Introduction
Given the current focus on security and an increase in the number of regulations, standards and guidelines, it is clear that security is here to stay. And despite the myriad of options for security guidelines, there are many common characteristics among all of them. That is the concept of a “defense in depth” approach to network architecture. This paper discusses what Honeywell has been implementing since 1999. It is not all-encompassing or the only way to architect a network, but the following information does outline some of the concepts, benefits and considerations included in designing a secure network.

A Secure Process Environment (SPE) design should include a method of reducing the requirement of computing and network knowledge for plant personnel without jeopardizing the security and safety of the personnel themselves or the plant infrastructure. The use of open-standards-based networks and systems for process control provides the opportunity for problems normally associated with business LANs and the open Internet to cause loss of productivity and safety issues within our production facilities. Attention needs to be provided as to how these systems are integrated into our corporate network infrastructures to ensure that our process systems are secure from attacks.

Using the correct network design and operational principals, process systems usually can be protected from intentional system attacks, accidental system conflicts, software viruses and Trojan horses. Most, if not all, of these problems can be controlled and potentially eliminated.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Overview</td>
<td>4</td>
</tr>
<tr>
<td>SPE Technical Design</td>
<td>7</td>
</tr>
<tr>
<td>SPE Server Integration</td>
<td>7</td>
</tr>
<tr>
<td>Domain Controllers</td>
<td>7</td>
</tr>
<tr>
<td>Process Terminal Servers</td>
<td>7</td>
</tr>
<tr>
<td>Server Management Console</td>
<td>8</td>
</tr>
<tr>
<td>Process Historian</td>
<td>8</td>
</tr>
<tr>
<td>Process Relational Database Management System (RDBMS)</td>
<td>8</td>
</tr>
<tr>
<td>Client Integration Server</td>
<td>8</td>
</tr>
<tr>
<td>Process LAN Data Collector Nodes</td>
<td>8</td>
</tr>
<tr>
<td>Other Process LAN Servers</td>
<td>9</td>
</tr>
</tbody>
</table>
# Table of Figures

| Figure 1: | Security Design | ................................. |
| Figure 2: | Equipment relationship to the SPE Layers | ....................................... |
| Figure 3: | Secure process environment network design | ....................................... |
| Figure 4: | Secure process environment design | ....................................... |
Overview

The SPE design creates a layered network that segregates all process equipment from the business LAN, creating a network that is dedicated to process equipment, while allowing the movement of data that is necessary for business decision-making.

The design incorporates a method of rejecting all communications from the business LAN to the process LAN, but it still allows the movement of data to exist.

Problems such as software viruses, Trojan horses and worms are controlled without the requirement of loading antivirus software on process systems. This provides antivirus protection for those industrial systems that are not certified to run with antiviral software.

This design does not remove the requirement of ensuring all systems are loaded with security patches, which remove vulnerabilities to attack. This does, however, minimize the risk to process systems and allows the process control security team some time to assess true risk associated with proposed patches. In some cases, the risk inherent in specific patches can be negated at the firewall or traffic filtering point. In reality, loading of security and service packs on process systems is often not a process engineer's primary concern, and these patches are often left until all other tasks are completed.

A security controlled network layer, the process DMZ LAN, is constructed between the business LAN and the new process LAN. This network provides an area for security control. Both the business LAN and the process LAN are able to communicate with systems on the process DMZ LAN.

Figure 1: Security Design
This design provides a security focus in a small and limited area of the networks, reducing administration costs. All security programming on the firewall and the process LAN router is now focused only on rejecting or authorizing communications to the process DMZ LAN and not to process equipment. The security focus is now directed to a limited number of servers and not to all equipment on the process LAN.

The systems and servers on the DMZ LAN are required to have security and service packs updated on a regular schedule. SPE Technical Design

The SPE design incorporates a simple principle. Equipment belonging to a different aspect of the business belongs on a different network with a security zone inserted in the middle. This DMZ LAN is provided for equipment that requires communication to both networks. For reference, please see figure 2 (below).

![Figure 2: Equipment relationship to the SPE Layers](image)

Communications through the model start with moderate to high-level security at the business LAN Layer and progress to a very high-level security at the process LAN layer.

Honeywell’s SPE network design creates a multi-layer network. Each of the layers is created using physically separate network equipment. Due to conflicts in priorities between process and business network communications, it is not recommended to use VLANs on shared physical equipment. Business traffic is increasingly including high-priority audio and video data on the network. In process control, the process data requires the highest priority.
Figure 3 (below) shows a simplified representation of the network layers in the secure process environment network design.

![Figure 3: Secure process environment network design](image)

Figure 4, on the last page, shows a more detailed representation of the network layers in the secure process environment network design.

The existing business LAN is connected to the process DMZ LAN using a firewall. The process DMZ LAN is then connected to the process LAN using a router.

The firewall provides a controllable access point for users requiring access to servers connected to the process DMZ LAN. This firewall, depending on the type of equipment, can provide firewalling based upon IP address and port filtering or on user authentication. It is recommended that all traffic from the WAN router on the business LAN be rejected by the process DMZ LAN firewall. Access to the process data is made available to the remote user via a client integration server on the business LAN.

The router between the process DMZ LAN and the process LAN is programmed with a simple filter to ignore any and all traffic coming from the firewall or only accepting communications from registered servers from the DMZ LAN. This is an essential part of the security, yet simple to attain. The programmed filter rejects all packets originating from the Business LAN or the firewall itself. This reduces the possibility of a firewall hack attempt to reprogram the router and allows for changes to the filter on that router.
Further attention is given to the IP addressing of the process LAN. The network address used on the process LAN should be selected from the private network addresses allocated by the Internet steering committee. A table of the private network addresses is provided below for reference. Due to the growth of Ethernet- and IP-enabled process equipment, it is wise to choose an address from the Class B set of addresses. This would provide sufficient IP addresses for most existing process facilities and provide room to grow. Careful thought should be given to allocating IP addresses to the various areas within the plant.

<table>
<thead>
<tr>
<th>Private Network</th>
<th>Start Address</th>
<th>End Address</th>
<th>Subnet Mask</th>
<th>Number of Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td>10.0.0.0</td>
<td>N/A</td>
<td>255.0.0.0</td>
<td>1</td>
</tr>
<tr>
<td>Class B</td>
<td>172.16.0.0</td>
<td>172.31.0.0</td>
<td>255.255.0.0</td>
<td>16</td>
</tr>
<tr>
<td>Class C</td>
<td>192.168.0.0</td>
<td>192.168.255.0</td>
<td>255.255.255.0</td>
<td>256</td>
</tr>
</tbody>
</table>

Table 1: Private network addresses example

**SPE Server Integration**

A complete integration of an SPE network includes the integration of several types of servers and systems. These systems and servers are connected to the SPE networks based upon the requirements of the systems and the users requiring access.

Systems that have a complete process function are connected to the process LAN, while systems that are required to provide data to the business LAN are connected to the process DMZ LAN. Please reference figure 3 for placement of the servers into the secure process environment.

**Domain Controllers**

A pair of servers connected to the process DMZ LAN provide a domain controller function for the process LAN. A domain control system ensures that a central user authentication system is available for the process LAN, reducing administration time on process systems. These domain controllers can provide the domain controller function for various manufacturers’ configurations of domain controllers. Additional domain controllers may be placed directly connected to the process LANs within each process unit.

These servers also provide for file and print server functions for the process LAN and are intended to run the latest available antivirus software with current virus definitions.

All software and patches required on the process LAN are copied to a drop point (file system share) on one of the domain controllers and then retrieved off of the drop point from the system on the process LAN requiring the software or patch. This ensures that all software is scanned for viruses without having antivirus software loaded on every system on the process LAN. This procedure also eliminates the use of floppy and CD-ROM disks.

**Process Terminal Servers**

An additional server or one of the domain controllers is also programmed to act as a terminal server. Since no communications are available directly to the process LAN servers from the business LAN, client software (e.g. DCS programming, SCADA view, among others) cannot access any system on the process LAN. All access software would be loaded on the terminal server. A user with access permissions would log in to the terminal server on the process DMZ LAN and then run the required client program. This procedure not only restricts user access but also reduces the number of licenses of client software required and simplifies the administration of software on user desktops. From this server, a user is able to use applications that connect to a server on the process LAN.
Server Management Console

A server management console provides a local workstation for server administration and testing of connections into the process servers. Server administrators would also use this console for the creation of long-term archives on CD-R or DVD-R. In any server environment, it is often necessary to have a general use workstation available for the testing of server applications and to perform functions that are not appropriate to perform on the servers. Performing administration tasks from a remote console helps increase server reliability by removing the direct human access to the server.

Process Historian

The historian server is connected to the process DMZ LAN. From this location, the historian can retrieve data from data collectors on the process LAN and provide data to users on the business LAN. Direct access to the process historian can be restricted to only those who have direct access to the server.

Process Relational Database Management System (RDBMS)

The process RDBMS would be connected to the process DMZ LAN. Access to the data and storage capabilities of the database server are available from both the business LAN and the process LAN. Access directly to the process RDBMS is restricted to only those who have direct access to the server.

Client Integration Server

The Client Integration Server (CIS) is the main access point for users accessing process data. It is therefore an integral part of the full secure process environment.

In order to reduce traffic and administration costs on the process DMZ LAN firewall, it is recommended that this server be connected to the business LAN. With the CIS connected to the business LAN, the business LAN domain controllers provide user administration and authentication. The CIS server would be given access rights through the firewall to the historian and process RDBMS servers on the process DMZ LAN.

Placing the CIS on the business LAN decreases the administration required on the process DMZ LAN firewall. This reduces the rules and filters required on the firewall and size and specifications of the firewall itself. Often a simple low-end firewall is required instead of an expensive firewall that provides user authentication and secure ID features.

The role of the CIS is to provide a single point of access to all process server and data sources. Preferably developed using web technology, all users would have access to the data and information from the process systems using a standard web browser. Using one of several available products, even real-time trends are available using a web-based interface. There is no need to load a user interface tool on a user’s desktop. This reduces administration, licensing and hardware costs for the company.

The use of a CIS can provide a significant reduction in support costs normally associated with client tools. As changes to the tools on the CIS are made, all users have access to the new tools without licensing, propagation and loading of software.

Process LAN Data Collector Nodes

Interface and data collection nodes should be connected to the process LAN. In some instances, however, they may be connected to the process DMZ LAN or to both the process DMZ LAN and the process LAN depending on the installation requirements. Attention should be given to the load added to the Process LAN router(s) when placing the data collectors.
Other Process LAN Servers

All network equipment and servers that require access to both the business LAN and the process LAN are connected to the DMZ LAN. If the equipment is directly required for the running of a process, all attempts should be made to have the equipment located on the process LAN.

Figure 4: Secure process environment design

‘Powered by Matrikon’ symbolizes that this product/solution is system and application independent.

For more information:
For more information about Industrial Cyber Security, visit our website www.honeywell.com/ps or contact your Honeywell account manager.
www.matrikon.com
security@matrikon.com

Honeywell Process Solutions
1250 West Sam Houston Parkway South
Houston, TX 77042
Lovelace Road, Southern Industrial Estate
Bracknell, Berkshire, England RG12 8WD
Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywell.com/ps