WHITE PAPER

invensys

# PROCESS CONTROL NETWORK SECURITY: INTRUSION PREVENTION IN A CONTROL SYSTEMS ENVIRONMENT

LifeTime PERFORMANCE

**WHAT'S INSIDE:**

## 1. GENERAL INFORMATION

The goal of this document is to provide an understanding of intrusion detection and prevention systems, why they are necessary, how and where they fit in the control system environment, and provide example scenarios.

Both IT network and process control networks have a basic requirement for intrusion detection/prevention systems to prevent unwanted or malicious traffic. However, the impact of an intrusion in each environment is very different.

In the IT environment, an intrusion would typically result in the loss of data or interruption of the ability to transact business, which could have significant negative financial impact. Process control networks carry real-time data that operates mission-critical processes. Intrusion on the process control network may have effects ranging from loss of production to safety issues resulting in injury. Depending on the severity of the event, environmental damage or loss of life may occur, resulting in legal action. In some cases, it could jeopardize the license to operate.

To protect critical networks against the complete spectrum of threats and vulnerabilities, next-generation intrusion prevention systems (IPS) must be "purpose built" from the ground up using a combination of innovative technologies to eliminate false positives, actively thwart attacks, and ultimately protect critical resources.

## 2. EXECUTIVE SUMMARY

Invensys' approach to site network(s) 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 meet 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 I/A Series® systems, is the comprehensive System Hardening Service, which implements Site Security Review Service recommendations specific to the security of the control system network. The System Security Hardening Service assists in tightening — i.e., hardening — the security of the I/A Series 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 focuses on one key security device — intrusion prevention systems — that should be part of overall business and control network architectures.

Traditionally, intrusion detection systems (IDS) have been a critical piece of security infrastructure implemented whenever critical business processes such as control systems are connected to TCP/IP-based local and wide area networks. Intrusion detection systems are able to detect network activity such as hacking attempts, virus and worm attacks, and other potentially threatening traffic capable of wreaking havoc on the control system. The technology behind them is simple – detect the threat and alert management to the activity.

Today, new-generation intrusion prevention systems (IPS) are not only able to detect threats, but mitigate them by blocking the traffic from entering your network. We will discuss both IDS and IPS in this white paper, with a greater focus on IPS, because it is logical to implement the tightest layer of security on our systems as technically possible in order to maintain the continuity of our business.

## 4. QUESTIONS FOR CONSIDERATION

*Why should an intrusion prevention system be used to detect threats? Doesn't a firewall protect my business and control system networks?*

Most networks today are protected by firewalls. A lot of faith is put into them in the belief that they block what is not allowed while permitting what they should. Firewalls have the capability to log lots of information, but they do not possess the ability to analyze data and alert designated authorities to detected events.

For example, a firewall can be configured to allow telnet for remote access to a control system. It will log all the connections related to telnet, but it cannot determine what someone is doing within that connection. A hacker can use telnet to gain access to the system and the firewall wouldn't think twice about allowing it. An intrusion prevention system will not only detect that someone is attempting to hack in by trying multiple passwords, it can also block the hacker by shutting down the telnet connection.

*Why is blocking important?*

Intrusion prevention systems will not only detect but can block traffic in real-time that is harmful to your business and control system networks. There are many types of attacks that can bring down a system with a single packet. Simply detecting this packet and alerting designated personnel about it are not enough. In fact, recent attacks of this nature include the SQL Slammer and MyDoom attacks affecting Microsoft Windows products.

*Isn't blocking dangerous? What if critical network traffic is blocked?*

With blocking technology, many people have concerns that legitimate traffic might be affected. This is entirely controlled by the end user of the IPS device and the diligence with which it is installed and configured. Firewalls themselves are quite capable of blocking legitimate traffic if not properly configured. An intrusion prevention system should be configured to block only those attacks that are well defined and not anomaly-based.

*What is Invensys doing to increase security on control systems using intrusion prevention systems?*

Invensys, in conjunction with our vendors, has developed customization into intrusion prevention systems to detect threats that have critical impact into control systems. The intrusion prevention system can stop these attacks from causing loss of production, or worse — injury or loss of life.

## 5. INTRUSION DETECTION SYSTEM TECHNOLOGY

Intrusion detection technology has been available for many years in various forms. It has progressed from system-based tools that monitor file changes to a network-based tool that can identify numerous activities.

The most common approach intrusion detection method used by IDS is to detect threats is through "signature" detection. Signatures are a collection of known symptoms of a known attack. One example of a signature attack would be a hacker attempting multiple passwords to access a system. The IDS can detect that someone is connected to a system and is receiving numerous "bad password" or "login failure" messages, often signaling a hack attempt. IDS vendors create these signatures and deploy them to their end users. Alternatively, signatures can be created by the end user to identify specific known attacks on their custom applications. Part of a good IDS deployment consists of regularly scheduled updates of the signatures.

Early intrusion detection systems were often plagued with "false positives" and "false negatives." A false positive is an alert generated by network activity that appears suspicious but is not necessarily harmful. An overabundance of false positives often left people dissatisfied with the IDS. Conversely, false negatives were not detected by the IDS system, and these were also an issue. Today, intrusion detection systems have very little false positives. Intrusion detection systems can be easily set up for your specific environment. For example, users with operating systems that are Windows-based can disable the IDS from reporting attacks that only affect UNIX systems.

From the beginning, intrusion detection systems have offered more detailed reporting of events than was typically reported by devices such as firewalls. Instead of just giving the source, destination, and protocol used in an attack, IDS can present more forensics, for example, a packet capture of the attack. Newer systems offer the ability to correlate similar events and identify them as a single attack, rather than reporting a single attack from a hacker. This allows for alarm consolidation, which results in fewer pages or notifications being sent out.

## 6. INTRUSION PREVENTION SYSTEM TECHNOLOGY

In the process control environment, alerting alone is not acceptable. Alerting requires human intervention — and time — to analyze each reported issue. By the time appropriate action can be taken, it may be too late to prevent serious damage from occurring.

Intrusion prevention systems incorporate all IDS functionality, and then take intrusion detection a step further with its ability to block an attack as it is happening, thereby preventing harm to your network or control system, rather than simply generating an alert when the attack occurs. Intrusion protection systems monitor the network much like an IDS but when an event occurs, the IPS will take action based on prescribed rules. In a well-designed IPS implementation, a malicious attack cannot occur because it is blocked before the danger reaches the intended target system, whereas an IDS simply generates an alert when an attack occurs.

Intrusion prevention systems are installed in-line on your network, thus all network traffic must traverse it. There is a concern that if the IPS device itself were to fail, network connectivity could be lost. IPS vendors have solved this by implementing an option to "fail open" or "fail closed." This is a user setting in which you can decide whether or not you want traffic to pass should the IPS equipment have a fault. Failing "open" will allow all traffic to flow through, which is not recommended as it will leave the network with no protection. The recommendation is to "fail closed," which will block or lock down the protected network.

One of the checkpoints of a network security assessment is to determine if disconnecting your control system from the plant or business network will interfere with safe operations of the control system. In cases in which the control system is responding to setpoints or other critical information from the business network, Invensys recommends using a high-availability solution to ensure that secure connectivity continues.

## 7. HOST-BASED INTRUSION PREVENTION SYSTEMS

The discussion above has been focused on intrusion prevention devices that monitor your network for attacks and are independent from the control system. This type of implementation is commonly referred to as "network-based IPS." There is another implementation of IPS, called Host IPS, which can be installed on each computer system on the network. Host IPS offers a "last resort" protection system for your control system. If a hacker is able to compromise the firewall and your network-based IPS has failed or has been compromised, a host-based IPS can still protect you. It works by making a baseline of the operating system and applications on your system and blocking any traffic coming from your network that could potentially interrupt the recorded "norm."

Invensys is working to provide a process control-specific host IPS for its I/A Series applications.
A unique blueprint outlining the control system's application functionality would determine what system actions could and could not be performed.

## 8. TECHNICAL OPTIONS

### Host-Based IPS Options

As mentioned above, a host-based intrusion prevention system can provide an added level of protection on the operating side of the network. The IPS is normally installed as an application that starts with your operating system. With IPS on the host, you have the same options as network IPS — signature or anomaly-based detection. In order to ensure system stability, it is best to choose an anomaly-based system on the host, since you do not want to burden it with listening to and identifying all network traffic. Since the host system knows what is permissible and what is not, it is easier to shut down anomalies.

### Network-based IPS Placement Options

Several physical options for installing a network-based intrusion prevention system are described below.

**Tap Mode**

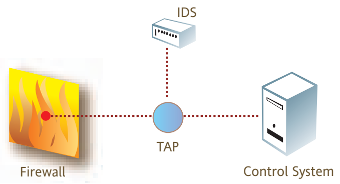
Tap mode allows you to monitor existing network traffic across a physical link without interrupting it. This mode allows intrusion detection, not intrusion prevention. A device called a tap will be placed in between the network and the systems you wish to protect. This tap allows a new connection to be made to the IPS for monitoring.

**Mirror Mode**

Port mirroring is the most common installation for IDS. Like tap mode, this does not allow for prevention, only detection. It requires that the switching device interconnecting your network to your system allows for mirroring or spanning, or uses a hub as opposed to a switch.

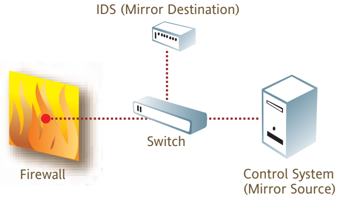
**Inline Mode**

Inline mode is required for IPS functionality. It places the IPS system in between the network and the system you are protecting. This is similar in design to tap mode, however in this implementation, all traffic must physically pass through the IPS. This allows the IPS to shutdown any offending network connections.

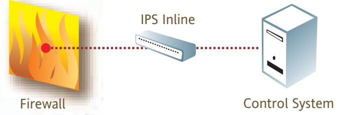


### Implementation Considerations

Installing an IPS requires “tuning.” This process consists of removing protocols not used on the network, removing signatures for operating systems and applications not in use, and adjusting for your particular bandwidth requirements.



Protocols and applications that are non-standard or might not be included in the off-the-shelf intrusion prevention system should also be taken into consideration. This will require careful planning as you must determine what are allowed network functions of the protocol and what should be alerted and/or blocked.



Whether selecting an IPS or IDS, alerting and reporting are very important features to consider when choosing a platform. Factors should include:

- Do the alerts contain enough information to suit your policy requirements?
- Can the alerts be delivered via an email or paging system?
- Can the alerts be generated on a path other than the network connection supporting the intrusion prevention system (backdoor access)?
- Can the IPS perform an action such as modify a firewall policy or send SNMP traps?

Like firewalls, intrusion prevention systems are also chosen by their network bandwidth capability. The following aspects should be taken into consideration when choosing an IPS:

- Number of physical connections
- Speed of the physical connections (throughput)
- Speed of the combined physical connections (aggregate throughput)
- Special IP network constraints such as VLAN use

## 9. REQUIREMENT SUMMARY

The network architecture implemented for process control network security needs to meet 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 prevent/detection
- Clearly defined change management policy and committed IT resources for on-going administration.

### Standards Used / Affected

- ISO 17799
- An IPS should always be implemented to adhere to corporate policy. The policy should be enforceable, as much as possible, by the intrusion prevention system.

### Assumptions / Issues

Connections to process systems with non-IP protocols might pose a problem as most IPS/IDS systems are TCP/IP based. These will not process data at physical layer two. Encrypted protocols cannot be monitored by intrusion prevention systems.

### Steps To Successful Implementation

These steps help facilitate a properly implemented intrusion prevention system:

- Vulnerability assessments
  - The IPS must be periodically tested for any known vulnerabilities to ensure that its operation is uninterrupted. A close relationship with the vendor should include a process for identifying known vulnerabilities and remedying them quickly.
- Periodic audits of security policy
  - Security, being an on-going process, dictates that you should maintain a policy that fits current and future needs. Your security policy should be updated to contain new protocols, applications, and user access levels on your system.
- Change control
  - Maintain a rigid set of change controls on the IPS. You should have a well-documented configuration as well as a log of any changes made to that configuration.

- Testing signatures
  - — Any generic IPS signatures should be tested before prevention/blocking is enabled.
  - — Testing of custom signatures should also be done to ensure your alerts are generated when required.
- Updating signatures
  - — As your IPS vendor updates signatures for new attacks, you should collect and test them.
  - — Once you have determined that the new signature applies to your system, you should install them on the IPS.
- Analyzing alerts / responses
  - — Skilled personnel who can identify hacking attempts collected by the IPS should be familiar with incident response skills. This includes analyzing alerts sent by the IPS, collecting the forensics, and delivering them to proper authorities.
- System monitoring
  - — The IPS should allow for a remote system to monitor the health of the device, and be capable of notifying you via pager or email that it is not collecting data.
- Well-defined corporate security policy
  - — Your network security plan should not rely on any one method alone for network and process control security. The security infrastructure should include anti-virus protection, firewalls, multi-level password authorization, network-based and host-based intrusion prevention systems.

## 10. FUTURE TECHNOLOGY

Vendors are beginning to merge their firewall technologies with IPS. This allows for a hardened device to sit between networks to provide more advanced blocking and monitoring technology. Invensys does not recommend that these be implemented in today’s process control systems due to issues such as being a single point of failure or not including enough unique signatures.

## 11. GLOSSARY

Table 1 – Glossary

| Term | Definition |
|---|---|
| IPS/IDP | A network Intrusion Prevention System (IPS) is a device that sits inline on the work, uses stateful inspection to analyze packet content, and blocks certain packets that match a signature and alerting on others |
| IDS | An intrusion detection system monitors packets on the network wire and attempts to discover if a hacker/cracker is attempting to break into a system (or cause a denial of service attack). A typical example is a system that watches for 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. A network IDS (NIDS) may run either on the target machine who watches its own traffic (usually integrated with the stack and services themselves), or on an independent machine promiscuously watching all network traffic (hub, router, probe). Note that a "network" IDS monitors many machines, whereas a host IDS monitors only a single machine (the one they are installed on). |
| Fail-closed | Desired failure mode of a firewall or IDS device. If it should fail, It will fail in a "closed" state, meaning that all connections are blocked. |
| False-positive | A false positive in an Intrusion Detection System (IDS) is an attack alarm that is raised incorrectly. |
| False-negative | A false negative in an Intrusion Detection System (IDS) is an attack that is missed because an alarm was not raised. |
| Sensor | The sensor is a network appliance that is easy to install and maintain on a network. It uses a rules-based engine to distill large volumes of IP network traffic into meaningful security events, which it forward to a Director. The sensor can also log security data, cut TCP sessions, dynamically manage a router's access control lists to shun intruders. |
| Tap | The IDS tap is a simple, secure and resilient connection into the network for the IPS/IDS Sensor. Well-designed taps fail-closed and do not create a potential point of failure in the network, eliminating the chance that the intrusion detection system can cause a network failure. When used with an IPS sensor, the tap allows the sensor to block offending traffic. |
| Telnet | The TCP/IP standard network virtual terminal protocol is used for remote terminal connection service and allows a user at one site to interact with systems at other sites as if that user terminal were directly connected to computers at those sites. |

## 12. ASSOCIATED DOCUMENTS

Invensys, (2005), Process Control Network Security: Reference Architecture

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

## FOR MORE INFORMATION

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

**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**