WHITE PAPER

invensys®

PROCESS CONTROL NETWORK SECURITY—REFERENCE ARCHITECTURE

LifeTime PERFORMANCE

WHAT'S INSIDE:

1. GENERAL INFORMATION

This document describes the reference architecture of best practices for a process control system network and its interfaces to a corporate network.

Its objective is to give the reader an understanding of the techniques utilized to securely connect these networks.

This discussion will not address every possible network configuration and requirement, as this will vary with individual customer configurations.

2. EXECUTIVE SUMMARY

Invensys' approach to site network and control system security is based on the following principles:

- View security from both management and technical perspectives
- Ensure security is addressed from both an IT and control system perspective
- Design and develop multiple layers of network, system and application security
- Ensure industry, regulatory and international standards are taken into account
- Prevention is critical in plant control systems, supported by detection

The first stage in building a solid defense against unwanted intrusion into business network and process control systems is to develop a security policy statement and then define the requirements to implement a secure process environment. Once security goals are clear, a detailed plan can be developed to the customer's needs.

Site Security Review Service is the initial step in Invensys' overall Network Security Services program to assist clients in defining clear security objectives and establishing an ongoing control system and site network security plan.

The next step for customers with IA Series® systems is the comprehensive System Security Hardening Service, which implements Site Security Review recommendations specific to the security of the control system network. System Security Hardening Service assists in tightening — i.e., hardening — the security of the control system against undesirable internal and external intrusion.

3. BACKGROUND

Developing a prevention approach to plant control systems requires a close examination of network security between the plant network layer and business/external systems. This document addresses the key network/technology areas for architecting plant and business network systems.

Today's production environments rely heavily on computer-based control systems to precisely control their processes. Historically, process control was operated as a separate network with no connection to IT business networks. Most process control networks have no consistent security design and until recently, many were implemented with no security or minimal security.

Current technology advances with open systems and the increasing demand for information are driving tighter connectivity between the two networks. An increasing number of companies are now leveraging the wealth of process data available from the controllers to provide feedback to the business systems. Devices in use on the process control network have the ability to gather real-time information about the process and have the ability to adjust to commands from the business network.

Many control systems share the same underlying operating systems that are widely used in the business network. As these two networks converge, it becomes critical the process control network is secure and protected from the threat of virus and worm infections faced by business networks. The threats from both internal and external sources have increased significantly. Ernst & Young reported in their "Information and Security Survey" that 60% of organizations expect to experience greater vulnerability as connectivity increases.

There are numerous incentives to protect business and control system networks from threats. The technical knowledge, skills and tools required to penetrate IT and plant systems are widely available. In addition, there are increasing regulatory mandates and guidelines issued by the US Government, as well as guidelines and best practices for securing plant control systems from advisory groups such as the ISA SP99 committee, NIST (Process Control Security Requirements Forum-PCSRF), NERC, etc.

As a result, it is vital that the security environment is now approached as a collaborative effort between Corporate IT and the process engineers to ensure reliability and stability of all segments of the overall network.

Invensys is recommending a network architecture for integrating plant and IT networks using a combination of firewalls, intrusion detection/prevention devices placed at strategic locations in the network, station lock-down procedures for services on the UNIX and Windows platforms and policy settings.

4. REQUIREMENTS

The security plan and architecture needs to address the following requirements:

- A prevention philosophy must be maintained to support security policies and procedures using:
  - Firewalls
  - Network-based intrusion prevention/detection
  - Host-based intrusion prevention/detection
- Clearly defined change management policy and committed IT resources for on-going administration
- Secure and unsecure protocols on the same network
- Monitoring, alerting and diagnostics of plant network control systems and their integration with the corporate network

- Need to move to an off platform data collector in a DMZ
- Retention of forensic information to support investigation/legal litigation
- Ensure secure connectivity to wireless devices

5. TECHNICAL OPTIONS

The approach is to segment the network into several zones. Each zone has a different set of connectivity requirements and traffic patterns. Segmentation is obtained by placing firewalls at strategic locations. Intrusion detection and prevention systems are deployed at key locations and alerts are reported to a monitoring center.

Network Overview — Multiple Zone Network

This configuration illustrates a design that provides four levels of overall security. The major zones or network areas are Internet, Data Center, Plant Network, and Control Network. There are additional zones to supplement the installation. The zones are detailed in the following sections. Each zone is separated by a firewall. Secure network design dictates that the perimeter firewall is from a different manufacturer to provide maximum resistance to penetration. While the diagram Figure 1 illustrates a single firewall, these may be a pair of high-availability units in a fail-over mode. For networks that require real-time or near real-time communications to the process control network, it is recommended that at a minimum this device is a high-availability or redundant unit.

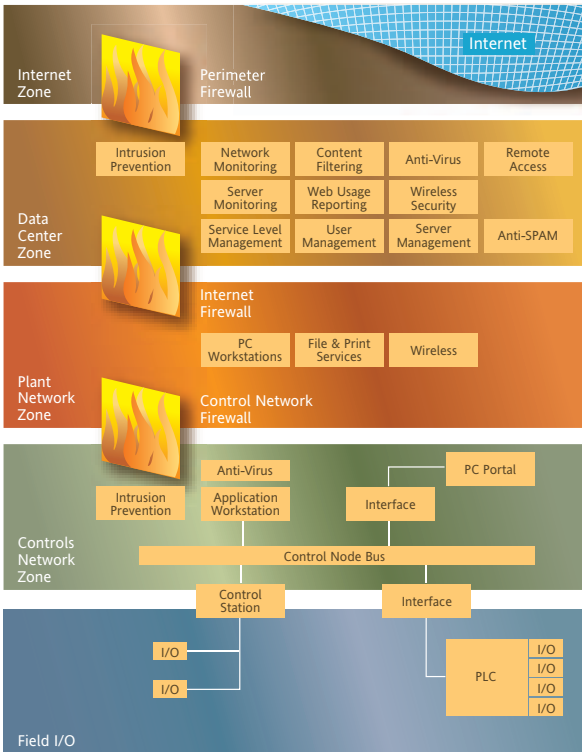


Figure 1 - Multiple Zone Network

Security Layers, Rings or Zones

The network is divided into the following major zones:

Field I/O — Communications that occur in this zone are typically direct hardwired communications between the I/O devices and their controllers. Security is accomplished by physical security means.

Controls Network Zone — This is the zone with the highest level of security. It is the network that carries the process control device communications. Traffic on this network segment must be limited to only the process control network traffic as it is very sensitive to the volume of traffic and protocols used.

Plant Network Zone — This zone carries the general business network traffic, (messaging, ERP, file & print sharing, and Internet browsing, etc.) This zone may span multiple locations across a wide area network. Traffic from this zone may not directly access the Control Network Zone.

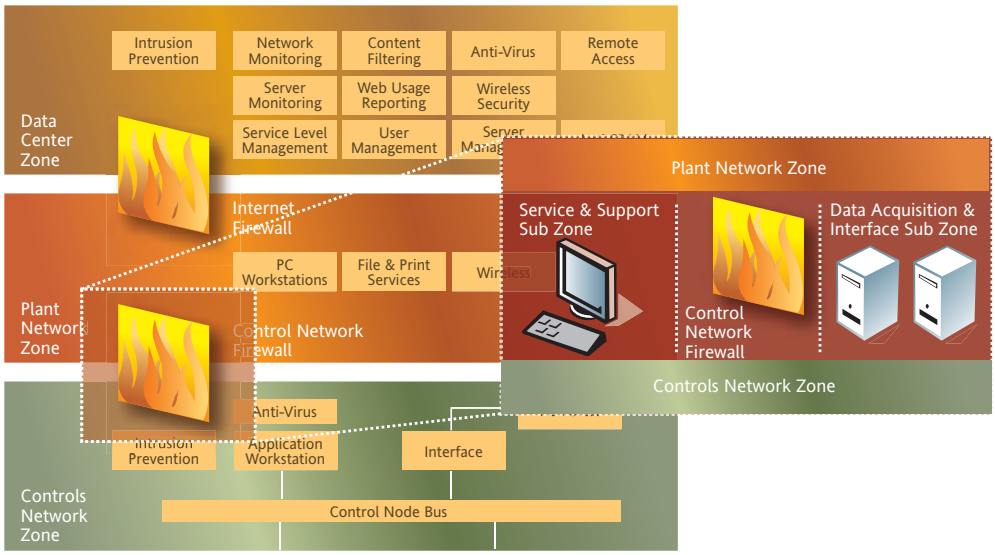
Data Center Zone — This may be a single zone or multiple zones that exist at the Corporate Data Center.

Demilitarized Zone — In a perimeter or external firewall, a special isolated zone referred to as a demilitarized zone (DMZ) is commonly created. The DMZ is a small network inserted as a "neutral zone" between a company's private network and the outside public network.

Internet Zone — This is the unprotected public Internet.

Additional sub-zones may be implemented to provide an extra level of control. This is commonly implemented as DMZs on the firewall as illustrated in Figure 2.

Figure 2 - Network Sub-zones



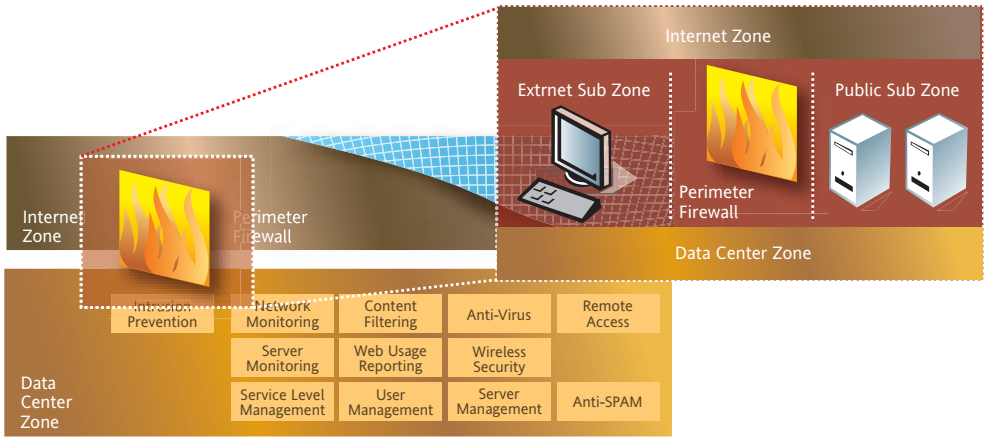
Typical uses of these sub-zones are:

Data Acquisition and Interface Sub-Zone — This sub-zone is the demarcation point and interface for all communications into or out of the Process Control Network. This sub-zone contains servers or workstations that gather data from the Controls Network devices and make it available to the Plant Network.

Service and Support Sub-Zone — This sub-zone is utilized by support agencies when servicing the Controls Network. This connection point should be treated no different than any other connections to the outside world utilizing strong authentication, encryption or secure VPN access. Modems utilized should incorporate encryption and dial back capability. Devices introduced to the network should be using updated anti-virus software.

It is also common for the perimeter firewall to have several DMZs defined as shown in Figure 3.

Figure 3 - Network Sub-zones with DMZ



Typical uses of these sub-zones are:

Demilitarized Zone (DMZ) — The DMZ sub-zone contains public facing web or ftp servers. The DMZ gives greater flexibility for the firewall ruleset to further control traffic that flows through it. It is common for external firewalls to have additional DMZs for other applications. An example is an Extranet DMZ, such as is commonly used to connect to the company's trading partners. The firewall will then provide the ability to restrict what your trading partners can access on the company network.

Extending these concepts to an internal firewall that is used to isolate the process control network is very straightforward. A typical example is an installation in which the firewall is located between the plant network (business network) and the process control network zones. A DMZ zone is created that contains the data collection and reporting servers. These servers will be accessible from the business network. Only these servers will be allowed to communicate with the process control network. It is also recommended that an additional DMZ be created for controlling remote administrstion and service connections to the process control network.

Public Sub-Zone — This is a sub-zone in which public-facing services exist. Web servers, SMTP messaging gateways and FTP sites are examples of services found in this sub-zone.

Extranet Sub-Zone — This is a sub-zone that is commonly used to connect to the company's trading partners. Partners connect by various methods including dialup, private lines, frame-relay and VPN. VPN connections are becoming more common due to the proliferation of the Internet and the economy of leveraging shared services. Firewall rules are used to further control the areas that partners are allowed to access as well as address translation.

Components

Business System Network

Perimeter Firewall — This is a firewall that controls the types of traffic to and from the public Internet.

Internal Firewall — This is a firewall that controls the types of internal site-to-site traffic and site-to-data center traffic. This is essential in controlling or containing the spread of network-born viruses, and provides an extra level in restricting the types of traffic that is allowed between sites. It also gives the ability to further protect the data center from internal intruders.

Process Control Network

Process Control Network Firewall — This is a hardware device that restricts the types of traffic allowed into and out of the Control Network Zone. It uses multiple network interfaces to allow the creation of additional zones or networks for services that are specific to Process Control Networks. Rules are created in the firewall configuration to allow only the permitted traffic. Additional information on recommended rules is detailed in the "Process Control Network Security — Firewall Recommendation And Configuration" document. The general rule of thumb is "deny everything and permit only the essential traffic." Firewall configuration should be managed in a consistent fashion to ensure that changes are documented. It is recommended that firewalls be monitored 7x24 whether by a group within the organization or a third-party provider, and an appropriate event-alerting and rectification process be enacted. It is also recommended that firewalls utilize a logging server to capture all firewall events either locally or in a central location. It is not recommended that the firewall be used for any services other than firewalls or VPN connectivity.

Intrusion Detection System/Intrusion Prevention System — Devices utilized to detect signatures or patterns on the network that would indicate unusual traffic patterns.

An Intrusion Detection System (IDS) monitors packets on a network wire and determines if the activity is potentially harmful, such as a worm attack. A typical example is a system that watches for a large number of TCP connection requests (SYN) to many different ports on a target machine, thus discovering if someone is attempting a TCP port scan. An IDS may run either on the target machine that watches its own traffic or on an independent machine such as an IDS appliance (also referred to as Host IDS).

An Intrusion Prevention System (IPS) encompasses the same monitoring techniques used in the IDS; however, it includes the ability to block the traffic that is deemed harmful. It prevents attacks from causing harm to your network or control system by sitting between your connection, the plant or business network, and the devices you are protecting. Like IDS, an IPS can run in host mode directly on the control system station.

Router — A device that forwards packets between networks. The forwarding decision is based on network layer information and routing tables, which are constructed either manually or automatically by routing protocols. Based on network requirements, routers may be utilized to connect the various network segments either directly or utilizing telecommunications links. Within the plant world, it is not recommended that routers are configured with access lists to mimic firewall functionality on a basic level. Routers lack a hardened operating system and do not have the robust capabilities of a true firewall.

Hub — A multi-port broadcast device. It takes whatever comes in any port and broadcasts it over all the other ports. As network nodes are added or traffic increases, every node on the segment has a greater chance of slowing communication or having a collision. Additionally, since Ethernet nodes currently do not differentiate between the relative importance of Ethernet packets, it is possible for non-essential traffic on the network to slow or collide with essential traffic (such as inter-PLC communication, or HMI polling.)

Bridge — A bridge acts as a "gatekeeper" between two collision domains. Physically wired into both LANs, this device is able to discern the source and destination address of an Ethernet packet. The bridge is also capable of "mapping" the locations of Ethernet nodes on either side of itself. By linking a control network and an office network with a bridge, you can stop traffic that is meant to travel between two computers in the office LAN from burdening devices on the other side of the bridge. When traffic occurs that is addressed for a device on the other side of the bridge from the originating address, the bridge will allow this traffic to pass. Compared to the completely shared network, the bridged network can reduce, but not eliminate, the opportunity for collisions and network slowdowns.

Switch — A switch is a multiport device that has the ability to "read" the address portion of an Ethernet packet and then send the packet out the port on which the destination node resides. Most modern switches have buffers that allow them to store and forward the Ethernet packets that are sent to it. Each port of the switch can connect either directly to a node or to a hub that can also have multiple nodes connected to it. Modern switches are capable of learning the unique addresses of devices attached to them or to a hub, which in turn is then attached to the switch without any programming. If a PC or PLC is plugged directly into a switch, the switch would only allow traffic addressed to that device to be sent down the connection cable to the device. By controlling the flow of information between ports, switches improve bandwidth utilization by reducing the number of collisions. It is important to note that process control networks communicate using the MAC address layer and that some consumer grade switches do not fully implement the standard and may not allow these devices to communicate. Generally speaking, commercial grade switches do not have this issue.

Media Converter/Media Access Unit (MAU) — A device utilized to connect various media types, such as fiber to ThinNet, to form a contiguous network.

Modem — A device utilized to connect devices asynchronously for out of band access to devices. In the plant world, the use of dial-back is recommended and should employ encryption techniques.

Wireless Access Point — A radio base station that is used to connect to the hardwired network. Wireless can be supported if implemented securely. Solutions provided must be capable of both preventing unauthorized access and ensuring that data transmitted is encrypted to prevent "eavesdropping." For maximum flexibility, devices selected must be capable of data encryption with dynamic or rotating keys, MAC address filtering and blocking, disabling SSID broadcasting, and complies with 802.11 & 802.1x standards. Consumer grade equipment is not recommended. Invensys recommends use of a VPN connection with software clients in lieu of WEP or proprietary data encryption. This allows supporting multi-vendor wireless hardware with a common solution.

VPN Concentrators — Devices that encrypt the data transferred between the concentrator and another concentrator or client based on a mutually agreed upon key. This technology is widely used today to allow remote users to securely access corporate data across the public Internet. The same technology can be used to add additional security accessing data across wireless and existing corporate WANs. In lieu of a separate VPN concentrator, it is possible to utilize VPN services that are integrated with the firewall.

Environmental Considerations

The surrounding environment must be considered when selecting the network wiring method. While unshielded twisted pair is accepted as the wiring method for an office environment, a plant environment introduces conditions that will result in problems. The plant environment may introduce magnetic field interference, radio frequency interference, temperature extremes, vibration, moisture, and dust in the air. The standard RJ-45 connector used on twisted pair wiring and equipment is not water or dust tight and will result in intermittent connections as it is exposed to adverse conditions. The gold plating on the contacts will degrade when exposed to vibration. An industrial version of this connector is not available and selecting a different connector will not allow the use of readily available network equipment. The cable itself is vulnerable to interference and the jacket material is thin enough that if it is run in conduit, it will introduce capacitance and degrade the performance of the network.

Coaxial cable interconnect methods like ThinNet and ThickNet are no longer considered acceptable wiring methods for office environments due to the proliferation of unshielded twisted pair. However, these are still valid wiring methods in the process control environment. The shielding of the cable provides for immunity to interference, plenum grade jacket materials are available and the connectors used provide for vibration, dust and moisture immunity.

The use of fiber-optic cable is increasing as the cost has decreased. It is immune to many of the environmental conditions found in the process control environment. The connectors used provide for vibration, dust and moisture immunity and most commercial-grade network equipment providers have standard options to support fiber-optic.

For additional physical environment information, refer to the IA Series Site Planning Guide, Document C0193AB — Section 1: Environmental Considerations.

Physical Security

Steps should be taken to ensure that adequate security measures are taken to restrict unauthorized access to all components utilized in the process control network. Network equipment should be installed in locked areas to prevent tampering. Cable runs should be installed in a method to minimize access. If equipment is installed in locked cabinets, ensure that adequate ventilation and air filtration are available.

Standards

Commonly found standards in process control networks are:

- Ethernet — IEEE 802.3 (10base5, 10base2, 10baseT, 100baseT, FDDI) (standards.ieee.org)
- TCP/IP — (Coexistence with IPX and other network protocols may cause issues with certain process controllers.)
- Device Integrator (Allows connectivity between foreign devices at the I/O level.)
- Fieldbus — A digital serial, multidrop, data bus for communication with low-level industrial control and instrumentation devices such as transducers, actuators and local controllers. The Physical Layer provides for transparent transmission of Data Link Layer entities across physical connections. It specifies the requirements for fieldbus component parts and also specifies the media and network configuration requirements necessary to ensure agreed levels of: a) data integrity before Data Link error checking; b) interoperability between devices at the Physical Layer. (www.fieldbus.org)
- PROFIBUS — One of the best-known industrial fieldbus protocols from Europe with an estimated 30% market share in Europe. PROFIBUS can be used in a very wide range of applications as a multi-application communications link for industrial devices, as well as cell-level communication. PROFIBUS utilizes a non-powered two-wire (RS485) network with up to 126 nodes and can transfer a maximum of 244 bytes of data per node per cycle. Communication (baud) rates are selectable but overall end-to-end network distance varies with speed. Maximum communication (baud) rate is 12Mbps with a maximum distance of 100M (328ft). The maximum distance is 1200M (3936 ft) at 93.75Kbps without repeaters. PROFIBUS connects to a wide variety of field devices including discrete and analog I/O, drives, robots, HMI/MMI products, pneumatic valves, barcode readers, weigh scales, transducers, and flow measuring equipment. PROFIBUS is an established standard, first introduced in 1989. The PROFIBUS protocol was originally developed by the committee founded by the German government. The resulting protocol was initially adopted as DIN standard 19245 and was recently adopted as a European Common Standard EC50170. (www.profibus.com)
- Modbus — An application layer messaging protocol, positioned at level 7 of the OSI model, which provides client/server communication between devices connected on different types of buses or networks. The industry's serial de facto standard since 1979, Modbus continues to enable millions of automation devices to communicate. Today, support for the simple and elegant structure of Modbus continues to grow. The Internet community can access Modbus at a reserved system port 502 on the TCP/IP stack. Modbus is a request/reply protocol and offers services specified by function codes. Modbus function codes are elements of Modbus request/reply PDUs. (www.modbus.org)
- Nodebus — The nodebus interconnects stations (control processors, application processors, workstation processors, application workstations, etc.) in the I/A Series® system, to form a process management and control node. Depending on application requirements, the node can serve as a single, stand-alone entity, or it can be configured to be part of a more extensive communications network. The nodebus uses a redundant IEEE 802.3 bus with CSMA/CD access protocol to provide high-speed, peer-to-peer communications between the stations. The nodebus can be implemented in a basic, non-extended configuration or it can be extended through the use of nodebus Extenders and Dual nodebus Interface Extenders (station attachment units). Its high speed, coupled with the redundancy and peer-to-peer characteristics, provides performance and security superior to that provided by communication media used in conventional computer-based systems.

- Vendor Specific (Proprietary)
- OPC — (OLE for Process Control) — OPC is a series of standards specifications that resulted from the collaboration of a number of leading worldwide automation suppliers working in cooperation with Microsoft. Originally based on Microsoft's OLE COM (component object model) and DCOM (distributed component object model) technologies, the specification defined a standard set of objects, interfaces and methods for use in process control and manufacturing automation applications to facilitate interoperability. The COM/DCOM technologies provided the framework for software products to be developed. There are now hundreds of OPC Data Access servers and clients. (www.opcfoundation.org)

Addressing

Process control networks utilize the following types of addressing for communications:

- MAC Addressing
- IP Addressing — Current addressing is static and management of addresses to prevent duplicates is critical.
- Addressing generated by the System Definition Configurator

Best practice guidelines for network design — plant and corporate systems:

General

- Allow only process control traffic on the process control network
- Use multi levels/zones of defense
- Install firewalls to isolate zones
- Utilize DMZs effectively
- Handle all external (support) connections in a DMZ
- Traffic logging
- Focus on prevention rather than detection
- Perform routing security audits
- Establish solid policies for design and operations

Data flow awareness

- Identify information is required from zones and levels
- User access levels

Firewalls in a plant world

- Utilize the firewall to provide firewall services only
- Do not use the firewall to provide other services (virus scanning, spam filtering, etc.)
- The firewall may be used to provide VPN access to the control network

Intrusion detection and prevention

- Create frequent backups of data and perform periodic restorations
- Host-based protection

- Real-time prevention decisions
- Protect from attacks at various phases
- Real-time correlation at the agent and enterprise level
- Implement proactive, not reactive security
- Design for flexibility to accommodate changes and unique requirements
- Provide for ease of deployment

Hardwired Network Connections

- Design considerations
- Bandwidth required
- Environment
- Electrical/RF/Magnetic/Interference potentials
- Cable locations
- Vibration
- Moisture and dust in the air
- Length of network segments
- Media conversion requirements
- Interfacing legacy systems
- Security
- Restrict access to network ports
- Use of fiber to minimize eavesdropping
- MAC address filtering on switches
- Restrict switches to allow only a single MAC address per port
- Proper identification of cables
- Route cables and fiber optics to minimize exposure to outside access, cutting cables, taps

Wireless (WiFi) Network Connections

- Design considerations
- Survey RF coverage area
- Identify any RF interference potentials
- Design goal is to limit coverage area to the facility
- Provide a db signal level for solid connectivity
- Use directional antennas as required
- Utilize only commercial grade equipment
- Select equipment that is compliant with 802.11 and 802.1x standards
- Security
- Install the wireless devices in a separate DMZ on the firewall

- Utilize MAC address filtering
- Utilize strong data encryption — Preferably VPN encryption on the wireless segment
- If WEP is utilized, use only dynamic or rotating keys
- Disable SSID broadcasting on the access points
- Disable/change SNMP community passwords on all access points
- Select an obscure SSID
- Monitor wireless segment for unknown nodes
- Monitor network performance and investigate any anomalies immediately
- Maintain separate, strong administration passwords on the access points
- Utilize event or syslogging and monitor
- Utilize a central authentication server
- Powerdown unit during off hours
- Use device-independent authentication so that lost or stolen devices cannot gain access to the WLAN.

Remote Access

- Utilize strong authentication
- Modem access should require dial back methods and encryption
- Utilize VPN for encryption

Physical security

- Implement strong physical security controls to prevent unauthorized access
- Label and maintain inventories of all devices

6. STANDARDS USED / AFFECTED

- ISO 17799

7. ASSUMPTIONS/ISSUES

- Ethernet network topology assumed
- Assumed that Internet access is provided to the sites from a centralized location

8. STEPS TO SUCCESS

- Assess the current level of security on your network
- Perform a security risk assessment
- Educate the organization on the need for security and best practices
- Design and document
- Policies

- Processes
- Solutions to security
- Pilot the protection technology and services
- Deploy protection technology and services
- Manage and support the security program to serve business goals
- Schedule regular tests and audits of the technology and process

9. ASSOCIATED DOCUMENTS

Invensys, *(2005), Process Control Network Security: Firewall Configuration and Policies*

Invensys, *(2004), Process Control Network Security: Intrusion Prevention in a Control Systems Environment*

FOR MORE INFORMATION

Please call one of our Customer Satisfaction Centers listed below, or your local Invensys representative:

invensys®

North America
1 866 746 6477 US, Canada
1 508 549 2424 Worldwide

Latin America
54 11 6345 2100

Europe and Africa
+44 7713 50 3476

Mideast
+44 7713 50 3476

Asia Pacific
65 68298899

http://www.invensys.com
http://www.ips.csc.invensys.com
ips.csc@invensys.com

W-15 0403054 7/05