Secure Networks™ for Process Control
Abstract

This paper is focused at providing guidance for designing and deploying Secure Networks supporting the process control environment. With the increasing dependencies of open-standards Ethernet and TCP/IP-based network systems in the process control environment, it is now critical to address the security vulnerabilities common to these communication infrastructures. Leveraging the pervasive nature of the network infrastructure can provide a valuable asset in the overall approach to securing critical infrastructure. The use of access control, proactive protection, and dynamic response technologies provides the best holistic approach to network security in process control.

In this paper, specific network security technologies and implementation practices will be explored.
# Table of Contents

Table of Contents .....................................................................................2

The Process Control Network .................................................................3

Spectrum of Security Challenges............................................................4

- Opportunistic Predators .................................................................4
- Targeted Attacks ................................................................................4
- Regulatory Mandates ..........................................................................4
- New Technologies ..............................................................................4

Designing a Secure Network for Process Control .........................5

- Access Control ..................................................................................5
- Proactive Protection ...........................................................................8
- Dynamic Response ............................................................................10

Secure Networks Reference Architecture for Process Control .....13

Summary .............................................................................................22

Appendix 1: Infrastructure Device Security Configuration .............23

- Disabling Unnecessary Features ......................................................23
- Secure Host VLAN ..........................................................................23
- Securing Dynamic Routing Protocols .............................................23
- Host Denial of Service Prevention ..................................................23
- Access Control Lists .........................................................................24
- Host Management Port Access Control (authentication) ...............24
- Passphrases .....................................................................................24
- Radius .............................................................................................25
- Inbound Rate Limiting / Class of Service .......................................25
- Flow Setup Throttling ......................................................................25
- MAC Locking ..................................................................................25
- Spanguard ........................................................................................25
- Broadcast Suppression .....................................................................25
- GVRP Disabled per Port ...................................................................26
- Discard VLAN Tagged Frames .......................................................26
- SNMP ..............................................................................................26
- Logging ............................................................................................26
The Process Control Network

The communications infrastructure in process control environments is evolving. There is a shift from the highly proprietary process control communications systems of the past to communication systems that are inline with the traditional business data networks of today. These network systems are heavily rooted in standards-based Ethernet (IEEE 802.3) for the communication medium and TCP/IP for the communications protocol. According to an industry survey by the Reed Research Group, 78% of the respondents currently use Ethernet and TCP/IP in their process control environments and 84% responded that they have current plans to use Ethernet and TCP/IP in their process control environments. Although this shift to a standards-based network communications approach brings about much desired consolidation of systems and resources, it also represents a new and potentially major security risk to process control systems and the critical infrastructure that they support. Threats such as Distributed Denial of Service Attacks must now be considered when deploying the supporting technology of a process control system. If the business-typical operating system platforms that are “monitoring” the plant environment become vulnerable to attack, the potential for loss of visibility or even control of critical processes becomes a reality. The results of an attack on these systems could result in a process malfunction which may have serious financial ramifications or even hazardous situations where environmental and human life issues may arise.

In addition to the new communication systems and architecture which supports the evolving process control environment, there is the changing requirement of administration and operation of these systems. As process control environments converge into the overall architecture of the enterprise network systems, IT organizations will likely have to take on the additive responsibility of securing not only the traditional computing environments of the enterprise network, but also the converged mission-critical data of the process control system. Access control technologies become even more critical with the requirements of user and system communication in a process control environment. Proactive protection must include all converged systems in its coverage model, threat response technologies must be effective in recognizing and mitigating potential dangerous events occurring anywhere in the converged network, and remediation of vulnerable and untrusted systems must be safely administered on the network system without risk to neighboring devices and systems.
Spectrum of Security Challenges

A wide range of security challenges confront the architect of new-age process control network systems. These can be broadly categorized as opportunistic predators, targeted attacks, regulatory mandates, and the impact of new technologies.

Opportunistic Predators

The most visible and alarming threats to the network infrastructure are caused by opportunistic predators. These are service-level attacks that, while not specifically targeting organizations or systems, can cause widespread disruption to plant processes. Increasingly sophisticated network-born “worms” and viruses have caused widespread damage resulting in lost business opportunity, employee and process downtime, and high recovery costs.

The typical worm has some distinct characteristics. It exploits a known vulnerability in a widely deployed system (such as Microsoft Windows or Cisco IOS) to gain privileged access to that system. Once access is achieved the worm will attempt to cover its tracks, then examine or alter confidential information, then launch attacks against additional systems. Worms are becoming more sophisticated - new blended threats seek to exploit multiple vulnerabilities and utilize many techniques to transmit and spread an attack. In addition, the accelerated rate of propagation of a dangerous worm makes it a significant culprit in the disruption of mission-critical services running on the network infrastructure. As opportunistic predators continue to evolve and become more sophisticated and devastating to the network connected systems, the stability and reliability of process control environments are in clear jeopardy.

Targeted Attacks

In contrast to opportunistic predators, targeted attacks are designed to compromise specific systems with the goal of stealing intellectual property or disrupting business or plant operations. Targeted attacks can also be connected with more sinister objectives including those of terrorists and rouge governments. Snooping attempts to monitor or analyze traffic on a physical network involve attempting to gather system credentials and then capture data or leverage connected systems for malicious purposes. Spoofing is the process whereby an alien machine or system represents itself as a legitimate network device in order to gain access to critical information or adversely impact critical processes. Snooping and spoofing are techniques used by the criminal or terrorist to exploit systems for financial gain, or in the case of critical infrastructure, to enact a disaster potentially taking human life.

Regulatory Mandates

Government agencies and international regulators are defining acceptable and unacceptable uses for corporate information, as well as tracking this use and imposing severe penalties when organizations fail to adhere to these rules. In addition, there are a number of security related standards and regulations that are being developed for critical infrastructure and its related process control systems. For example the ISA SP99 standard is taking a more concerted approach to addressing the issue of network security in the process control environment. The US Department of Homeland Security now has specific regulations within the Homeland Security Act pertaining to information security in critical infrastructure.

Complying with these regulations demands a commitment of technology resources which can significantly increase operational expenses. Architecting the process control system must now include the technologies and methodologies required to meet emerging government and industry regulations.

New Technologies

With the introduction of new networking technologies in the process control environment comes risk. As more robust, efficient systems are recognized in process control, a significant amount of analysis must be given to the potential for associated security risks. Better operational models and higher efficiency is important for the ultimate goals of the process environment, but this and more can be in jeopardy if a careful design is not formulated to eliminate security risks. In addition to the introduction of new technologies into the process control environment itself, there is the trend of widened visibility and operational models. Many process control environments are moving toward the inclusion of a secure interface with the business network. This accommodates an operational model which includes involvement by offsite experts and vendors, but also opens the door to additional access control security concerns. Careful design must be given to balance the benefits of a highly efficient operational model and the potential risks that come with the expanded connectivity required to realize this model.

Faced with the combination of this broad spectrum of security challenges and the convergence of the business and process control environments, there is urgent need to upgrade security defenses and countermeasures. The network infrastructure can act as the integration point for communications security technologies because of its pervasive presence and ability to control both individual users and devices. However in order to make the network infrastructure become this full participant in the security architecture of IT systems, it must become an intelligent system that delivers additional value to the business.
Designing a Secure Network for Process Control

Building a secure network for a process control environment requires attention to several aspects of network design. Technologies used and the deployment of those technologies must tightly secure the specific process control network environment from internal and external attacks or breaches. Both proactive and reactive protection methodologies must be implemented to ensure that mission-critical communications run unaffected by security events. In addition, centralized command and control of security policies must be realized for operational effectiveness.

Using Enterasys’ Secure Networks architecture, with the Enterasys® I-Series and Matrix/SecureStack line of switch products, Dragon intrusion defense products, and NetSight management applications, a comprehensive approach to access control, proactive protection, and dynamic response is realized – creating a highly specialized network security model for the process control environment.

Access Control

There are several different access control requirements that must be addressed in the process control environment. The most obvious requirement being the guarantee that only persons who are authorized to operate systems and applications connected to the process control network are allowed to do so, and others are restricted from any communications at all. It is important to consider this requirement of access control for both internal (on-site) personnel as well as external (off-site) personnel. Additional consideration for this requirement must be given to the access of the process control network from the level-4 or “business network”. Another requirement is to have controls in place to strictly manage what physical devices and end-systems are allowed to even connect and communicate on the level-1, 2, and 3 networks in the process control environment. This is the concept of machine-centric access control policies vs. human-centric access control policies. Both are critical when implementing a comprehensive security strategy. Finally, there is an additional requirement to control the access of systems and services by other systems and services. This is the concept of controlling which specific types of applications and communications are allowed to occur on the process control network. Communication policies must be enforced to strictly control access to mission-critical applications and the related communications protocols which support them. With these policies, the availability of mission-critical applications can be guaranteed by controlling who has access to these applications and how they are used on the infrastructure.

Deploying an Enterasys Secure Network addresses each of these specific access control requirements. Leveraging sophisticated network infrastructure hardware and firmware along with a centralized management aspect, access to the critical process control communications environment can be strictly controlled to align with security policies. The following information describes the technologies and implementation involved with an Enterasys access control solution for the process control environment.

1. Human-centric authentication and authorization.

Leveraging a forced authentication configuration on Enterasys access layer switches, access to the network is restricted to only the users who have the appropriate credentials. Several authentication schemes can be utilized including basic manually entered “user name” and “password”, digital certificates, 2-factor authentication (ex. smartcards), and even biometrics (ex. fingerprint). The configuration of the authentication requirements is done centrally from NetSight Policy Manager - a single point of policy administration and through the use of a standards-based RADIUS and directory service. Users who do not supply appropriate credentials when required are prevented from any and all communication on the process control network. The details of the authentication process for human-centric access control are shown below in Figure 1.

![Figure 1: Secure Networks Human-Centric Access Control](image)

With this deployment of human-centric access control, the Enterasys network switch in the process control environment will restrict any and all communication on the network until the user utilizing that end-system provides the correct credentials to the authentication service.

In addition to the capabilities of the Enterasys network switch to force a user to provide credentials before allowing any network communications, specific technology in firmware allows for the authentication of the end-system device itself. Using the centralized management and configuration methodology, the network switch can be made to reject any and all communications except from “allowed” end-systems. This can be regardless of whether or not a “user” attempts to authenticate from the end-system device. This is a very effective approach to securing what physical devices can connect and actually communicate on the process control network. The details of the authentication process for machine-centric access control are shown below in Figure 2.

![Figure 2: Secure Networks Machine-Centric Access Control](image)

With this deployment of machine-centric access control, the Enterasys network switch in the process control environment will restrict any and all communication from an end-system unless the MAC-Address of the end-system is recognized by the authentication service as a valid address to communicate on the network. In addition, once the end-system’s MAC-Address is validated, the network switch can “lock” the specific end-system device to the specific physical port it is connected to by using the MAC-Address as an identity. The end result of this machine-centric access control methodology is that exact connectivity on the process control network can be “hardened” and no unknown device can communicate on the network.

3. Application and service authentication and authorization.

Not only is it important to control the access that humans and machines have to the process control network, it is an ideal security practice to control access to certain applications and services based on the user or device connecting to the network. This methodology provides an approach of granularity with secure access control policies. The fact that a human or particular end-system can be authenticated as appropriate to communicate on the process control network, does not in itself guarantee that subsequent communications will be restricted to appropriate applications and services. A granular approach to access control policies will include specific network communications traffic permissions and restrictions based on the identity of the human and/or machine that is authorized to communicate on the network. This is the concept of enforcing a set of secure communications policies for an identified user and/or end-system on the network. The approved communications policies should match the operational “role” of the user and/or end-system within the context of the process control environment. Role-based administration is the modeling of both IT security technologies and process control operations. This is achieved through the creation of the relationship hierarchy, shown in Figure 3. In this graphic, note that the business/process functions are modeled at the top (Roles/Behavioral Profiles), and technological considerations are at the base (Network Traffic Classification Rules), with the Services/Applications layer providing the bridge between these two. The high-level focus can be on the specification of the roles in the environment and on mapping the appropriate services to them. The details of the classification rules needed to realize each service can be left to technicians familiar with packet formats, frame types and protocols.
The ability to include services in multiple roles further simplifies the operation by eliminating the need to duplicate service creation for each discrete role. A service can be constructed once, and used again as needed for as many roles as is necessary.

In order to recognize the comprehensive model of secure access control defined above in the three aspects of: human-centric, machine-centric, and application/service-centric authentication and authorization, the specific network infrastructure components (network switches) must support some unique and advanced security technologies. Human and machine-based credential verification must be enabled through the use of Extensible Authentication Protocol (EAP) – specifically IEEE 802.1X standard for authentication. Web browser-based authentication challenges must be enforceable from the first point of entry into the network infrastructure. Machine-centric credential verification such as physical addresses, manufacturer identification, and embedded credentials must be supported by the network infrastructure components. Back-end RADIUS Authentication/Authorization/Accounting (AAA) services must be utilized in conjunction with the network infrastructure components to identify the connecting user or device, authorize network communications and usage, and enforce specific security policies based on identity. This requires that the network infrastructure switch has the capability of appropriately communicating with a RADIUS Server using a standard authentication packet exchange sequence. The network infrastructure must also support the ability to granularly classify network communications traffic and make forwarding, filtering, and Quality of Service (QoS) decisions based upon the established security and network usage policies. Figure 4 depicts the controls on a network switch necessary for secure access control in a process control environment.

Figure 3: Secure Networks Policy Relationship Hierarchy

Figure 4: Secure Networks Switch with Advanced Access Control and Policy Enforcement
Proactive Protection

Proactive protection is the concept of taking deliberate steps to prevent security breaches and inappropriate network usage by identifying vulnerabilities and threats before they establish themselves in the network. In a process control environment, protection against threats is critical to ensure the safe and effective availability of systems. Being proactive with respect to this protection can make the difference between stopping a security problem before it is ever established and reacting to a security problem once it has affected the critical processes. One aspect of proactive protection is to ensure that the network infrastructure components themselves (meaning the underlying communications system) are secure from attack. If the network communications system itself is impacted from a security attack and not able to forward critical application traffic, the entire process control is in jeopardy. Another aspect of proactive protection is to ensure that any known dangerous or threatening usage of the network is strictly prohibited. Any network traffic associated with a known threat profile must not ever be allowed to enter the network anywhere in the process control environment. Finally, end-systems of any kind that connect to the process control network must be analyzed and assessed for trustworthiness before they are allowed to communicate on the network.

Deploying an Enterasys Secure Network addresses each of these specific proactive protection requirements. Leveraging sophisticated network infrastructure hardware and firmware along with a centralized management aspect, a strong layer of security can be applied to protect the process control environment from a multitude of attacks and undesirable network activities. The following information describes the technologies and implementation involved with an Enterasys proactive protection solution for the process control environment.

1. Secure network infrastructure components.

When implementing any component or device (such as a switch or router) into a network, it is important to ensure that appropriate configurations are made to proactively protect that device from attack or exposure to a separately targeted attack. There are several architectural capabilities of the network infrastructure device that must be considered to effectively apply an appropriate device-specific security configuration. The key areas of configuration are: the ability to disable unnecessary features, the ability to secure the device against service availability attacks, the ability to secure administrative protocols, and the ability to secure the management and control of the device itself. A set of infrastructure device features that enable this secure configuration include:

- Selectable Device Features (on/off)
- Secure Host VLAN Configuration
- Dynamic Routing Protocol Authentication
- Host Denial of Service Prevention Configuration
- Host Port Access Control Lists
- Authenticated Host Management Access
- RADIUS Configuration
- Inbound Traffic Rate Limiting
- Flow Setup Throttling
- Spanning Tree Protocol Controls and Protection
- Broadcast Suppression Controls
- Multicast Controls
- Secure Management Protocols
- Secure Logging

By deploying a network infrastructure device that has these types of controls and features, the process control network communications hardware itself can be proactively protected from attack. To get additional detail on each of these important device-specific features, see the “Infrastructure Device Configuration” information in Appendix 1 of this paper.
2. Acceptable network usage policy

In a process control environment, network communications should be strictly controlled so that only the required protocols and application traffic are allowed. Dangerous and unnecessary traffic should be restricted from the network. This is the concept of proactively protecting the entire network system from exposure to potential threats introduced through non-acceptable communications traffic. An acceptable network usage policy must be enforceable throughout the network infrastructure so that only “acceptable” communications traffic can traverse the infrastructure and unacceptable communications traffic is filtered right at the entry point onto the network infrastructure. Enforcing this type of communications requires advanced traffic controls to be imbedded into the network switches where end-systems are directly connected. Also, a centralized command and control point of management must be present to configure the appropriate communications rules and to configure the switches to enforce the rules. With this policy framework in place, every point of entry into the process control network can be provisioned (centrally) to allow any necessary traffic from a connected end-system, but to filter any unnecessary or known dangerous traffic. Included in the filtered traffic policy rules can be the restriction of protocols and application traffic that can be misused (either maliciously or non-maliciously), presenting a threat to the process systems. Examples of network communications traffic that should be filtered at the immediate entry point to the network may be SNMP, routing protocols, DHCP server, known worms and network viruses (through layer 4 port and socket identifiers), etc. By enforcing an acceptable network usage policy at all points of connection within the process control network, a significant foundation of proactive protection can be established for the entire communications environment. The details of enforcing acceptable network usage policies in a process control environment are shown below in Figure 5.

![Figure 5: Secure Networks Acceptable Use Policy Enforcement](image)

3. End-System assessment.

Proactive protection technology utilizes embedded controls in the network infrastructure components to recognize end-systems before access to the network is permitted, and trigger an evaluation and assessment of the end-system’s trustworthiness. End-system assessment can identify critical vulnerabilities in an operating system, security software, or application that could result in the end-system becoming dangerous to the process control environment by introducing a threat or even becoming infected and propagating a threat. It is a well known fact that major operating systems can contain imbedded security flaws. Antivirus software is also a threat management application that must be provisioned in order to maintain its effectiveness in preventing security attacks to the end-system, and propagated from the end-system. As these well-known operating systems become more and more important in the process control environment, attention must be paid to the inherent security risks associated with them. Recognizing these system vulnerabilities in real-time can be a difficult task. Proactive protection technology allows for the automatic launching of vulnerability assessment applications once an end-system attempts to connect to the network, and then again in regular intervals while the end-system is a connected member of the network environment. Using advanced access control technologies, the end-system (no matter what it is) can be identified the moment it connects to the network. The intelligent network infrastructure in the process control environment can restrict the network and service usage of the end-system while triggering a comprehensive assessment of the end-system's patch levels and configuration. If the end-system passes the assessment and proves to be in conformance with the established security policies for communicating in the process control environment, the appropriate application and service usage will be allowed. The dynamic nature of this technology allows for an enhanced layer of security while maximizing process efficiency. The details of end-system assessment in a process control environment are shown below in Figure 6.
Dynamic Response

Dynamic response is the concept of a fully integrated systems-level response to an identified threat or undesirable communications event on the network. Having an automated and dynamic response to identified security problems is critical in establishing a “time-to-respond” metric that allows critical communications to applications and services in the process control environment to stay effectively available. The reality of any network system environment today is that no matter how good the proactive protection technologies are in preventing security breaches, there will be new and emerging threats that slip by. Solid Intrusion Detection System (IDS) technology is critical in providing a level of deep inspection of communications traffic on the process control network. If the IDS technology identifies any security anomaly, specific source isolation and mitigation technologies must be leveraged in an integrated fashion to quickly eliminate the threat to the environment at its source. This dynamic response solution is an integrated collection of intrusion detection, source location services, and managed responsive action. When fully integrated into a cooperative system, this dynamic response solution can effectively mitigate threats bypassing any proactive protection measures in a matter of seconds.

Deploying an Enterasys Secure Network addresses each of the required technologies and their integration required to realize dynamic response to network threats in the process control environment. Leveraging sophisticated network infrastructure hardware and firmware along with intrusion detection security appliances and centralized management, a security solution can be formed to dynamically remove any threat as soon as it enters the network. The following information describes the technologies and implementation involved with an Enterasys dynamic response solution for the process control environment.

1. Intrusion and threat detection.

Intrusion detection systems are designed to identify “intrusions” to the network or more broadly described, anomalous network communications behavior that constitutes a security threat of some kind. This is accomplished through the analysis of network traffic, looking for matches to known or custom developed “signatures” which describe a particular threat. In addition to network traffic, intrusion detection systems will search through various system and device logs and data output to identify any pattern indicating a threat. The intrusion detection system is deployed as either a “network-based” or “host-based” system, and they can be used separately or together to form a comprehensive identification framework. Network-based IDS utilizes a strategically placed network attached appliance that simply analyzes any traffic that passes by its connection to the network. Host-based IDS utilizes specific software coexisting on a network attached host (typically a server or important service appliance). In either case, the result of a threatening traffic flow on the network that has a corresponding signature in the IDS, is “detection”. Once a threat or security breach is detected, the IDS will provide certain information about the “event”. Security event information will include a description of the threat causing the event, and any source Layer 3 address information that is found to be related to the traffic associated with the threat. Although this information is critical to understanding more about the threat to the process control environment, it does not typically identify the exact source in the physical network where the threat originated. The benefit of the integrated technologies in the dynamic response solution allows this threat information to be shared with other components that can pinpoint the exact physical location of the source of the threat. The details of intrusion detection are shown below in Figure 7.
2. Location of the threat source.

Identifying threats to the process control network environment is critical, but if the source of the threat is not dealt with, the required end result of full mitigation will not be achieved. The most important and unique premise of the dynamic response approach to mitigating threats is the integration of the event detection information with an advanced technology that can locate the exact physical port where the threatening traffic is originating from. Since the event information in the intrusion detection system only identifies the layer-3 source address (the IP address for TCP/IP communications), the exact physical location of the threat source cannot be isolated. It is imperative to obtain the key end-system identifier of the physical source address (MAC-address). To do this, the event information is used to trigger a resolution of the source layer 3 address to the source layer 2 address (MAC address). Leveraging advanced node and alias information maintained on real-time on the network infrastructure switches and a management and control software application, the entire process control network infrastructure can be queried to resolve the physical address that is associated with the layer 3 address obtained from the IDS event information. Network infrastructure components are interrogated and the switch where the end-system originating the threat is connected responds with the source MAC address associated with the layer 3 address. Included in this information is the physical port where the source MAC address is currently connected and generating traffic. Now armed with this information, the dynamic response solution can perform the appropriate mitigating action against the exact source of the threat. The details of the source location process are shown below in Figure 8.
3. Managed response.

The ultimate goal of the dynamic response solution is to totally mitigate any threat to the process control environment before it can cause any major impact. As described above, the first two steps to this goal are to identify a threat or security breach that bypasses any of the proactive protection measures put in place. The second step is to resolve the physical location of the source of the threat by using the information contained in the identified security event and the intelligence of the Enterasys network infrastructure products. Once an exact location (physical network switch port) is identified, appropriate action can be delivered. It is important to recognize that “action” can vary greatly based upon what the administrator of the network would like to do about any particular security event, and the capabilities of the network infrastructure device housing the source port of the threatening end-system. The one critical aspect of an effective dynamic response solution is that it is “dynamic”. In other words, it is critical to absolutely minimize the “time-to-respond” metric when addressing real-time threats. Any mitigating action to a serious event must be pre-determined (based on the event type and severity) so that no human intervention is necessary to perform the necessary action. Once the actions are configured, the entire dynamic response system can automatically mitigate threats as they appear on the process control network.

The action taken against the source of a threat to the process control network can be as minimal as “notification” of the event and its source to security administrators, and as severe as turning off the physical switch port where the source of the threat is located. The benefit of the pre-defined action is that a security administrator can determine up front what action should be taken against a particular type of threat, and then configure that action to take place in the event of a corresponding security breach. Leveraging an intelligent network infrastructure, granular policy enforcement can be accomplished as an action to a particular security event. Restrictive network communications rules and even quarantine status can be enforced on the source port where an offending end-system is connected upon the identification of a threat. In order for an effective set of action rules to be enforced as part of the dynamic response solution, the network infrastructure products must be able to accommodate the policy rules as determined by the dynamic process. In addition, there must be a centralized administration and control software point for aligning appropriate policy rules to be enforced with specific security event types. The details of managed response are shown below in Figure 9.

In order for the dynamic response solution to be effective in a process control environment, the three technologies described above must be fully integrated. The effectiveness of the solution is in the ability to fully automate the process of detecting a security breach, locating the source of that breach, and taking action against that threat by enforcing an appropriate network communications policy at the point of network communications for the source. This is only accomplished through the use of a sophisticated architecture of intelligent and policy-aware network infrastructure products, advanced configuration management, and industry-leading intrusion detection. The diagram below (Figure 10) depicts the integrated relationship between the critical technologies involved with dynamic response.
Secure Networks Reference Architecture for Process Control

This section will introduce a reference architecture for deploying Secure Networks in a process control environment. Using an example of a typical critical infrastructure process control network, the technologies and solutions offered in the previous section will be positioned and depicted as an integral part of the reference architecture. The result of the careful deployment of the technologies and solutions described in the preceding sections of this paper will provide for a “Secure Network” deployment and ultimately a highly secure and reliable process control environment.

The diagram below depicts a typical process control network with connectivity between the various network levels within a plant environment.
Access control technologies are dispersed throughout the Secure Network. All aspects of access control requirements are deployable in this reference architecture. Human-centric authentication and authorization is positioned at the entry point of the level-4 business network for the remote user. It is also strategically positioned at the demilitarized zone between the level-4 and the level-3 networks. Finally, human-centric authentication and authorization is positioned within the level-3 process control monitoring network. In each of these security points, user’s of the communications network must be authenticated, and access to critical services must be authorized. Figure 12 depicts human-centric access control within the reference architecture.

![Human-Centric Access Control in the Process Control Network](image)

Machine-centric authentication and authorization is contained within the level-2 and level-3 networks. End-system accountability is provided through the strict access control paid to the end-systems attempting to connect to the infrastructure in these high security environments. Only designated end-systems will be allowed to communicate on the level-2 and level-3 networks, and the entire connected end-system environment will be “locked down” in the level-2 network. Figure 13 depicts machine-centric access control within the reference architecture.

![Machine-Centric Access Control in the Reference Architecture](image)
Application and service authentication and authorization is enforced in the level-2 and level-3 networks for both local originating network traffic and remote originating traffic. Only the required application and service network traffic is allowed to exist on the level-2 or level-3 networks. All other communications traffic will be eliminated before it enters the network. In addition, specific restrictions of application and service communications will be enforceable to individual users on these networks based upon their role within the process control environment. Figure 14 depicts the application and service communications policy enforcement within the reference architecture.
Figure 14: Application-Centric Access Control in the Process Control Network

Proactive protection of the critical processes and services within the reference architecture is accomplished with the positioning of the technologies described earlier. The requirement of secure infrastructure components is accounted for wherever there exists critical infrastructure products which could be compromised or outright attacked, impacting their ability to deliver the foundations communications availability required for the process environment. Figure 15 depicts the positioning of secure infrastructure components.
Proactively protecting against known threats and communications vulnerabilities is accomplished through communications policy enforcement in the level-2 and level-3 networks. The advanced security features of the network access switches in these levels allow for the enforcement of specific traffic policies, eliminating all known threats and undesirable traffic from ever entering the network. Figure 16 depicts the positioning of the enforcement of proactive protection communications policies.

Figure 15: Secure Infrastructure Components in the Process Control Network
Providing end-system assessment technology to proactively protect from untrusted or dangerous end-systems is critical in the level-2 and level-3 networks of the process control environment. Any end-system connecting to the network in these environments will be recognized and remotely assessed before being allowed to communicate on the network (regardless of the user of the end-system). Figure 17 depicts the location of pervasive end-system assessment.
Finally, the usage of dynamic response technologies (as explained earlier in this paper) is critical in providing real-time protective measures to the process control environment. Threats and other security breaches that may be undetected by the proactive protection layers must be immediately identified and mitigated before they can seriously affect the process environment. Strategic deployment of network and host-based Intrusion Detection Systems within the process control environment and within the DMZ where remote access to the process control environment is obtained is critical in quickly identifying any security breaches. The use of the advanced location services as described earlier in this paper must be effective in isolating the exact source of any real-time threat to the process control environment. The advanced features and capabilities of the network infrastructure components within the level-2 and level-3 process control networks allows for the enforcement of appropriate mitigating action against any threat exposed through the dynamic response solution. Figure 18 depicts the combined technologies that integrated together from the dynamic response requirements for the reference architecture.
Using each of the key security technologies detailed in this paper, an effective security position can be realized in the modern communications infrastructure of the process control environment. With access to the communications infrastructure, the mission critical applications and services in the process control environment can be controlled and secured; significant proactive measures can be implemented to protect against known threats and dangerous communications behaviors on the process control network; and real-time threats to the process control environment can be automatically isolated and mitigated using innovative dynamic response security technologies. The result is a highly available and secure process control environment.

Using the reference architecture detailed above, an example can be applied of a remote contractor requiring secure access to the level-3 process control network. The contractor must establish a secure path of communications to the level-3 network, while at the same time not introducing any collateral threats or vulnerabilities to the highly critical process control environment. The detailed information below will walk through this example using the reference architecture and pointing out the critical security safeguards along the way to establishing secure communications with a monitoring station on the level-3 network.
1. A trusted contractor requires access to a monitoring station in the level-3 network in a critical process control environment. Traditional practices may have required the contractor to be present on-site within the level-3 network to gain the required access. In this case, the contractor is remote, and actually some several thousand miles from the physical site of the level-3 network. Using the deployment of Secure Networks and established connectivity between the process control environment and the business network, the remote contractor can obtain controlled access to the level-3 network without jeopardizing the company's security of its process control environment.

2. Using human-centric credentials, the remote contractor establishes a highly secure encrypted VPN tunnel into the company's business network DMZ. All communications are completely secured and private using traditional VPN technology.

3. Upon establishing identity, the remote contractor is given specific network policies so that a static encrypted communications path is provided between the business network (level-4) DMZ and the process control network (level-3) DMZ. This is done using a point-to-point VPN tunnel. The remote contractor has no visibility of any of the systems and services within the business network. The secure encrypted tunnel through the business network to the process control environment is point-to-point with no other communications options.

4. Once the remote contractor's path of connectivity is terminated securely to the level-3 DMZ, specific VLAN and layer 3 addressing identifiers are provisioned for the communications entering the level-3 network. In addition, firewall rules are established to prevent any communication from the DMZ into the level-3 network unless they originate from a trusted source terminating on the VPN gateway in the same DMZ.

5. A network-based IDS is positioned within the level-3 DMZ to monitor all traffic entering the level-3 network. Any anomalous traffic behavior will be instantly recognized, and policy rules will be provisioned within the DMZ switches, routers, and firewalls preventing the traffic from entering the level-3 network.

6. Once the secure traffic from the remote contractor enters the level-3 network, it is authenticated as being from a trusted source and as being an appropriate application or service request. All communication within the level-3 network is policed to be in compliance with the acceptable network usage policies for the process control environment. Any deviation from the established communications policies within the level-3 network will cause the filtering of the undesirable traffic, or the severing of the entire communication flow from the remote contractor.
7. Once securely communicating within the level-3 network and utilizing the appropriate monitoring end-system and application, the remote contractor can perform the required tasks which may constitute communications from a level-3 end-system to a level-2 end-system. Any communications of this type brought on by the remote contractor would be subject to the standard policy rules of communication within the process control network. Only approved communications will be allowed, and any deviation will cause the severing of the entire connection. In addition, all communications within the level-2 and level-3 networks is monitored by network-based IDS. If any threatening or undesirable traffic is recognized, the dynamic response solution will immediately quarantine or “kill” the source of the remote contractor’s communications, right at the entry point into the level-3 network.

In this example, using the technologies and practices detailed in this paper, a more efficient use of remote resources can be safely established. Designing and implementing a Secure Network can greatly increase a company's operational effectiveness by using modern network communications infrastructure within the process control network and the connectivity between the process control and business networks.

Summary

Designing and implementing Secure Networks in the modern process control environment is critical to ensuring safe and efficient communications and process operations. With the evolution of process control technology including dependencies on traditional Ethernet and IP-based networking, an increase in operational effectiveness can be achieved. At the same time, increased security awareness is a must. Securing the process control network environment and the operational communications within it is a strategic requirement.

Leveraging the multitude of advanced technologies imbedded in the Enterasys Secure Networks products and solutions, a highly secure and effective operational model can be realized. With over 15 years in innovation of network communications policy technologies, centralized configuration and control solutions, and specific security products, Enterasys offers the process control industries a best-in-class Secure Network architecture. Covering all critical aspects of securing a network with access control, proactive protection, and dynamic response, Enterasys leads the way in securing critical infrastructure.
Appendix 1: Infrastructure Device Security Configuration

This section details global features, as well as architectural considerations of the infrastructure devices themselves, which can be deployed to help limit exposure to potential attacks to the network infrastructure. The infrastructure device features and architectural considerations discussed are:

- Disabling unnecessary features
- Containing device management host ports to a secure VLAN
- Using encryption on dynamic routed protocols
- Securing device management

Not all network infrastructure products deployed in the network will be configurable in the same manner. It is important to consider the necessity of these imbedded advanced features when choosing the appropriate network infrastructure products for implementing a secure process control network.

Disabling Unnecessary Features

To reduce the potential vulnerability of malicious attack of the network infrastructure itself, administrators may take the approach of disabling unnecessary features. Many potential security threats can be addressed in advance before more complex security technologies are utilized. As an example, Telnet, which is very useful for connecting to and managing network devices, should be disabled where SSHv2 is available. While Telnet is simple and ubiquitous, it sends data in clear text, allowing a hacker to examine the Telnet session for passwords and other important data. By disabling a feature such as Telnet, a security hole is patched which otherwise could allow a hacker to easily obtain information that can be used later for an attack. Other examples of features that could be disabled globally or on a per port basis throughout the Secure Network are web management utilities, host generated (the infrastructure device) multicast network management protocols, and SNMPv1 which also sends much of its data in clear text (SNMPv3 should be used in place of SNMPv1 wherever available).

Secure Host VLAN

A secure host VLAN is a non-default management VLAN whose only members are the host entities of the network infrastructure devices, administrators of the devices, management stations/servers, and Inter-switch-links (ISL) in a switched environment. A switch’s management interface should only be accessible by IT administrators, network management stations, and servers. General users or other devices on the network should not have the ability to contact the host. By isolating the management host ports of the infrastructure devices from general users on the network, the chances of an attacker modifying a configuration file or compromising the host via a Denial of Service (DoS) attack are reduced.

Securing Dynamic Routing Protocols

When securing dynamic routing protocols, the IT administrator should configure all user ports as passive interfaces with respect to dynamic routing protocols. Additionally, the administrator should ensure network devices authenticate before exchanging network routes. The task of configuring user ports as passive interfaces is essential. Routing updates provide detailed routing information about the network. This information can provide a hacker with topological information that can be used to exploit the network. In the event that a hacker is able to obtain topology information from the network, implementing authentication for dynamic routing protocols will prevent impersonation of network infrastructure devices or injection of invalid routes into the network. Using authentication can also prevent a malicious user from injecting malformed packets targeted at the routed interface in an attempt to tear down peering sessions in OSPF. There are two forms of authentication for dynamic routing. The first and less secure of the two authentication methods is simple authentication. Simple authentication provides a clear text key which is used to validate the integrity of routing updates. The second and more secure way of authenticating dynamic routing is through MD5 authentication which uses the MD5 algorithm to validate the integrity of routing updates. MD5 authentication should be used whenever possible throughout the routed interfaces in Secure Network.

Host Denial of Service Prevention

There are several Host DoS prevention mechanisms that can be implemented within the Secure Networks infrastructure devices:

**LAND**

A land attack is an IP-spoofing type attack that sends TCP SYN packets with identical source/destination IP addresses and identical source/destination TCP port numbers. Because the IP addresses and port numbers are the same, some implementations of TCP/IP stack will conclude that the packet originated from itself. This can potentially cause the device to hang or crash.

The LAND command enables land attack prevention and discards frames deemed illegal.
FRAGMICMP

The FRAGMICMP command protects against fragmented ICMP packets by discarding frames deemed illegal. By creating overlapping IP fragments it is possible to cause systems to crash, exceeding the allocated buffer size for a given packet type. One such attack that can overflow a buffer is the Ping of Death which uses a fragmented ICMP packet that exceeds the maximum 65,535 bytes of data allowed by the IP specification. (Reference the Total Length field, of 16 bits, which limits the size to 65,535.) The oversize fragmented packet is sent to an unsuspecting system. When the system reassembles the fragmented packet, it may crash, hang, or reboot due to the size of the packet when it is reassembled in memory.

LARGEICMP

The LARGEICMP command enables large ICMP packet protection, by specifying the packet size above which the protection starts, and automatically discarding illegal frames. Valid packet size values are 1 to 65535. The default is 1024.

PORTSCAN

At attacker could execute a scanning utility such as NMAP or Nessus in order to search the network for open TCP or UDP ports to exploit.

The PORTSCAN command provides protection by notifying an admin via SYSLOG when a port scan occurs, no further action is taken.

CHECKSPOOF

Spoofing is network identity forgery and is accomplished by replacing the hardware MAC address and/or the source IP address in the IP header in order to conceal the identity of the attacker. Because many tools randomly spoof the source address in every packet they generate, it is difficult for the network administrator to locate the attacker.

When the CHECKSPOOF command is enabled, spoofed packets are discarded. This command works by looking up the return path of an address to verify that the packet would egress from the same interface where it arrived. This feature should only be enabled on access devices. CHECKSPOOF reduces the success of source address spoofing, but does not stop an attacker from using a forged address of another host within the permitted prefix. Special care should be taken on dual homed access nodes due to the potential of asymmetric routes.

Access Control Lists

Access Control Lists (ACLs) should be used to control access to the host entities on the Secure Networks infrastructure devices as well as access to servers. For example, an access control list could define a list of management stations that have privilege to use SNMP for managing devices on the network. By defining a finite list of management stations the vectors that a hacker can use to compromise the network are limited. Another potential ACL to consider is to explicitly deny users access to the management stations defined in the first ACL. Access control lists coupled with dynamic policies can severely hamper an attacker's chances of compromising a network when deployed appropriately.

Host Management Port Access Control (authentication)

Host “Access Control Authentication” authorizes user access of remote terminal, local console, and Webview management via a central RADIUS Client/Server application. When RADIUS is enabled on the infrastructure device, the local user accounts for host port management are bypassed. Instead, usernames and passwords configured on the RADIUS server are used. Only in the case of a RADIUS timeout will login credentials for host port management access be compared against credentials locally configured on the network device. This feature will force users attempting to access the host management interfaces of infrastructure devices to authenticate themselves to the enterprise directory before any authorization is given. IT administrators would be authorized to manage the infrastructure device once the appropriate credentials are submitted to the RADIUS server.

Passphrases

A best practices password policy should be implemented for password protected infrastructure devices to help protect them from being compromised by brute force password attacks. Passwords should be at least 8 characters long, should not be dictionary based, and should contain at least 3 of the following types of characters:

- Lower case characters
- Upper case characters
- Numbers
- Special Characters (symbols on number keys accessible via SHIFT)

Password aging and history should be used to force periodic changing of passwords.
RADIUS
When deploying RADIUS authentication, a primary and secondary RADIUS server should be implemented to prevent a single point of failure. RADIUS is a critical element when using dynamic policies and host access control authentication. From the internal network, only switch hosts and remote access servers should be allowed to communicate with the RADIUS server. All others should be explicitly denied access via policy and ACL deployment. The RADIUS secret should adhere to the same rules as network passwords as discussed in the “Passphrase” section.

Inbound Rate Limiting / Class of Service
Inbound rate limits should be set on all user ports in a Secure Network. Rate limits are associated with a class of service on the network. As an example, if guest users are given a CoS of 1 on the network, an Inbound Rate Limit of 512 Kb/s can then be applied to any traffic with a CoS of 1. Providing Inbound Rate Limiting to untrusted and trusted users can limit the impact a Distributed Denial of Service attack (DDoS) can have on the network. By setting inbound rate limits, a greater number of hosts need to be compromised in order to execute a successful DDoS. The appropriate rate limit values should be established through proper investigation of typical and expected network usage parameters.

Flow Setup Throttling
Flow Setup Throttling will allow the IT administrator to define an appropriate number of acceptable flows per port, as well as monitor the new flow arrival rate. By defining an Enterprise User Policy and action for their particular environment, network administrators can regain control of malicious worms and viruses.

A flow is defined as a combination of L2/L3/L4 packet information. The relevant packet fields are source and destination MAC addresses, source and destination IP addresses, and source and destination TCP or UDP port numbers. An Enterasys switch examines all traffic at the point of entry into the switch port. During this examination process, the switch is required to inspect these packet fields to determine if this data flow is part of an existing conversation or if it is the first packet of a new flow. Once the data flow is determined to be new, the switch is required to make a decision on the exit port used to leave the switch. This completes the process of creating a L2 or L3 flow table entry. All flows are unidirectional in nature even when bidirectional communications exist. Switch port and VLAN classification/prioritization rules define and apply the level of packet inspection that is desired.

Flow Setup Throttling can be implemented in a Secure Network to prevent network Denial of Service symptoms caused by worms such as MS-Blaster, Slammer and Sasser. These worms attempt to replicate themselves by scanning for uninfected machines through the use of TCP, UDP and IP address scans. Case study networks at Enterasys have used a minimum flow threshold of 30 (SNMP Trap issued) and a maximum flow threshold of 50 (Port set to Disabled) as a reference. When an infected PC begins a scan of various ports to search for other computers to replicate the virus, the port will be disabled preventing the worm from spreading and protecting the network from a potential Distributed Denial of Service attack. The flow requirements for a customer network may vary from any case study and an analysis of flow requirements must be completed prior to implementing this feature.

MAC Locking
MAC Locking will allow the IT administrator to enforce the “one MAC address per port” rule which will prevent users from connecting “wild” devices such as rogue switches or Wireless Access Points aimed to connect multiple users in an uncontrolled environment. When MAC Locking is enabled on a port, the first “X” MAC address(es) seen (learned) on the port are automatically locked and other MAC addresses on the port will not be learned. Any traffic associated with the unlearned MAC addresses will be discarded. The locked MAC address(es) are released if a link down occurs. Note that the only management task related to MAC Locking is to enable MAC Locking on ports and eventually define the “X” value. The typical recommendation is to configure MAC locking so that only a single MAC address may be used on a port in order to mitigate against the threat of MAC address spoofing and to prevent users from connecting multiple devices on individual switch ports.

Spanguard
Spanguard is an Enterasys-specific switch feature designed to prevent BPDU (Bridge Protocol Data Unit) spoofing on user ports. When Spanguard is enabled, reception of a BPDU by a port will cause the port to be locked and its state set to blocking. The port will be locked for a globally specified time, which may be forever if the timer value is set to 0. The port will become unlocked when the timer expires, it is manually unlocked, or the configuration is changed such that Spanguard is no longer enabled. Spanguard can be utilized in the Secure Networks to prevent an attacker from injecting superior BPDUs into the network in an attempt to cause network topology changes. If Spanguard is not enabled, such an attack will cause re-spanning issues that could be disruptive to all users on the campus network as ports are sent into blocking, MAC address tables are flushed, and high rates of flooded traffic are seen on the network. This could cause a significant loss of availability of critical IT services.

Broadcast Suppression
Broadcast Suppression limits the amount of received broadcast frames that the specified switch port is allowed to forward to other ports. Broadcast suppression can be enabled on a Secure Network to protect against broadcast storms, leaving more bandwidth available for critical data. A potential attacker could easily use a packet generator application run by a PC to inject high rates of broadcast traffic. If broadcast suppression is not enabled and the broadcast threshold is not set to a low value, the attacker can very easily impact all users within, and prevent legitimate traffic from traversing the broadcast domain.
GVRP Disabled per Port

The purpose of GVRP (Generic VLAN Registration Protocol) is to dynamically propagate VLANs across a switched network. When a VLAN is declared, the information is transmitted out GVRP configured ports in a GARP formatted frame using the GVRP multicast MAC address. A switch/router that receives this frame examines it and extracts the VLAN IDs. GVRP then creates the VLANs and adds the receiving port to its tagged member list for the extracted VLAN ID(s). The information is then transmitted out the other GVRP configured ports of the device. It is the very nature of GVRP to propagate network information. Unfortunately, when GVRP is enabled on user ports, any attacker with a network analyzer can gain detailed VLAN information such as VLAN names and Filter-ID information. To put this into perspective, the attacker could extract from a GVRP packet that the “management” VLAN for the infrastructure devices resided on VLAN 50. That attacker could then inject frames tagged with VLAN 50 in an attempt to gain access to router and switch management. It is recommended that GVRP be disabled on all user ports throughout a Secure Network environment.

Discard VLAN Tagged Frames

When the Drop VLAN Tagged Frames feature is enabled, any packet already tagged with a VLAN that ingresses the port will be dropped. This provides extra security by preventing general users on the network from connecting to a network device capable of VLAN tagging in an attempt to gain access to various VLANs on the network. In most cases, the feature should be enabled on user ports in a Secure Network to prevent users from tagging their own traffic. It should be disabled on inter-switch link ports, where tagged packets should be accepted. If the user ports allow tagged frames, the attacker could simply set the network interface card on any PC to send tagged frames on any VLAN, including those normally restricted to users such as the management VLAN.

SNMP

SNMP v3 should be used instead of SNMP v1 on all capable devices throughout the Secure Network. Authentication and privacy passwords should be enabled when configuring the SNMP v3 parameters. SNMP v1 should not be used since it is a clear text protocol and susceptible to packet sniffing. On legacy infrastructure devices in the network that do not support SNMP v3, ensure that the default community string is changed to something other than public with read-only access. If write access is needed when using SNMPv1, a different community string should be used for each device in the network. Only official IT network management stations should have management access via SNMP. All user ports should be configured such that SNMP is explicitly discarded via policy.

Logging

SYSLOG messages should be sent to a centralized server. If at all possible, a backup SYSLOG server should also be implemented in another remote location. This gives the IT administrator the ability to correlate messages from multiple devices as well as insure no logs have been tampered with. SYSLOG provides the information needed to detect and diagnose a potential break in.