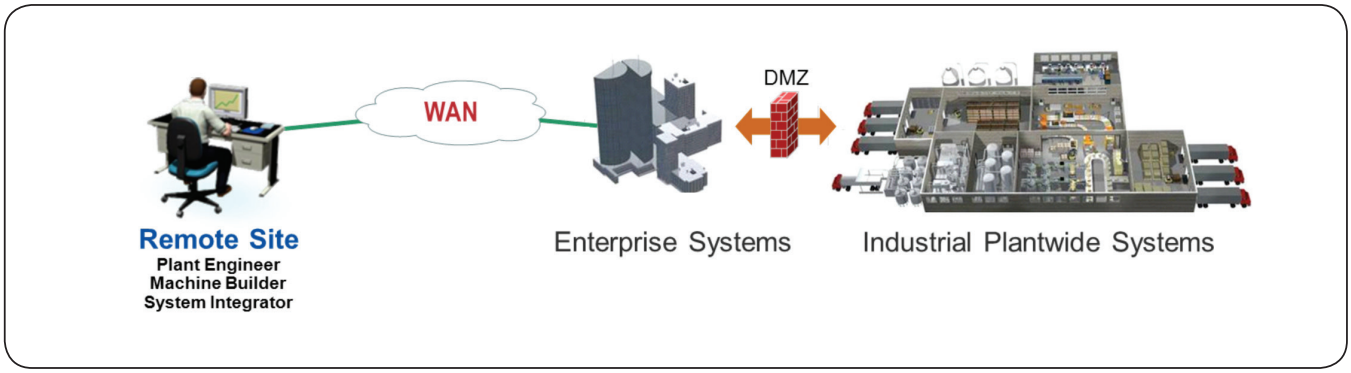


Example: Indirect Access for Stand-alone IACS (Preferred Approach)



Example: Indirect Access for Enterprise-Integrated IACS (Preferred Approach)

(Larger manufacturer with production (manufacturing) and business (IT) systems integration)



Potential Remote Access Solutions

Dial-up Modems

Modems have traditionally been an overlooked "backdoor" remote access method for IACS applications. They are typically the least preferred method to access an IACS. However, if this is the remote access method decided upon based on remote access policy and physical infrastructure limitations, then a multilayered security approach should be taken as well as disconnecting the power to the modem when not in use.

The modem should have the following capabilities:

- Configurable Dial-In Accounts
- Caller ID, allowing only authentication to certain programmable phone numbers
- Call Back features
- Encrypted Authentication

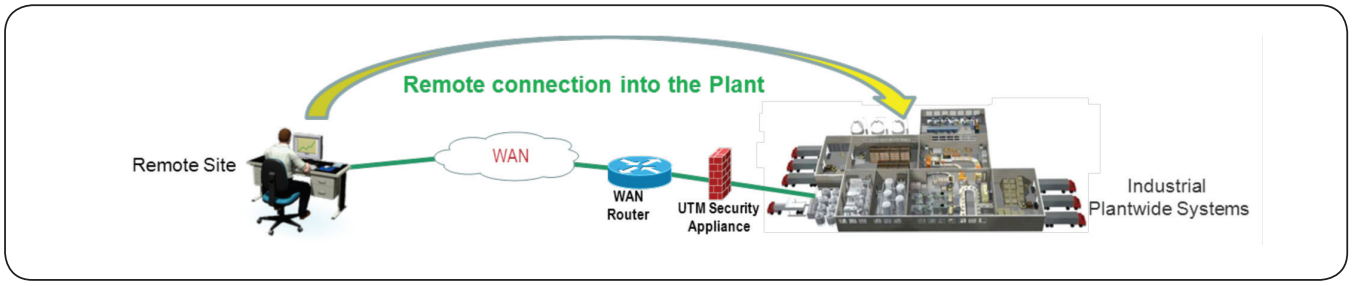
In addition to deploying a modem with built-in security, other layers of defense should be employed as well. Some of these defenses include: implementing a CIP enabled firewall, establishing an IPsec or SSL VPN, configuring an intrusion detection/prevention system (IDS/IPS), providing anti-virus protection, etc. Most modern firewalls provide multiple layers of security in a single box often referred to as a Unified Threat Management device (UTM).

NOTE: For further guidance on modem security please refer to:

- Department of Homeland Security – Recommended Practice for Securing Control System Modems
  - http://www.us-cert.gov/control_systems/practices/documents/SecuringModems.pdf
- Rockwell Automation Network and Security Services
  - http://www.rockwellautomation.com/services/security/

Remote connection into the Plant (WAN Routers/Modems: DSL, Cellular, Satellite, Cable, T1's, etc.)

When traditional modems are not an option due to the infeasibility of installing phone lines, cellular access to establish a WAN connection provides an excellent alternative. This is becoming a popular option due to the increasing coverage area, speed, cost and convenience.



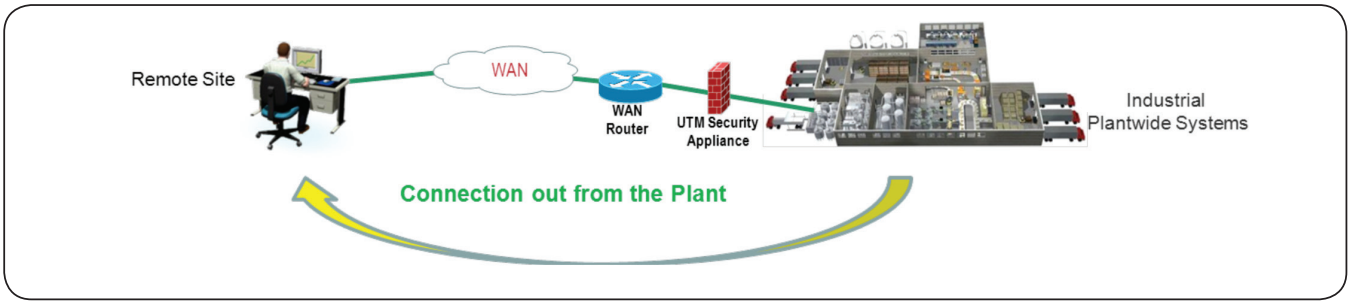
However, as stated above regarding dial-in modems, cellular WAN connections using cellular modems and routers should be used in conjunction with other security technologies to provide "Defense-In-Depth" or at a minimum have these features built into the device (UTM bundle). Other WAN connectivity options include: DSL, Cable, T1's, Satellite, etc. The type of connectivity that will be used to establish WAN connectivity to the standalone system will be dependent upon the manufacturer's location, budget constraints, and access policy. One thing to note is that when implementing a VPN, typically a static IP address would need to be assigned by the WAN provider.

The following are some security features to look for when designing a solution:

- Does it have VPN capabilities? SSL? IPsec?
- Does it provide a firewall?
  - Does it filter industrial protocols? CIP, Modbus, etc.
  - Deep Packet Inspection?
- NAT (Network Access Translation)?
- Is it built for industrial use?
- Anti-virus, Spam filtering?
- Can it provide auditing?
- Does it have an intrusion detection and/or prevention system?

Connection out from the Plant (Webex, GoToMyPc, Gateway VPN devices, etc)

End user initiated connections can also provide secure remote access capabilities provided the control system has personnel onsite and that there is already secure internet connectivity established using multi-layer security controls. The remote support person can request a remote session using technologies such as Webex, etc.



However, the PC/Laptop onsite would need to have all the necessary software installed to provide remote capabilities as well as IT configuring the necessary rules to allow outbound access.

The risk of opening up outbound connections to the internet (http/https) to use such services should not be overlooked and should be restricted to certain sites and IP addresses to prevent browsing the web from the control systems. The use of web browsers can pose significant risk and have been known to be a source of attacks.

Another solution is a "Gateway VPN" device that resides in the control system and establishes remote access through a "Hosted VPN" service. Care should be taken with this solution to analyze the "Hosted" service provider, their location, whether they are adhering to best security practices, and are aligned with established IACS security standards, such as ISA-99 and NIST 800-82, as well as meet the security requirements of the manufacturer's security policy.

Enterprise-Integrated IACS

Potential Solution

- Rockwell Automation & Cisco CPwE Secure Remote Access solution
  - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp009_-en-e.pdf

Customized Solutions

For customized solutions, Rockwell's Network and Security Services Team can design a secure solution that meets your needs.

- http://www.rockwellautomation.com/services/networks/
- http://www.rockwellautomation.com/services/security/

Summary

The evolution of secure remote access capabilities allows OEMs to improve productivity, reduce cost and respond more quickly to events that impact their customer. By using these Secure Remote Access solutions the OEMs can provide real time remote support. 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 for standalone systems give OEMs 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.

Given the critical nature of IACS applications, however, its important that any remote access solution provides the appropriate levels of security to meet the needs of the manufacturer and align with established IACS security standards. Applying the principles of "Defense-In-Depth" ensures that there is never direct unsecure remote access to an IACS application.

Additional Resources

Alliance Member

- Cisco – Integrated Services Routers

  - http://www.cisco.com/en/US/products/ps10906/Products_Sub_Category_Home.html

Rockwell Automation

- Remote Access Modems

  - http://www.rockwellautomation.com/services/onlinephone/modems/

Encompass Partners

- http://www.rockwellautomation.com/encompass/

Glossary of Terms

CIP - Common Industrial Protocol

The Common Industrial Protocol (CIP) encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications – control, safety, synchronization, motion, configuration and information. CIP is owned and maintained by the ODVA. The ODVA is an international association comprising members from the world's leading automation companies.

DMZ - Demilitarized Zone

Refers to a buffer or network segment between two 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/solutions/Verticals/CPwE/CPwE_chapter4.html#wp1050554

IACS - Industrial Automation and Control Systems

Refers to the set of devices and applications used to automate and control the relevant manufacturing process. Rather than use various terms with a similar meaning (e.g., production systems, plant floor systems, we standardized on this term for use in this paper). That is not to suggest any specific focus or limitations. We intend that the ideas and concepts outline herein are applicable in various types of manufacturing including but not limited to batch, continuous, discrete, hybrid and process. Other documents and industry references may refer to Industrial Control Systems (ICS). For the purpose of this document, those terms are interchangeable. This document use IACS, as reflected in the ISA 99 standards, and is aligned with the Cisco and Rockwell Automation Converged Plantwide Ethernet (CPwE)

IPA-3 - Internet Protocol

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

IP Protocol Suite

A set of networking standards on which the internet and most enterprise networking is based. It includes the Layer 3 Internet Protocol (IP), the Layer-4 Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

IPS - Intrusion Prevention Systems

A network security device that monitors network activity for malicious or unwanted behavior. See more on Intrusion Prevention Systems at wikipedia: 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

Focuses on security for industrial automation and control systems. For more, see:

http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

Manufacturing Zone

A network zone in the Plant Logical Framework as shown in Chapter 2 of the Cisco and Rockwell Automation Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. The zone contains the complete set of applications, systems, infrastructure and devices that are critical to the continued operations of the plant. In other documentation (for example ISA 99), this zone may also be referred to as the Control zone. The terms are interchangeable in this regard.

NAT - Network Address Translation

Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.

Plant - Production Facility, Factory or Factory Floor

This document chose to use the term plant as a keyword to describe the area in which the manufacturing process and control takes place. This is not to exclude similar words such as factory, production facility, or any other term used to refer to the area in which the manufacturing process exists. In fact, they can be used interchangeably, but for the purpose of consistency, the term Plant is used.

Remote Terminal Session

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 appears 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.

Subnet or Subnetwork

In IP networks, a subnet is a network sharing a particular subnet address. Subnetworks are networks arbitrarily segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks.

UTM - Unified Threat Management

A comprehensive solution that has recently emerged in the network security industry and since 2004, has gained widespread currency as a primary network gateway defense solution for organizations.[1] In theory, it is the evolution of the traditional firewall into an all-inclusive security product that has the ability to perform multiple security functions in one single appliance: network firewalling, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data leak prevention and on-appliance reporting.

See more on UTM at Wikipedia: http://en.wikipedia.org/wiki/Unified_threat_management

VPN - Virtual Private Network

A network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or traveling users an access to a central organizational network. VPNs typically require remote users of the network to be authenticated, and often secure data with encryption technologies to prevent disclosure of private information to unauthorized parties. VPNs may serve any network functionality that is found on any network, such as sharing of data and access to network resources, printers, databases, websites, etc. A VPN user typically experiences the central network in a manner that is identical to being connected directly to the central network. VPN technology via the public Internet has replaced the need to requisition and maintain expensive dedicated leased-line telecommunication circuits once typical in wide-area network installations.

See more on VPNs at wikipedia: http://en.wikipedia.org/wiki/VPN

WAN - Wide Area Network

A wide area network (WAN) is a telecommunication network that covers a broad area (i.e., any network that links across metropolitan, regional, or national boundaries). Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations. In essence this mode of telecommunication allows a business to effectively carry out its daily function regardless of location.

http://en.wikipedia.org/wiki/Wide_area_network

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication ENET-WP025A-EN-E – March 2012