Solution Profile

## Summary

Developing a comprehensive cyber security program to protect a facility's critical assets is built upon three elements:

- Foxboro I/A Secure Based Features: Establish secure foundation for the I/A system.
- Cyber Security Solutions: Extend cyber security beyond the I/A systems, into the DCS network.
- Cyber Security Maintenance: Post support ensuring compliance of the network.

## Business Value

The Invensys Security Platform is tailored to Foxboro I/A and DCS controls systems to meet cyber security requirements.

- Cyber Security Solutions are platform and system agnostic
- Cyber Security Solutions are based on a lifecycle methodology
  - Assessment
  - Development
  - Implementation
  - Management
- Cyber Security Solutions are built on "Best Practices" policies and procedures.

Real Collaboration.
Real-Time Results.™

# Invensys Global Security Compliance Platform

## Element 1: Foxboro I/A Secure Based Features

As the need to secure critical infrastructure becomes more important, no element is more critical than the Foxboro I/A infrastructure. Invensys Foxboro I/A Secure based features now include the ability to centrally manage anti-virus scans, DAT file updates, HIDS, and DLP from one central location on all Foxboro I/A Secure based Systems.

The Foxboro I/A series includes the following features for cyber security compliance:

- ePolicy Orchestrator (ePO)
- Virus Scan
- Host Intrusion Detection (HIDS)
- Data Loss Prevention (DLP)
- Active Directory (A/D)
- Hardened OS
- Whitelisting
- Station Assessment Tool (SAT)
- Backup Exec System Recovery (BESR)

### ePolicy Orchestrator (ePO)

ePolicy Orchestrator (ePO) is a unifying security management open platform by McAfee. ePO makes risk and compliance management simpler, enabling clients to connect security solutions to their enterprise infrastructure to increase visibility, gain efficiencies, and strengthen protection.

**Reference:** ISO27001, ISO17799, NERC CIP-007

### Virus Scans

Virus scans prevent, detect, and remove malware, including but not limited to system viruses, computer viruses, computer worms, Trojan horses, spyware, and adware. Early prevention and detection eliminates the threat and potential damage to equipment, safety, and resources.

**Reference:** ISO27001, ISO17799, NERC CIP-007

### Host Intrusion Detection System (HIDS)

Host Intrusion Detection System (HIDS) monitors and analyzes the internals of a computing system. A host-based IDS monitors all or parts of the dynamic behavior and the state of a computer system. Besides such activities like dynamically inspecting network packets targeted at this specific host (optional component with most software solutions commercially available), a HIDS might detect which program accesses what resources and discover that, for example, a word processor has suddenly and inexplicably started modifying the system password database. Similarly, a HIDS might look at the state of a system and its stored information, (whether in RAM, in the file system, log files, or elsewhere) and check that the contents of these appear as expected, e.g. have not been changed by intruders. One can think of a HIDS as an agent that monitors whether anything or anyone, internal or external, has circumvented the system's security policy.

**Reference:** ISO27001, ISO17799, NERC CIP-007

## Data Loss Prevention (DLP)

Data Loss Prevention (DLP) systems enable organizations to reduce the corporate risk of the unintentional disclosure of confidential information. These systems identify, monitor, and protect confidential data while in use (e.g. endpoint actions), in motion (e.g. network actions), and at rest (e.g. data storage) through deep content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination), and with a centralized management framework.

**Reference:** ISO17799, CIP-007

## Active Directory (A/D)

Active Directory (A/D) is a directory service created by Microsoft for Windows domain networks. Server computers that run Active Directory are called domain controllers. Active Directory provides a central location for network administration and security. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory verifies the password and specifies whether the user is a system administrator or normal user. Foxboro I/A Secure Systems utilizing A/D now have the ability to tie ePO policies into the Foxboro I/A A/D deployment for controlling Foxboro I/A computers as well as Foxboro I/A account management.

**Reference:** ISO27001, ISO17799, NERC CIP-007, NIST SP800 53.3

## Harden OS

Factory hardening is a procedure that updates patches and anti-virus software and disables unused ports and services. System hardening is necessary because default operating system installations focus more on ease of use rather than security. Most systems can have security measures enabled that will make them suitable for high security and high reliability environments. Foxboro I/A Systems include hardening, removing basic levels of unneeded services, and Windows software. Reducing available network switch ports (disabling), changing default passwords, removing un-used accounts, locking down services, removing unnecessary applications, and restricting access to the outside world wherever unnecessary are examples of hardening services.

**Reference:** ISO27001, ISO17799, NERC CIP-007, NIST SP800 53.3

## Whitelisting

Whitelisting is the opposite of Blacklisting. Whitelists contain only those programs you wish to grant access to as opposed to those you do not. This makes Whitelisting a lot less labor intensive since you only have to keep up with the applications you know about.

**Reference:** ISO27001; ISO17799, NERC CIP-007

## Foxboro I/A Series Station Assessment Tool (SAT)

Foxboro I/A Series Station Assessment Tool (SAT) is a Windows-based Foxboro I/A Series application automatically installed on all Foxboro I/A Series workstations and servers with Windows operating systems on the MESH network for Foxboro I/A Series software V8.5 and later releases. It supports full functionality on all stations including those installed with InFusion™ applications.

**Reference:** NERC CIP Evidence Documentation

## Backup Exec System Recovery (BESR)

Centrally manage backup and recovery tasks for multiple desktops across the network. Schedule backups to run automatically, including event-triggered backups, without disrupting network usage. Built-in software encryption of backups ensure security of critical data. This includes backups that are scheduled, maintained, and discarded appropriately to prevent de-duplication.

**Reference:** ISO27001, ISO17799, ISA99-2, NIST SP800 53.3, NERC CIP-009

Solution Profile

## Element 2: Global Cyber Security Solutions Program

### Cyber Security Lifecycle Methodology

The comprehensive lifecycle management approach ensures that the Invensys CISP team's cyber security solutions are network and control system agnostic. This approach divides the lifecycle of any network system into four distinct stages: Assessment, Development, Implementation, and Management.


#### Stage 1: Assessment & Planning

Review of the current network, identifies any problems or issues, and suggests areas for improvement.

**Assessment Services**

- Active Directory Workshops
- Technology Roadmap
- GAP Analysis
- Site Assessments
- Electronic Security Perimeter (ESP) Definition Workshops

#### Stage 2: Development of Architecture & Design

Using an assessment or plan as a guideline, elements are identified and actions required to implement and develop the detailed designs required to make it happen.

**Development Services**

- Network Design
- Procedure & Policy
- Remote Access
- Access Controls
- Network Management
- Anti-Malware
- Security Management
- Change Management

#### Stage 3: Implementation & Modernization

The network design is turned into reality through the procurement, staging, and commissioning of the client's new or system upgrades.

**Implementation Services**

- Jump Servers
- Network Management
- Backup Management
- McAfee ePO
- SEIM
- Firewall

#### Stage 4: Management & Optimization

The Invensys Security team will work closely with the management of the network, providing a mechanism to improve and optimize the continuously changing landscape of network usage.

**Management Services**

- Network Management
- Backup
- Patch Management
- Managed Security Services (24/7/365)

In addition to the above host of cyber security offerings, the Invensys security team also offers a comprehensive list of additional cyber security solutions to help address any internal needs, regulatory requirements, or program mandates. All of these elements are synergistic, providing not only a broad scope of security but the defense in depth necessary for true cyber security compliance.

## Active Directory (A/D) Workshop

The A/D is a technology that provides a central location for access to user information for a given network. Central user account information provides authentication, authorization, password management, and updates enforcing security policies for computers that are part of the A/D domains. The A/D workshop reviews all of these variables and provides a matrix of users and checklist for verification. A/D workshops provide customers with the information and solutions to manage more than just Foxboro I/A systems on the DCS network with A/D technology.

## Technology Roadmap

The Technology Assessment workshop helps clients develop a roadmap for the secure network support of current and future business and industrial control system requirements. A secondary network is essential in providing an infrastructure to host the security solutions detailed in this document. Users will be able to design a secondary network in support of cyber security management requirements for centralized management of:

- Backups
- Anti-virus management
- Patch management
- Event management
- Network performance monitoring and historical data reporting
- Security event historical data and reporting
- Active directory access controls
- Secure remote access relay server
- Support of future requirements

## Procedures / SOPs

Standard operating procedures serve many roles in a successful cyber security program, such as establishing the purpose for deployment, defining expectations, defining scope of systems to be included, and identifying the control and procedures necessary to achieve the desired outcome.

## Secure Zone

The Invensys "Secure Zone" is our method of implementing firewall technologies to support functionally different zones. Leveraging these zones allows the secure hosting of services like logging, remote access, historians, etc. This solution provides electronic access point protections to cyber assets and Foxboro I/A components. The solution also enables Network Address Translation (NAT) capabilities and can be leveraged to prevent IP traffic directly to the MESH network. The Secure Zone logically sits between the Business Network and the Industrial Network providing these important services.

Solution Profile

## Change Management

Change management centralizes functions related to electronic documentation and system management for DCS networks. System management includes configuration management, alarm and operator action management, and system management.

## Event Logging

The ability to log events on the network is a critical tool for tracking and analyzing cyber security events for troubleshooting, remediation, and analysis. Foxboro I/A Cyber Assets (Workstations and Switches) will forward security events to a central monitoring server. The central monitoring server will collect data from the various systems, provide notification on selected events, and act as a repository to allow the data to be analyzed at a later date. In addition, system logging will accommodate SYSLOG, SNMP TRAPS, and Windows Events.

## Patch Management

Patch management is still the single most important action that can be taken to reduce missing security patches and network security breaches. The Invensys Security team eliminates this risk by providing on-demand or fully automated detection and installation of missing patches. Patch management enables administrators to manage Industrial Control Systems and Microsoft patches and service packs for all languages supported by Microsoft. Patch Management also provides features like patch rollback and uses an existing WSUS patch repository.

## Network Management

Network management tools offer monitoring and management options that can extend the reach of a single operator and improve the effectiveness of monitoring and troubleshooting performance problems on the Industrial LAN or Foxboro I/A MESH Network. This Invensys solution reduces the lack of visibility to most network segments or devices. Only through greater visibility and shared knowledge can DCS administrators prevent outage issues. The Network Performance Monitoring and Alarming component provides a network availability and performance monitoring solution that delivers the critical information clients need to stay on top of their evolving networks by enabling them to quickly detect, diagnose, and resolve network performance problems and outages. It provides the ability to monitor and analyze real-time in-depth network performance statistics for routers, switches, wireless access points, servers, and any other SNMP-enabled devices.

## Remote Access Relay Server

The Remote Access Relay Server will provide Read-Only views associated with remote Foxboro I/A, remote HMI access, and Compliance/History Cyber Assets located in the Electronic Security Perimeter (ESP) Zone. To protect Cyber Assets located in the ESP Zone from Business Network access, the Invensys Security team will deploy an intermediate access platform as a relay server (Remote Access Relay Server). Deploying this solution prevents direct access to the Data Acquisition, Compliance/History, and DCS secure zones. Remote access may be required to do the following:

- Perform administration functions
- Run diagnostics
- Perform configurations
- Allow for non-operator observation and non-routine access

## Managed Secure Services

Process control networks are specialized environments that require mission-built solutions and generic solutions for securing IT systems. While some standard security tools and techniques can be used to protect process control systems, careful deployment or tailoring is necessary. In response to these threats, the Invensys Security team has taken its industry experience and market-leading Managed Security Services to create an Industrial Security Monitoring Solution that is built from the ground up to meet the needs of Process Control Systems.

The following items are examples of why Managed Security Services are required:

1. Lack of trained resources: Co-managed security monitoring solutions augment existing staff and provide 24/7/365 security professionals for monitoring, reporting, and critical event alerting.
2. Real-time review of security issues: Health monitoring and reporting of all firewalls within the DCS network help ensure systems are protected.
3. No resources to review intrusions in real-time. Intrusion detection capability detects intrusions and intrusion attempts at the electronic security perimeter.

## Element 3: Cyber Security Best Practices

Standards organizations like those in the list below help companies develop effective Cyber Security strategies. While these organizations have different approaches, they all have a common element—to establish a "best practice" approach to cyber security.

- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- Nuclear Energy Institute (NEI)
- International Society of Automation (ISA)
- National Institute of Standards and Technology (NIST)
- Institute for Information Infrastructure Protection (I3P)
- International Atomic Energy Agency (IAEA)
- Internet Engineering Task Force (IETF)
- International Organization for Standards (ISO)
- ISA Automation Standards Compliance Institute (ISA Secure)

Invensys' Critical Infrastructure and Security Practice (CISP) adheres to the best practice approach through its lifecycle methodology, which ensures that the solutions are network and control system agnostic. Our solutions are dependable and repeatable processes; easily map to any standard regulation; implementable at any process road map stage; and are vendor agnostic and industry independent.

## Cyber Security Best Practices Approach

Cyber security best practices are intended to provide guidelines on network security that will not only reduce external threat vectors, but also internal. Items are presented in order of priority.

- Always apply and maintain the latest Invensys-authorized Operating System (OS) and application patches.
  - Download updates directly from the patch source or via secure file server.
  - Assess which patches are required for each individual asset and apply as necessary, ensuring deployment does not impact operations.
  - Ensure all required patches have been successfully applied.
  - WITHOUT applying the current Invensys-authorized patches, individuals will be increasing the attackable surfaces of individual DCS workstations and servers.

- Always use current anti-virus definitions.
  - Ensure that the latest anti-virus definition files have been downloaded and run from the Invensys Support Website.
  - Verify through the McAfee client that the update was successfully installed.
  - Test new DAT in a test bed environment, prior to release into production environment.
  - WITHOUT keeping anti-virus current, the servers and workstations will not have the current malware signatures, leaving the equipment vulnerable to current attacks.

- Update authorized application software.
  - Ensure application software such as Adobe, if authorized, is updated. File types such as *.pdf* are one of the top distributors of malware if not routinely updated.
  - WITHOUT updating third party software on the inventoried system, additional vulnerabilities will remain in place.

- Enable Network Anti-Virus / Intrusion Prevention System.
  - Ensure that the most current anti-virus definition files and Intrusion Prevention System policies are enabled on all capable network appliances protecting the second Ethernet networks.
  - WITHOUT using a device that incorporates intrusion detection system (IDS), you will not have a baseline of normal network activities versus an attack. Antivirus module will provide an alert and a secondary screen for network malware.

- Harden Servers and Workstations. Hardening Non-DCS assets is a requirement and typically will not have negative effects on the DCS. Hardening DCS assets may be performed and will vary from Non-DCS asset hardening.
  - Ensure all software and hardware patches and updates are current.
  - Run A/V scans.
  - Disable all unused ports and services.
  - Harden Bios.
  - Use static IP addresses, disable DHCP on the interfaces, and disable unused interfaces.
  - Disable NetBIOS, unless specifically mandated by the IT department; disable NetBIOS over TCIP/IP (via WINS tab).
  - WITHOUT hardening servers, there is greater risk for attacks. Hardening reduces the attackable profile of the system.

- Do not use a USB stick unless it has been scanned and confirmed that it is free of problems with the latest *dat* file.
    - Designate and use specific USB equipment where required.
    - If using USB equipment to bridge air-gaps, always use a specific designated station in conformance with DCS security policies.
    - WITHOUT restriction on USB devices, their portable nature can be used to compromise your security perimeter.

- Change default "admin" passwords.
    - Use strong passwords consisting of more than 6-8 characters using special characters when applicable.
    - WITHOUT policies to ensure that "admin" passwords are changed, individuals can use "admin" passwords to escalate their privilege levels. Automated attacks by malware using "admin" passwords are prevalent.

- Control User Rights.
    - Verify that **only** authorized accounts are members of the local system administrators group.
    - Do not use accounts across domains.
    - When applications cannot use special characters, a service account should be created with authentication compatible with the application.
    - Wherever Group Policies are in use:
        - Change local system administrator passwords.
        - Implement password aging, history, and complexity requirements.
        - Ensure that Restricted Groups policy is enabled and used.
    - WITHOUT policies that specify user privilege criteria, individuals can receive privileges beyond those required for the task at hand. If too many users have elevated privileges beyond their needs, malware can use this as threat vector.

- Always implement Backup and Restoration.
    - Use a network backup repository.
    - Back up the network repository to a geographically disperse secondary storage site for disaster recovery or to removable media that can be stored off site.
    - If removable media is elected, then a rotation policy should be implemented to ensure that multiple copies of the backup exist off site.
    - Periodically conduct recovery exercises using test bed equipment.
    - Determine relative storage capacity available and automated a backup schedule for individual workstations and servers.
    - WITHOUT implementing a back up policy, customers will have no recourse to restore to a condition prior to an attack date if required.

- Take inventory of network assets.
    - Keep inventory current of all network assets and status.
    - Update inventory as network changes are made to both hardware and software.
    - Run network scans to collect asset information (log files, etc.) where authorized. Non-DCS assets typically may be scanned without issues but DCS asset scanning should incorporate a limited tuned methodology for scanning DCS assets.
    - Run regular network audits to ensure all systems are up to date.
    - WITHOUT a network inventory, you do not have a baseline of what normal network assets are and that goes towards the network scan, complicating what are known devices and what are known patches. Knowledge of what specific network firmware is running and what network security equipment is present can be critical in determining whether or not vulnerabilities exist.

- Use physical network isolation when possible.
  - WITHOUT using physical network isolation, cross contamination of the DCS platform is possible from the corporate system.

- Use logical network segmentation (secure zones) when possible with strict Firewall Rules.
  - Isolate and control flow of information between Business Network(s) from PCN through use of firewalls.
  - Require strict firewall rules with specific (/32) source, destination, port, and protocol.
  - Use DMZs
  - WITHOUT using a secure zone, there will be no buffer before the network traffic traverses into the DCS network.

- Enable Firewall Logging.
  - Ensure that all firewall policies protecting the Process Control Networks (PCN) and supporting infrastructure have logging enabled.
  - Monitor firewall logs as appropriate, paying special attention to locate potentially malicious or abnormal traffic.
  - WITHOUT firewall logging, you will not have visibility into dropped traffic or attacked traffic.

- Use Network Management Systems (NMS).
  - Implement NMS to provide system audit and logging.
  - Monitor system logs for failed login attempts.
  - Generate and review reports for abnormal events.
  - WITHOUT using NMS, there will not be a consolidated location for viewing all logs. The NMS system reports provides consolidated insight to all systems, which is invaluable for day-to-day operations and in the event of a cyber attack.

- Don't click links or files that aren't verified.
  - DCS assets should not have internet access; some Non-DCS assets may have outside DCS access to business network website interfaces. Even business networks could be compromised, so verify all access leaving the DCS network to un-trusted networks.
  - Ideally, the DCS network should be isolated from internet connected networks.
  - WITHOUT policies restricting web access, users can potentially comprise the security perimeter by clicking on malicious links and installing unauthorized software.

- In the event of a Cyber Incident:
  - Create an Incident Response Plan before an Incident so that you are prepared in the event of an Incident. Steps that are typically part of incident response plans are:
    - *Do not* start updating anti-virus.
    - *Do not* start running anti-virus patches.
    - *Do* get a triage team together.
    - *Do* get copies of all the logs.
    - *Do* make a VM image of the affected system.
  - WITHOUT an incident response team and procedures, the opportunities to collect the forensic evidence required to determine the attack vector and point of origin can be lost or compromised, depriving the client the opportunity to work with the antivirus vendor and other agencies.

- Download and run latest McAfee Stinger tool.
  - WITHOUT collecting the necessary forensic evidence to work with the antivirus vendor, the client may not detect the variant that was not completely remediated by the Stinger tool.

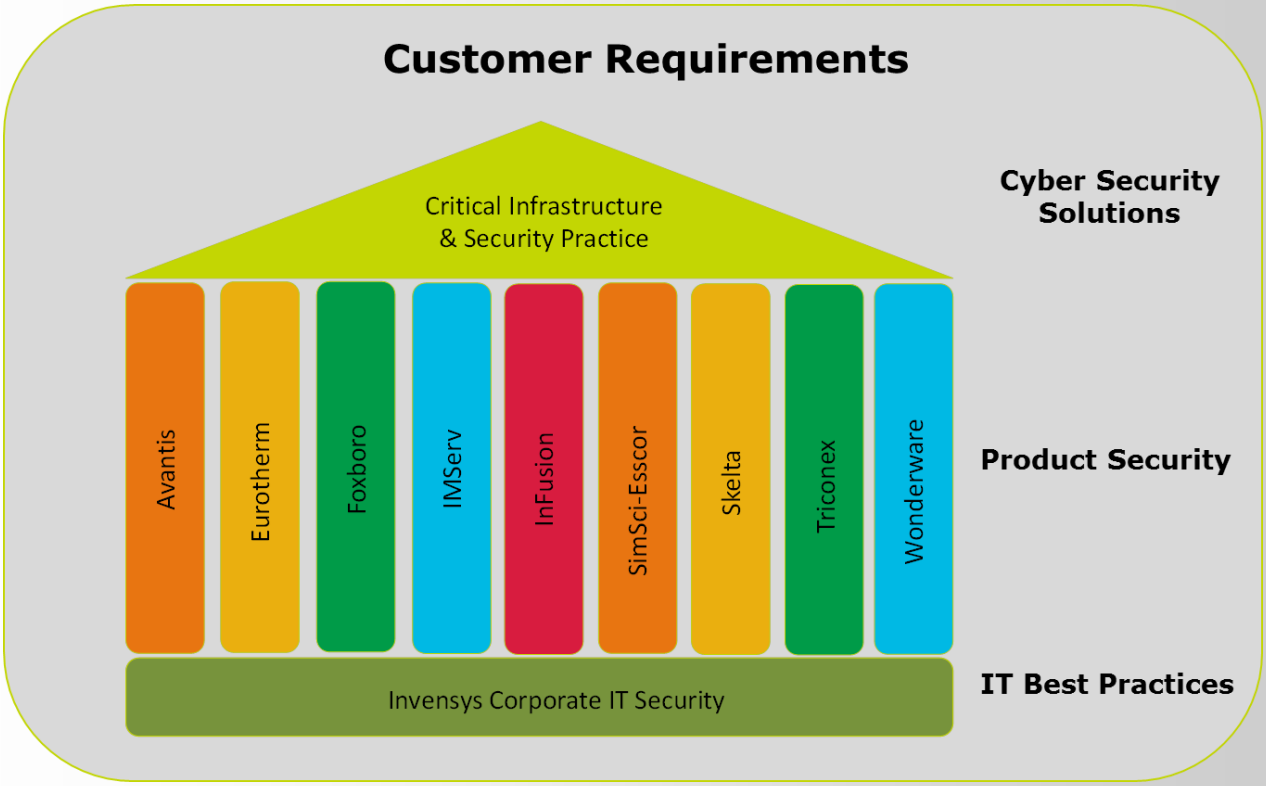
## Cyber Security DNA

At Invensys, security is a primary focus in all development efforts to ensure that we meet our customer's requirements. The Invensys Critical Infrastructure & Security Practice (CISP) security team builds on the firm corporate IT security practice and the cross portfolio product security development, delivering complete integrated security solutions and security programs for our client's entire plant and infrastructure. With this alignment, it ensures that our Cyber Security solutions reflect the best Invensys has to offer.

The core team is made up of process engineers, network engineers, and IT specialists that have backgrounds in network remediation, data communications, network security, and wireless RF. The team represents a cross section of industries such as oil, gas, mining, nuclear, telecom, and power generation that provides us with the ability to work alongside our clients and communicate effectively with cross functional teams. The team has years of specialized Cyber Security experience and extensive industry knowledge. When combined, CISP can deliver Cyber Security solutions for any regulatory or industry requirement facing customers today.

CISP members have the following certifications:

- CISSP
- CCNP
- CCS1
- CCSA
- CWNA
- CCIE
- NNCDA
- CCNA
- CCDA
- CEH
- ECS
- ESS
- MCSE
- CISM
- CISA
- CCSE
- OSCP
- JNCIS



invensys™

Solution Profile

## Invensys Global Cyber Security Solution Matrix

| Component | Functionality | Benefits |
|---|---|---|
| **Network Assessment Tools** | Network and Software Tracking & Change Management | Detailed analysis of what is happening on the network; visibility of applications installed, state of hardware and security on your network. Provides history of network changes and change notifications |
| | Cyber Assets Inventory | Creates an inventory of IP devices on ESP network |
| **Patch Management** | Identify & install missing Operating System and Third Party software updates | Scanning profiles to identify missing patches for specialized mission specific cyber assets such as DCS HMIs. Patch remediation tracking |
| **Network Performance Monitoring & Alarming** | Monitor Protected Cyber Assets | Quickly detect, diagnose and resolve network performance problems; real-time dashboards enable at-a-glance network performance tracking |
| **Centralized AV Management with ePO** | Apply AV protection to Protected Cyber Assets | Centralized AV management, controls and updates to ESP Cyber Assets |
| **Centralized Host Access Controls for HIDs, DLP and Whitelisting** | Apply access controls to Protected Cyber Assets | Centralized Host Access Controls and management for ESP Cyber Assets |
| **Event Logging and Reporting** | Security Information and Event Management | Provides centralized event monitoring services collecting data from various systems, archiving events and providing notification capabilities with a central repository of data logs |
| **Centralized Backup Storage** | Protected Cyber Asset backup management and controls. Repository for ESP Cyber Asset backups and storage. | Enables quick backup, restore and testing for ESP Cyber Assets |
| **Remote Relay Access Server** | An intermediate device such that the Cyber Asset initiating interactive remote access does not have direct access to Cyber Asset(s) within the ESP. | Remote Access to establish relay bastion host for relaying remote connections to ESP Cyber Assets. Ability to deliver Read Only—Administrative function; diagnostics and configuration; non-operator observation |
| **Protected Cyber Assets Identification Workshop** | Identify and classify Protected Cyber Assets and identify potential Electronic and Physical Security Perimeters for easier management and maintenance | Identify Protected Cyber assets with an identified repeatable methodology. Identifies exactly what is protected and why |
| **Technology Roadmap Workshop** | Identify network strategy for connecting DCS networks to business networks | Establish security methodology for connecting dissimilar networks. Establish technology plan and requirements for DCS network |
| **Managed Secure Services** | Designed specifically for process control networks; 24/ 7/365 monitoring of security devices with timely identification and remediation of security vulnerabilities | Eliminates need for expensive full-time security expertise; maximizes reliability and uptime; continues data analysis to identify existing and predict future security challenges; enforces policy management and change control |
| **AD Workshop** | Identify staffing, security and access control requirements for protected cyber assets | Implementing of active directory structure capable of meeting requirements for protected cyber assets |
| **Supporting Services** | Gap analysis; assessments; incident response; documentation policy and procedure creation, updates and assessments; network management | Customizable services that complement any Cyber Security program; services can be leveraged individually to identify and fill any gaps in client's program or against their internal security posture |
| **Engineer Operating Instructions** | Detailed instructions for performing task associated with maintaining compliance for Protected Cyber Assets | Task instructions developed for DCS staff to perform task required for implementing, changing and updating Protected Cyber Assets |

## Invensys Global Locations

To learn more about how the Invensys Cyber Security Team can work with you and your team to address your cyber security needs, contact one of the Invensys global offices to meet with one of our cyber experts.

The Invensys Cyber Security Team has:

- Specialized experience
- Extensive industry knowledge
- Hands-on implementation background


**North America**
Invensys Operations Management
10900 Equity Drive
Houston, TX 77041
TEL +1-713-329-1600

**Latin America**
Invensys Systems Argentina
Nuñez 4334
(1430) Buenos Aires
Argentina
Tel: +54-11-6345-2100

**Europe and Africa**
Invensys Systems France S.A.
10, Avenue du Centaure
B.P. 8255 Cergy
95801 Cergy Pontoise Cedex
FRANCE
Tel: +33 1 34 43 25 25

**Middle East**
Jebel Ali Free Zone
P.O. Box 61495
Dubai
United Arab Emirates
Tel: +9714 8074700

**Asia Pacific**
IPS (S) Pte Ltd.
15 Changi Business Park Central 1
Singapore 486057
Tel: +65 6829 8888


**To learn more about Invensys' Critical Infrastructure and Security Practice (CISP) solutions, contact your sales representative or visit: http://iom.invensys.com/CyberSecurity**


invensys

Invensys • 5601 Granite Parkway III, #1000, Plano, TX 75024 • Tel: (469) 365-6400 • Fax: (469) 365-6401 • iom.invensys.com





Rel. 12/11 PN XX-XXXX