Honeywell

Experion PKS
Network and Security Planning Guide

EP-DSX173
210
10/04

Release 210

Honeywell

Document	Release	Issue	Date
EP-DSX173	210	0	October 2004

Notice

Honeywell trademarks

Other trademarks

Support and other contacts

United States and Canada

Contact	Honeywell IAC Solution Support Center
Phone	1-800 822-7673. In Arizona: (602) 313-5558 Calls are answered by dispatcher between 6:00 am and 4:00 pm Mountain Standard Time. Emergency calls outside normal working hours are received by an answering service and returned within one hour.
Facsimile	(602) 313-5476
Mail	Honeywell IS TAC, MS P13 2500 West Union Hills Drive Phoenix, AZ, 85027

Europe

Contact	Honeywell TAC-EMEA
Phone	+32-2-728-2704
Facsimile	+32-2-728-2696
Mail	Honeywell TAC-EMEA Avenue du Bourget, 1 B-1140 Brussels, Belgium

Pacific

Contact	Honeywell Global TAC - Pacific
Phone	1300-300-4822 (toll free within Australia) +61-8-9362-9559 (outside Australia)
Facsimile	+61-8-9362-9169
Mail	Honeywell Global TAC - Pacific 5 Kitchener Way Burswood, WA, 6100, Australia
Email	GTAC@honeywell.com

India

Contact	Honeywell Global TAC - India
Phone	+91-20-2682-2458
Facsimile	+91-20-2687-8369
Mail	TATA Honeywell Ltd. 55 A8 & 9, Hadapsar Industrial Hadapsar, Pune -411 013, India
Email	Global-TAC-India@honeywell.com

Korea

Contact	Honeywell Global TAC - Korea
Phone	+82-2-799-6317
Facsimile	+82-2-792-9015
Mail	Honeywell Korea, 17F, Kikje Center B/D, 191, Hangangro-2Ga Yongsan-gu, Seoul, 140-702, Korea
Email	Global-TAC-Korea@honeywell.com

People's Republic of China

Contact	Honeywell Global TAC - China
Phone	+86-10-8458-3280 ext. 361
Mail	Honeywell Tianjin Limited 17 B/F Eagle Plaza 26 Xiaoyhun Road Chaoyang District Beijing 100016, People's Republic of China
Email	Global-TAC-China@honeywell.com

Singapore

Contact	Honeywell Global TAC - South East Asia
Phone	+65-6580-3500
Facsimile	+65-6580-3501 +65-6445-3033
Mail	Honeywell Private Limited Honeywell Building 17, Changi Business Park Central 1 Singapore 486073
Email	GTAC-SEA@honeywell.com

Taiwan

Contact	Honeywell Global TAC - Taiwan
Phone	+886-7-323-5900
Facsimile	+886-7-323-5895 +886-7-322-6915
Mail	Honeywell Taiwan Ltd. 10F-2/366, Po Ai First Rd. Kaohsiung, Taiwan, ROC
Email	Global-TAC-Taiwan@honeywell.com

Japan

Contact	Honeywell Global TAC - Japan
Phone	+81-3-5440-1303
Facsimile	+81-3-5440-1430
Mail	Honeywell K.K 1-14-6 Shibaura Minato-Ku Tokyo 105-0023 Japan
Email	Global-TAC-JapanJA25@honeywell.com

Elsewhere

Call your nearest Honeywell office.

World Wide Web

Honeywell Solution Support Online:

`http://www.ssol.acs.honeywell.com`

Training classes

Honeywell holds technical training classes on Experion PKS. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see `http://www.automationcollege.com`.

Related documentation

For a complete list of publications and documents for Experion PKS, see the *Experion PKS Overview*.

Contents

Contents

Contents

Contents

Introduction

1

This guide contains networking and security information applicable to Experion PKS.

If you have specific security concerns such as protecting your Experion PKS against viruses or preventing unauthorized access, you might like to start by consulting the checklists in the topic “Security checklists” on page 13.

Alternatively, you can choose from the following list of topics.

For information about ...	Go to ...
Developing a security program	“Developing a security program” on page 21.
A strategy for backups and recovery	“Disaster recovery” on page 31.
The physical security of your system	“Physical and environmental considerations” on page 33.
Measures for keeping security-related software up to date	“Microsoft security updates and service packs” on page 39.
Anti-virus measures	“Virus protection” on page 45.
Network port access and connections through firewalls	“Network security” on page 51.
Working with Windows domains	“Windows domains” on page 63.
Securing your operating system	“Securing access to the Windows operating system” on page 69.
Monitoring and auditing the security of your system	“System monitoring” on page 87.
Security issues specific to Experion PKS	“Experion PKS security features” on page 93.

Related documents

The following documents complement this guide.

Document	Description
Overview	Provides a comprehensive overview of Experion PKS, including basic concepts and terminology.
FTE Overview and Implementation Guide	Gives an overview and provides planning and implementation details of FTE.
Server and Client Planning Guide	Contains high-level planning and design topics for Experion PKS servers and clients, as well as for controllers other than Process Controllers.
Control Hardware Planning Guide	Contains planning and design topics applicable to Process Controllers.
Software Change Notice (SCN)	Contains last-minute information that was not able to be included in the standard documents. It may include important details related to networking and security.

Security checklists

2

This chapter provides a number of checklists to help you think about security issues that should be considered for your site. They also provide alternative ways of navigating through this document, depending on your key concerns.

The checklists cover two broad areas:

- Mitigating against specific security threats
- Protecting your system assets

Mitigating against threats

This topic describes some of the main threats that may exist on a process control network and the steps that can be used to mitigate against them.

Attention

As general principles of good practice it is strongly recommended that you do not allow:

- The use of any unauthorized CDs, DVDs, floppy disks, USB memory sticks, or similar removable media, on any node that is part of, or connected to, your Experion PKS system. This is of critical importance in relation to the nodes in your process control network.
- Port scanning of online systems, as this could lead not only to performance degradation but to system failure.

Infection by viruses and other malicious software agents

This threat encompasses malicious software agents such as viruses, trojans, and worms.

Possible effects

The intrusion of malicious software agents can result in:

- Performance degradation
- Loss of system availability
- The capture, modification, or deletion of data.

Mitigation Steps

Table 1 Mitigating against infection by viruses and other agents

Mitigation steps	For more information, see ...
Ensure that your virus protection and Microsoft security hotfixes are up to date on all nodes in your process control network and the systems connected to it.	“Virus protection” on page 45
Ensure that there are no email clients on any nodes of your process control network.	“Viruses and email” on page 49
Use a firewall and DMZ for the business network to process control network interface.	“Connection to the business network” on page 57

Table 1 Mitigating against infection by viruses and other agents

Mitigation steps	For more information, see ...
Use Honeywell's High Security Network Architecture.	"High Security Network Architecture" on page 53
Lock down the nodes in your system.	"Honeywell High Security Policy" on page 73

Unauthorized external access

This threat includes intrusion into the process control system from the business network and possibly an intranet or the Internet. The motivation for this intrusion could be malicious, for example, to shut down or disable the process control system, or to steal data. One difficulty in protecting against this threat is that the perpetrator potentially has a lot of time to find a way of accessing the system, and can defeat countermeasures one by one.

Possible effects

Unauthorized external access can result in:

- Loss of system availability
- Incorrect execution of controls causing damage to the plant, or theft or contamination of product
- The capture, modification, or deletion of data
- Loss of prestige

Mitigation Steps

Table 2 Mitigating against unauthorized external access

Mitigation steps	For more information, see ...
Use a firewall/DMZ for the business network to process control network interface to restrict access from the business network to process control network.	"Connection to the business network" on page 57
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	"Setting password and account policies" on page 70
Monitor system access.	"System monitoring" on page 87
Use Honeywell's High Security Network Architecture.	"High Security Network Architecture" on page 53
Lock down the nodes in your system.	"Honeywell High Security Policy" on page 73

Unauthorized internal access

This threat encompasses unauthorized access from systems within the process control network. This threat is the most difficult to counter since attackers may well have legitimate access to part of the system and they simply want to exceed their permitted access.

Possible effects

Unauthorized internal access can result in:

- Loss of system availability
- Incorrect execution of controls causing damage to the plant, or theft or contamination of product
- The capture, modification, or deletion of data

Mitigation Steps

Table 3 Mitigating against unauthorized internal access

Mitigation steps	For more information, see ...
Ensure Station security.	“Station security” on page 99
Use physical security for process control network systems.	“Physical and environmental considerations” on page 33
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 73
Use and enforce a strong password policy.	“Setting password and account policies” on page 70
Ensure strong access controls are in place on the file system, directory, and file shares.	“File system and registry protection” on page 79
Monitor system access.	“System monitoring” on page 87

Accidental system change

This threat encompasses inadvertent changes to executables or configuration files.

Possible effects

Accidental system change can result in:

- Loss of system availability
- Loss of data

Mitigation Steps

Table 4 Mitigating against accidental system change

Mitigation steps	For more information, see ...
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	“Setting password and account policies” on page 70
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 73
Ensure strong access controls are in place on the file system, directory, and file shares.	“File system and registry protection” on page 79

Protecting assets

The following tables list steps you can take towards making your system assets more secure.

In this context, the term *asset* is used in the conventional sense to mean something of value to the company. The use of the term asset in this topic therefore needs to be distinguished from the use of the term in the context of the Experion PKS asset model, discussed later in this guide (see “Assets” on page 110).

Experion PKS server

Table 5 Protecting Experion PKS servers

Protection measures	For more information, see ...
Ensure that your virus protection and Microsoft security hotfixes are up to date on all systems.	“Virus protection” on page 45
Set the minimum level of privilege, and enforce a strong password policy, for all accounts.	“Setting password and account policies” on page 70
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 73
Use physical security for process control network systems.	“Physical and environmental considerations” on page 33

Experion PKS Station

Table 6 Protecting Experion PKS Stations

Protection measures	For more information, see ...
Ensure that your virus protection and Microsoft security hotfixes are up to date on all systems.	“Virus protection” on page 45
Ensure Station security.	“Station security” on page 99
Set the minimum level of privilege and enforce a strong password policy for all accounts.	“Setting password and account policies” on page 70
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 73
Use physical security for process control network systems.	“Physical and environmental considerations” on page 33

Domain controller

Table 7 Protecting domain controllers

Protection measures	For more information, see ...
Ensure that your virus protection and Microsoft security hotfixes are up to date on all systems.	“Virus protection” on page 45
Take steps to implement and enforce physical security.	“Physical and environmental considerations” on page 33
Set the minimum level of privilege and enforce a strong password policy for all accounts.	“Setting password and account policies” on page 70

Network components

Network components include routers, switches, and firewalls.

Table 8 Protecting network components

Protection measures	For more information, see ...
Secure all network components with strong passwords.	“Setting password and account policies” on page 70
Take steps to implement and enforce physical security.	“Physical and environmental considerations” on page 33

Developing a security program

3

A security program is a risk-analysis driven, life-cycle approach to securing the process control network. This chapter describes the key components of a security program:

- Forming a security team
- Identifying assets that need to be secured
- Identifying and evaluating threats
- Identifying and evaluating vulnerabilities
- Implementing change management
- Creating and implementing a mitigation plan
- Planning ongoing maintenance

Forming a security team

In forming a team you should:

- Define executive sponsors. It will be easier to ensure the success of security procedures if you have the backing of senior management.
- Establish a cross-functional security core team consisting of representatives from:
  - Process control
  - Business applications
  - IT system administrators

Identifying assets

In this context the term *asset* implies anything of value to the company. The term includes equipment, intellectual property such as historical data and algorithms, and infrastructure such as network bandwidth and computing power.

In identifying assets that are at risk you need to consider:

- People, for example, your employees and the broader community to which they and your enterprise belong.
- Equipment and assets, for example:
  - Control system equipment
  - Plant equipment: network equipment (routers, switches, firewalls) and ancillary items used to build the system
  - Network configuration information (such as routing tables and ACLs)
  - Intangible assets such as bandwidth and speed
  - Computer equipment
  - Information on the computing equipment (databases) and other intellectual property.

Identifying and evaluating threats

You need to consider the potential within your system for unauthorized access to resources or information through the use of a network, and the unauthorized manipulation and alteration of information on a network.

Potential threats to be considered include:

- People, for example, malicious users outside the company, malicious users within the company, and uninformed employees.
- Inanimate threats, for example, natural disasters (such as floods, earthquakes, fire) or malicious code such as a virus or denial of service.

Identifying and evaluating vulnerabilities

Potential vulnerabilities that should be addressed in your security strategy include:

- The absence of security policies and procedures
- Inadequate physical security
- Gateways from the Internet to the corporation
- Gateways between the business LAN and process control network
- The improper management of modems
- Out-of-date virus software
- Out-of-date security patches or inadequate security configuration
- Inadequate or infrequent backups

You might also want to use failure mode analysis to assess the robustness of your network architecture.

Creating a mitigation plan

As part of your plan of defense you need to write policies and procedures to protect your assets from threats. The policies and procedures should cover your networks, your Windows nodes, and any other operating systems.

You should also perform risk assessments on your process control system equipment. A full inventory of your assets will help you to identify threats and vulnerabilities.

You are then in a better position to decide whether you can ignore, mitigate, or transfer the risk.

Implementing change management

A formal change management procedure is vital for ensuring that any modifications to the process control network meet the same security requirements as the components that were included in the original asset evaluation and the associated risk assessment and mitigation plans.

Risk assessment should be performed on any change to the process control network that could affect security, including configuration changes, the addition of network components and installation of software. Changes to policies and procedures might also be required.

Planning ongoing maintenance

Constant vigilance of your security position should involve:

- Regular monitoring of your system
- Regular audits of your network security configuration
- Regular security team meetings whose role it is to stay up to date with the latest threats and with the latest technologies for dealing with security issues.
- Ongoing risk assessments as new devices are placed on the network (see “Implementing change management” on page 27)
- The creation of an Incident Response Team
- Being proactive about security by reviewing additional security resources; for example:
  - Honeywell’s ACS Web site

    `http://www.acs.honeywell.com`

    In particular, go to:

    Support > Online Support > Solutions Support Online
  - Microsoft

    `http://www.microsoft.com/security`
  - US Government Accountability Office

    `http://www.gao.gov/`
  - Process Control Security Requirements Forum (PCSRF)

    `http://www.isd.mel.nist.gov/projects/processcontrol/`
  - National Cyber Security Partnership

    `http://www.cyberpartnership.org/`
  - Cisco

    `http://www.cisco.com`
  - Computer Security Institute

    `http://www.gocsi.com`
  - The National Institute of Standards and Technology document *System Protection Profile - Industrial Control Systems*

    `http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.doc`

- The Instrumentation, Systems, and Automation Society
  Go to: `http://www.isa.org`
  Choose: **Standards > Committees**
  Then choose: ISA-SP99, Manufacturing and Control Systems Security

More detailed information on creating a security program can be found in the ISA document *Integrating Electronic Security into the Manufacturing and Control System Environment*, which includes a detailed life-cycle approach similar to the approach developed for safety-related system in the IEC 61508.

Disaster recovery

4

As part of your security strategy you should define a comprehensive backup and restore policy. In formulating this policy you need to consider:

- How quickly data or the system needs to be restored. This will indicate the need for a redundant system, spare offline computer, or simply good file system backups.
- How frequently critical data and configuration is changing. This will dictate the frequency and completeness of backups.
- The safe onsite and offsite storage of full and incremental backups.
- The safe storage of installation media, licence keys, and configuration information.
- Who will be responsible for backups, and the testing, storing, and restoring of backups.

For detailed information about backup strategies and specific instructions for backing up your Experion PKS system, see the topic “Backups and recovery” in the *Server and Client Administration and Startup Guide*.

Physical and environmental considerations

5

Although the security issues for Experion PKS are generally the same as for any IT server, the physical security of a process control network is particularly important. If the hardware is rendered inoperable, the entire system (and hence the plant or building security) is rendered inoperable.

Physical location

In addressing the security needs of your system and data, it is important to consider environmental factors.

For example, if a site is dusty, you should place the server in a filtered environment. This is particularly important if the dust is likely to be conductive or magnetic, as in the case of sites that process coal or iron.

If vibration is likely to be a problem, you should mount the server on rubber to prevent disk crashes and wiring connection problems.

In addition, you should provide stable temperature and humidity for the server as well as for backup tapes and floppy disks.

A major cause of downtime in the IT world is hardware theft, either of whole computers or of individual components such as disks and memory chips. To prevent this, the computer and monitor should be chained to the furniture, and the case locked and closed.

If computers are readily accessible, and they have a floppy disk or CD drive, you might also consider fitting locks to floppy and CD drives, or (in extreme cases) removing the floppy and CD drives from the computers altogether. These suggestions apply to both the main server and to the control room computers running Station.

Depending on your security needs and risks, you should also consider disabling or physically protecting the power button to prevent unauthorized use.

For maximum security, the server should be placed in a locked area and the key protected.

Protecting against unauthorized booting

External media drives can enable anyone to bypass Windows security and gain access to your system.

If there is easy access to a computer, and it has a floppy disk or CD drive, it can be booted from an alternative operating system. This can be used to circumvent file system security, and could be used to install damaging software, or even to reformat the hard disk.

It is therefore extremely important to prevent the use of all unauthorized removable devices and media such as CDs, floppy disks, and USB memory sticks.

There are several other steps that can be taken to reduce the risk of unauthorized access, including:

- Setting the BIOS to boot only from the C drive
- Setting a BIOS password (check that this does not prevent automatic startup)
- Physically securing the computer (for example, in a locked room or cabinet) or fitting locks to the floppy and CD drives.
- Removing (in extreme cases) the floppy and CD drives from the computer.
- Registry settings may be used to prevent certain drive letters (floppy drive and CD drive) from being visible to Microsoft Windows Explorer. Note, however, that this does not prevent those drives from being accessed via a Command window.

Caution

Incorrect changes to the registry may create problems or cause severe damage to your system. Changes made to the Windows registry happen immediately, and no backup is automatically made.

Before making changes to the registry, you should back up any valued data on your computer. For detailed information about backing up and restoring system data like registries, see the topic “Backups and recovery” in the *Server and Client Administration and Startup Guide*.

Control room access

Providing physical security for the control room is essential to reduce the potency of many threats. Frequently control rooms will have consoles continuously logged onto the primary control server, with speed of response and continual view of the plant considered more important than secure access. The area will also often contain the servers themselves, other critical computer nodes and plant controllers. Limiting those who can enter this area, using smart or magnetic identity cards, biometric readers and so on is essential. In extreme cases, it may be considered necessary to make the control room blast-proof, or to provide a second off-site emergency control room so that control can be maintained if the primary area becomes uninhabitable.

Network and controller access

Many plant controllers are intelligent programmable devices, with the ability to be manipulated through loader software running on a laptop or similar computer connected directly to them. In order to prevent unauthorized tampering, the controllers should be physically protected in locked cabinets, and logically protected with passwords or other authentication techniques. Network cables are also vulnerable to damage or unauthorized connection. For maximum protection, cabling should be duplicated and laid in separate hardened cable runs.

Reliable power

Reliable power is essential, so you should provide an uninterruptible power supply (UPS). If the site has an emergency generator, the UPS battery life may only need to be a few seconds; however, if you rely on external power, the UPS probably needs several hours supply.

Microsoft security updates and service packs

6

An important part of your overall security strategy is to set up a system for ensuring that the operating system software is kept up to date. Such a system should include:

- The application of security updates (or patches) or hotfixes (see “Security updates and hotfixes” on page 40).
- The installation of service packs (see “Service packs” on page 42).
- The setting up of a Security Hotfix Response Team (see “Security Hotfix Response Team” on page 43).
- A secure process for distributing Microsoft hotfixes and virus definition files (see “Distributing Microsoft hotfixes, patches, and virus definition files” on page 44).

Attention

Frequent updates to critical process control system nodes can be error prone, and may, over time, destabilize your system so they should be undertaken judiciously and with care.

Security updates and hotfixes

Microsoft releases a range of security updates (or patches) and hotfixes.

- Security updates are publicly released fixes for a product-specific vulnerability.
- A hotfix is a single, cumulative package that includes one or more files that are used to address a problem in a product. Hotfixes address a specific customer situation and may not be distributed outside the customer organization.

Timely information on security updates and hotfixes can be obtained by subscribing to the Microsoft Security Bulletin Summary at

`http://www.microsoft.com/technet/security/bulletin/notify.mspx`

Attention

Because Windows NT 4.0 Workstation and Server support has expired, Microsoft is not under any obligation to deploy security updates for NT 4.0.

If possible, you should wait until Honeywell has validated (that is, qualified) updates and hotfixes before installing them. It is also recommended that you implement a controlled system for the distribution of all updates and hotfixes (see “Distributing Microsoft hotfixes, patches, and virus definition files” on page 44).

Attention

- If you have a PHD node in your Experion PKS system, you should install security updates and hotfixes as soon as they are available.
- Before installing security updates and hotfixes on the critical nodes in your process control network, you should refer to Honeywell’s Solution Support On-Line site (see “Qualification of Microsoft updates” on page 40 for instructions on navigating to the site). This site provides information on the status of qualified updates and hotfixes for Honeywell Process Solutions (HPS) products (that is, Experion PKS, TPS, and Uniformance). For non-HPS products, you will need to refer to the supplier’s hotfix and patch rules.

Qualification of Microsoft updates

In this context, qualification means that Honeywell sells and supports the product, or has tested a product for use in conjunction with its own products or services. Honeywell qualifies Microsoft updates and hotfixes for operating systems, Internet Explorer, and SQL Server products within a short period of time but generally only qualifies updates denoted as “Critical”.

You may wish to contact your local Honeywell Technical Assistance Center (TAC) for advice in relation to Microsoft security updates and hotfixes, or go to the Honeywell ACS Web site for a list of Microsoft security hotfixes that have been qualified by Honeywell:

1. Go to `http://www.acs.honeywell.com`.
2. Select **Support > Online Support > Solution Support Online**.
3. And then select **Microsoft Security Hotfix Information > Qualified Microsoft Security Hotfixes > EPKS / PlantScape**.

Honeywell's **Microsoft Security Hotfix Information** Web page also provides links to a number of Microsoft sites that have information related to security hotfixes.

In any case, before implementing any updates, it is best to verify them on a non-production computer, or when the plant or building is not active, to ensure that there are no unexpected side effects.

The Microsoft web site `http://www.microsoft.com/technet/security/current.aspx` is a prime source of information on current and past hotfixes.

Service packs

A service pack is a tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Service packs may also contain additional fixes for problems that have been found internally since the release of the product, and a limited number of customer-requested design changes or features.

Qualification of Microsoft service packs

Microsoft performs full integration testing of their service packs against the operating system and their own applications. Honeywell will follow that with system integration testing of the service pack which in most cases will be part of a scheduled and planned release. Because of this, it is recommended that you wait until Honeywell has qualified the service pack prior to your own qualification testing.

You may wish to contact your local Honeywell Technical Assistance Center (TAC) for advice in relation to Microsoft service packs or look up the Honeywell ACS web site:

1 Go to `http://www.acs.honeywell.com`

2 Select **Support > Online Support > Solution Support Online**.

In any case you should verify service packs on a non-production computer, or when the plant or building is not active, to ensure that there are no unexpected side effects.

Security Hotfix Response Team

The responsibilities of a Security Hotfix Response Team (SHRT) might include:

- Monitoring the Microsoft and Honeywell software update sites.
- Monitoring the anti-virus software updates.
- Risk assessment of each security update, anti-virus update and hotfix as it is made available.
- Determining the amount of verification required for any update and how the verification is to be performed. In extreme cases it may be helpful to have an offline system available so that full functionality testing is possible. This would be particularly useful where it is normal practice to install hotfixes as soon as they are announced, rather than waiting for Honeywell qualification.
- Determining when the update is to be installed. There may be times when the SHRT determines that an update is so important that you cannot wait for Honeywell's verification cycle and so you need to verify and install it early on all of your systems.
- Deploying qualified hotfixes on the Experion PKS servers and dedicated (control room) Station clients. Note that the corporate IT policy for updating Windows computers should be sufficient for the rotary Station and engineering computers.
- Periodically run the Microsoft Baseline Security Analyzer to ensure that hotfixes have not been missed. For details, see "Microsoft Baseline Security Analyzer" on page 88.

Distributing Microsoft hotfixes, patches, and virus definition files

It is important to install hotfixes, patches, and updates to virus definition files on all nodes (including non-Experion PKS nodes such as PHD servers) in your Experion PKS system and the systems connected to it.

It is, however, not best practice to distribute Microsoft hotfixes, patches, and updates to virus definition files directly from the business network to nodes on the process control network as this is contrary to the goal of minimizing direct communication between nodes on these networks. Honeywell therefore recommends that a patch manager and an anti-virus server be located in the DMZ (see “The demilitarized zone” on page 58). Both roles can be performed by a single server. Honeywell provides a service to design and configure nodes in a DMZ: contact Honeywell Network Services on 1-800-822-7673 (USA) or +1 602-313-5558 (outside the USA).

Implementing a hotfix, patch, and anti-virus management system that is dedicated to the process control network helps to ensure more controlled and secure updates, which sites can also tailor for the unique needs of their particular process control environment. It also helps address the issues that arise when an anti-virus product that is supported by the process control equipment vendor is not the same as the anti-virus product supported by the corporate IT department.

Attention

Honeywell qualifies Microsoft hotfixes, updates, and patches. It is strongly recommended that hotfixes, updates, and patches are not implemented until this qualification has been carried out (see “Qualification of Microsoft updates” on page 40 and “Qualification of Microsoft service packs” on page 42).

Virus protection

7

Anti-virus measures are an essential element of a comprehensive process control security strategy. It is therefore important to not only install anti-virus software, and to run regular virus checks, but also to keep the anti-virus software and virus signatures up to date.

For general guidance on anti-virus measures:

1. Go to Honeywell's ACS Web site: `http://www.acs.honeywell.com`.
2. Choose **Support > Online Support > Solutions Support Online**.
3. Then choose **Microsoft Security Hotfix Updates > AntiVirus Overview and Recommendations**.

Honeywell support for third-party anti-virus software

Honeywell has tested (and supports) both McAfee VirusScan and Norton AntiVirus for use in conjunction with Experion PKS.

Honeywell Services has an offering to qualify other third party packages.

Anti-virus best practices

The following anti-virus measures are recommended as best practice.

Best practice measures	More detail available
Install anti-virus software on each node connected to the process control network.	“Installing anti-virus software” on page 46.
Use active virus scanning (for example, McAfee VShield).	“Virus scanning recommendations” on page 47.
Ensure that signature files are updated on a regular basis. Where it is not practical to do this daily, it is worth monitoring those Web sites which publish information about new virus attacks so that the system can be isolated if a specific threat appears. Note that a virus which is deemed low risk for corporate systems may pose a high risk to a control system if it causes a denial of service.	“Anti-virus signature file deployment” on page 48.
Changes in anti-virus software revisions should be tested offline before being deployed to process control nodes.	

Installing anti-virus software

Install anti-virus software on every Windows node in the process control environment. It is recommended that you set up template servers for the controlled distribution of anti-virus signature files to the PCN as outlined in “Distributing Microsoft hotfixes, patches, and virus definition files” on page 44.

- Experion PKS
  - Experion PKS Stations (Flex Stations, Console Stations and Console Extension Stations) / Experion PKS Station TPS
  - Experion PKS Server / Experion PKS Server TPS
  - Application Control Environment (ACE) node
- TPS
  - GUS nodes
  - Application Processing Platform (APP) nodes
- Other
  - Process History Database (PHD) servers

- Advanced control nodes
- Honeywell and third party application nodes
- Subsystem interface nodes (for example, tank gauging)

Virus scanning recommendations

Virus scanning and system performance

Attention

Do not automatically schedule full system scans on any Experion PKS node as this can result in severe degradation of performance, and could therefore:

- Impact operators ability to respond to a situation, or
- Result in execution cycle overruns on an Application Control Node.

The Experion PKS system requires a certain amount of system resources, including CPU, memory, disk access, in order to perform reliably. Shortages of these resources may lead to decreased system performance.

To ensure continued high reliability service from your Experion PKS system, it is suggested that any third party applications, including anti-viral software, only be run when system resource conditions on the node are adequate to meet the needs of the system. When configuring anti-viral software you may need to consider limiting the system resources that are used during scanning. If you encounter system difficulties related to low system resources, it is suggested that you tune your system appropriately by limiting the system resources third party applications use or restrict the use of those applications.

The tuning of anti-viral software should consider balancing performance against risk. On some systems, the high performance of the server node is balanced against the performance of the scanning engine. Some anti-virus scanners allow you to set maximum CPU usage. For the majority of customers, the default installation of anti-viral software will fully meet the demands of those customers; however, for customers whose systems have extremely high CPU and I/O demands, the default installation of anti-viral software may impose system limitations. Honeywell has tested anti-viral software successfully on extremely large systems by limiting the CPU utilization of anti-viral software to as low as 10%. Please refer to your anti-viral software documentation for specific procedures on how to limit CPU utilization.

For those customers who are experiencing performance related issues because of resource starvation, there are further steps you can take to limit the amount of resources anti-viral software consumes. Anti-viral web-sites have up-to-date information regarding specific configuration steps a customer can choose to

lessen the performance drain that anti-viral software imposes. To find the proper balance between server performance and virus protection you may need to make configuration choices such as disabling scanning on reading of files and changing the default process-based scanning to per-process scanning.

Excluding directories from scanning

Experion PKS creates many files during normal operations and the system resource overhead of scanning each of these files for viruses is extremely high. Honeywell tests anti-viral software with the following directories excluded from scanning:

```
\Documents and Settings\All Users\Application Data\Honeywell\
\Program Files\Honeywell\Experion PKS\server\data
\Program Files\Honeywell\Experion PKS\Engineering Tools\system\er
```

Further virus scanning recommendations

Ensure that the boot sectors of all floppy disks are scanned.

When an infection is detected, infected files should be moved to a quarantine directory and a message provided to the user that an infected file was found. The user should be allowed to clean up the infection.

It is also important to regularly review virus scan reports.

Anti-virus signature file deployment

The most common attacks on a control system are non-directed virus and worm attacks. New viruses and new strains of existing viruses are being created all the time. It is therefore essential to update anti-virus signature files frequently by:

- Subscribing to the updates of your anti-virus software vendor(s)
- Leveraging enterprise anti-virus policies and practices

It is also important to test anti-virus signature files offline before deploying them to ensure that the signature file does not break the anti-virus software or cause problems on the computer. For example, you could first test the signature files on:

- A staged test system
- One or two nodes

When implementing the automatic deployment of signature files:

- Stagger automatic deployment to eliminate the potential for common cause failure. For example: deploy to three or four nodes per hour.
- Follow the recommendations of your anti-virus software vendor for distribution server/services.
- Stage the distribution on a test system.

Attention

In line with the best practice of minimizing communication between the business network and the process control network, it is recommended that updates to anti-virus signature files be distributed from a server located in a DMZ as outlined in “Distributing Microsoft hotfixes, patches, and virus definition files” on page 44.

Viruses and email

Many viruses and similar malware propagate via email. Not only do these viruses cause damage to the computer, often rendering them inoperable, they also cause significant network traffic by mass-mailing to other addresses. Because of the nature of Ethernet LANs using TCP/IP, a small increase in traffic can cause an exponential increase in delays and errors, which may prevent the timely delivery of controls and alarms.

Attention

It is therefore strongly recommended that email clients not be installed on any node connected to the process control network.

Network security

8

This chapter describes key network security considerations. It covers:

- A list of sources of information for network planning issues
- Honeywell's High Security Network Architecture
- The connection between the process control network and the business network, including information about firewall configuration for eServer, Station, DSA-connected servers, and engineering Stations
- Remote access considerations
- The use of dual-homed computers

Network planning

General network planning issues for an Experion PKS process control network are described in the following documents:

- *Experion PKS Overview* describes the basic concepts and terminology as well as the capabilities of an Experion PKS process control network.
- *Control Hardware Planning Guide* provides detailed planning information for all aspects of Experion PKS process control network planning. It also describes ControlNet, Ethernet, and FTE networks as well as PLC connections.
- *Fault Tolerant Ethernet Overview and Implementation Guide* includes information about configuring a system that conforms to Honeywell's High Security Network architecture. It contains information about network equipment specifications, configuration, IP addressing, and network topologies.
- *Experion PKS Server and Client Planning Guide* contains planning information for Experion PKS, including information about distributed systems architecture (DSA), server redundancy, and data exchange.

High Security Network Architecture

Honeywell's High Security Network Architecture represents best practice for Fault Tolerant Ethernet based systems under Experion PKS Release 200 and later. It comprises a specific set of qualified network components, including switches and routers, and template configuration files to assist with the setup of switches and routers.

A summary of the key security-related features of Honeywell's High Security Network Architecture follows.

To implement Honeywell's High Security Network Architecture, follow the instructions contained in the sections "Planning a Honeywell FTE Network" and "Use of IP addresses in an FTE Network" in the *Fault Tolerant Ethernet Overview and Implementation Guide*.

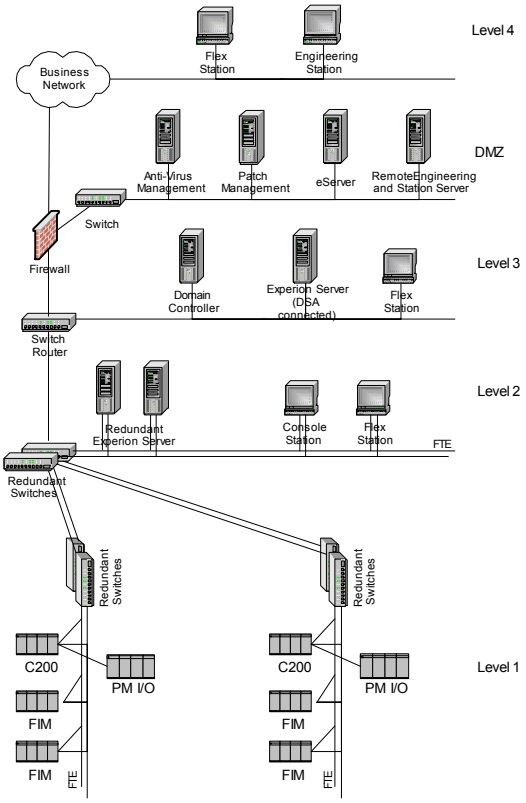
Supported topologies

High Security Network Architecture has the following levels. At each level the node membership, IP subnetting, and switch configuration are different.

Table 9 Summary of levels

Level	Function of this level
Level 1	Real time control (controllers and input/output)
Level 2	Supervisory control and the operator interface
Level 3	Advanced control and advanced applications (non-critical control applications)
Demilitarized Zone (DMZ)	Nodes that require access to process control and business networks
Level 4	Business network applications such as Manufacturing Execution Systems (MES) and Manufacturing Resource Planning (MRP) solutions.

Figure 1 The levels in an Experion PKS system



About Level 1

At Level 1 controllers (C200) and Fieldbus Interface Modules (FIM) connect to redundant Level 1 switches.

The Level 1 network is the most critical network in the system as a failure or loss of service on this network can result in loss of control. The network should be configured so that all Level 1 devices that control a given area of the plant are connected together in the same secured network.

Traffic on the Level 1 network should be limited to communication with other Level 1 nodes and with the Experion PKS servers and Stations at Level 2. Network traffic on the Level 1 network should be prioritized such that CDA traffic is highest priority. Broadcast and multicast traffic should be prioritized as the lowest priority, and protection needs to be provided to reduce the probability of broadcast and multicast storms.

About Level 2

At Level 2 Experion PKS servers, Stations, and other nodes connect to Level 2 switches. There are also uplink connections from the Level 1 switches.

The Level 2 network must be a highly reliable and highly available network to maintain constant view to the process. A failure of the Level 2 network can result in a loss of view of the process.

IP subnetting of nodes, priority queuing, and access lists in the switches are used to control network traffic between Level 2 and Level 1 as follows:

- Internal Level 1 traffic has a higher priority than traffic between Level 2 and Level 1 nodes. Peer-to-peer controller communication will not be disrupted by other network traffic.
- Only Level 2 nodes that need to communicate with Level 1 nodes are permitted to do so. No communication between Level 3 (and higher) nodes and Level 1 nodes is permitted.
- Bandwidth limits are configured for Level 2 nodes to protect against broadcast, multicast, and unicast storms.

  If these thresholds are set for low tolerance of high traffic bursts, then problems may be encountered with traffic between redundant servers being interpreted as an attack.

About Level 3

At Level 3 domain controllers, plant-wide applications, DSA-connected Experion PKS servers, Stations, and other nodes are connected to a Level 3 router, which also has switch functionality. There are also uplink connections from the Level 2 switches and, if required, a connection to a firewall that serves as the gateway to the business network.

A failure of the Level 3 network can result in a loss of advanced control.

IP subnets, access lists, filtering, and virtual LANs are used to control network communication as follows:

- Access from Level 3 to Level 2 nodes is only enabled if it is required.
- In addition, the type of communication is limited; for example, if authentication of Level 2 nodes by the domain controller at Level 3 is the only communication required, traffic is limited to this type.

If the nodes at Level 2 are part of a Microsoft Windows domain, these nodes will have to communicate with the domain controller which, as a best practice, should be part of the Level 3 network.

About the Demilitarized Zone (DMZ)

A demilitarized zone (DMZ) serves as a buffer zone between the PCN and the business network. It is a separate network segment connected directly to the firewall. In the topology diagram "The levels in an Experion PKS system" on page 54 the DMZ is located between Levels 3 and 4.

Servers placed in the DMZ can be accessed by nodes at Level 4, permitting the supply of data but preventing nodes at Level 4 from having direct access to any systems on the levels below. For more information, see "The demilitarized zone" on page 58).

About Level 4

Level 4 is the business network (see "Connection to the business network" on page 57). It is generally administered by the corporate IT department and is outside the scope of these guidelines.

Other topologies

Topologies other than that shown in diagram "The levels in an Experion PKS system" on page 54 are supported but are not considered best practice.

For small scale networks it is acceptable to combine the functionality of Level 1 and Level 2 switches. It is also possible to have a Console Station connected directly to the Level 1 switches where the geography of the plant dictates this.

Connection to the business network

The best practice is to completely separate the process control network from Level 4, the business network, as shown in the diagram "The levels in an Experion PKS system" on page 54.

The nature of network traffic on these two networks is different: Internet access, FTP, email, and remote access will typically be permitted on the business network but not on the process control network.

Rigorous change control procedures for network equipment, configuration, and software changes may not be in place on the business network.

Process control network traffic should not go on the business network as it could be intercepted. Security and performance problems on the business network should not be able to affect the process control network.

However, practical considerations often mean that a connection is required between the process control and business networks. This connection is a significant security risk and careful consideration should be given to the design. In this case it is strongly recommended that only a single connection is allowed and that the connection is through a firewall and a DMZ.

Firewall configuration

The firewall should use a restrictive security policy, that is, all access should be denied unless explicitly permitted.

MAC or IP address source and destination filtering is used to permit only specific nodes on the business network to communicate with specific nodes on the DMZ, and, if necessary, the PCN. MAC address filtering is preferred as IP address filtering can be vulnerable to spoofing. For nodes that require access permitted traffic must be limited to server-to server traffic only; for example, between Experion PKS servers or a Process History Database (PHD) server.

TCP port filtering should be used to stop denial-of-service attacks to well-known ports.

Honeywell provides a service to design and configure firewalls: contact Honeywell Network Services on 1-800-822-7673 (USA) or +1 602-313-5558 (outside the USA).

The demilitarized zone

A demilitarized zone (DMZ) is a separate network segment that connects directly to the firewall (as shown in Figure 1 on page 54). Servers containing data from the process control system that needs to be accessed from the business network are put on this network segment. Best practice is that only these systems be accessed from the business network.

For detailed information on firewall configuration, contact Honeywell Network Services.

With any external connections the minimum access should be permitted through the firewall. Only identified ports required for specific communication should be opened. The following sections describe the access required for specific node types.

eServer

An eServer provides read-only access to Experion PKS graphics from a web client. Best practice is to locate the eServer in the DMZ as shown in "The levels in an Experion PKS system" on page 54.

The communication between this server in the DMZ and other Experion PKS servers on the process control network uses DSA. The firewall needs to be configured to allow full IP to IP access between these servers.

There are two types of eServer: standard and premium access. Premium access provides a more functional graphic on the Web client.

With standard access the connection between the eServer in the DMZ and the client on the business network uses HTTP. Port 80 must be opened between these nodes in the firewall.

Premium access uses the Honeywell display protocol in addition to HTTP. Ports 80 and 50000 need to be opened in the firewall for access between the eServer in the DMZ and the web client.

Flex Station

If a Flex Station on the business network needs to connect to an Experion PKS server on the process control network, best practice is to use a DSA-connected Experion PKS server in the DMZ as shown in the diagram "The levels in an Experion PKS system" on page 54. The communication between this server in the DMZ and other Experion PKS servers on the PCN uses DSA. The firewall needs to be configured to allow full IP to IP access between these servers.

Communication between the Station and the Experion PKS server uses the Experion PKS display protocol in addition to HTTP. Port 50000 needs to be opened in the firewall for access from Station to the Experion PKS server.

Where display files are to be shared amongst multiple Level 4 Stations, a file server should be placed in the DMZ. The file share should give individual operator (or Experion PKS Windows group) accounts “read access” to the directory containing the display files. The file share should also give the Level 3 `mngr` account “write access” so that changed displays can be distributed using the Experion PKS file replication service.

If Station’s point browsing functionality is to be used, then TCP port 2910 must also be opened

DSA-connected Experion PKS servers

Where Experion PKS servers need to communicate with another Experion PKS server through the firewall using DSA, IP to IP access between these servers must be enabled in the firewall.

By default DSA communications will use random UDP ports allocated by Windows 2000. Constraints may, however, be applied using registry settings. See the Microsoft technical article *Using Distributed COM with Firewalls*.

In addition, multicast messages on UDP port 2911 must be able to pass between all the DSA nodes.

Engineering Station on the business network

There may be a requirement for an engineering Station on the business network to configure Experion PKS servers on the process control network. The best practice is to use a Microsoft Terminal Services client on the business network, connected to a server in the DMZ (see “About the Demilitarized Zone (DMZ)” on page 56) that is running Configuration Studio.

Configuration Studio is an integrated tool used to configure your Experion PKS system, which can be accessed remotely from an Experion PKS Remote Engineering and Station Server. For details see “Configuring Remote Engineering and Station Server” in the *Server and Client Configuration Guide*.

The benefits of this arrangement are:

- Using Microsoft Terminal Services avoids exposing file shares to Level 4.
- Using a dedicated Remote Engineering and Station Server simplifies configuration, and removes the need to run Microsoft Terminal Services on every Experion PKS server. This is to be avoided since Terminal Services consumes a significant portion of the fixed size operating system resource known as “session space.” If this resource is exhausted, as it will be in a large system with numerous Stations and scan channels, then Experion PKS will not start correctly, resulting in partial loss of view.

Microsoft Terminal Services requires TCP port 3389 to be opened From the Level 4 client to the DMZ. Security requirements for Microsoft Terminal Services are discussed in “Securing Windows Terminal Services” on page 82.

Configuration Studio requires that its file share be accessible to Level 2/3 and that it can access TCP port 2910 on all Level 2/3 Experion PKS servers. Furthermore, multicast messages on UDP port 2909 must be able to pass between the Configuration Studio and all Experion PKS servers.

Securing network equipment

The configuration of network equipment such as switches, routers, and firewalls is a critical part of the security for a process control network. Each piece of this equipment should have a unique name and be secured by a strong password.

During normal operation, do not enable HTTP or Telnet on devices that support these features. However, if substantial re-configuration is needed, they may be enabled for the duration of the maintenance.

Remote access

Modems with a dial-up capability provide a means of bypassing boundary security when accessing the process control network. Best practice is to not allow modem with a dial-up capability to connect to any node on the process control network. If remote access via dial-in modems is required, RAS should be used and configured as described in “Securing RAS” on page 82.

NetMeeting, Carbon Copy, and similar access tools

Remote access tools such as NetMeeting, Carbon Copy, and so on should be used with care. By default they should be disabled. When remote access is permitted, its use should be closely monitored, and its configuration set for maximum protection. For example, alarm summary icons can appear in black and white (or be invisible) when using NetMeeting server.

Dual-homed computers

Best practice is not to allow any system to have a network connection to both the process control and business networks. All connections between the process control network and the business network should be through the firewall.

Windows domains

9

In planning your system, you also need to consider how the Windows-based nodes in the process control network will fit into the IT infrastructure, and how users will be given access to both the process control network and the business network. This is achieved through the use of Windows domains and workgroups as discussed in the following sections.

About domains

A *domain* is a collection of computers that share a common domain database and security policy. A domain is managed by a *domain controller*, the server that authenticates domain logons and that maintains the security policy and the master database for a domain. Each domain, and each computer within that domain, has a unique name. A *Domain Name Server* (DNS) is used for the transparent translation of computer names to IP addresses when connections are made.

Domain environments

The operating system for your domain controllers can be either Windows NT 4.0, Windows 2000 Server or Windows Server 2003. The differences are described in this section.

For domain controllers using Windows NT 4.0, authentication makes use of the NTLM protocol. This is the most typical configuration for larger existing Experion PKS sites.

In a Windows 2000 or Windows 2003 domain the account information is held within the Active Directory infrastructure (AD) and security information is transported by Kerberos, a more secure protocol than NTLM. (For more about NTLM, see “Use NTLM Version 2” on page 85.)

Windows domains also use Organization Units (OU). An OU is a group of objects (for example, users) to which common Group Policy can be applied. It is the smallest unit to which administration rights can be granted. An OU enables an administrator to manage operator accounts independently of the overall domain administration. OUs also allow the application of Group Policy to users and computers within the OU. This is useful for controlling dedicated operator computers so that they all have common security settings, as well as a common appearance and execution environment.

You can use the High Security Policy to implement a secure environment. For information on High Security Policy see “Honeywell High Security Policy” on page 73.

For more information

For more information on OUs and Group Policy see:

- Microsoft Windows 2000 Server Resource Kit (see the topic “Deployment Planning Guide: AD Infrastructure”
- Microsoft Windows 2000 Server Resource Kit (see the topic “Distributed Systems: Desktop Configuration Management”)
- Microsoft Windows 2003 Deployment Kit (see the topic “Designing and Deploying Directory and Security Services”).

Windows domains: forests, trees, and DNS

Domains in Windows 2000 Server and Windows Server 2003 are significantly more flexible and more complex than in Windows NT 4.0. Domain concepts like forests, trees, and dynamic DNS allow users to closely integrate Windows 2000 or Windows 2003 domains in IT and process control.

It is important to understand and be familiar with these concepts before installing a new Windows 2000 or Windows 2003 domain, or upgrading existing Windows NT 4.0 domains as it is not easy to modify these constructs after a domain has been established. If you establish a domain and then subsequently decide on a different architecture, a significant amount of manual work may be required to migrate to the new architecture. Honeywell recommends that the process control and IT departments liaise closely to determine the best method of integrating the business IT infrastructure with the process control domain architecture.

Domain membership

Active Directory's scalability allows the largest of organizations to utilize a single domain implementation. At this time, however, Honeywell recommends that customers maintain a separate Windows domain for process control network systems in order to accommodate process control requirements.

A separate domain for the process control network has the following advantages:

- Increased security and reliability
- Centralized and independent management of security
- The ability to customize security policies for the process control network
- Changes to the business domain do not affect the process control network
- Interaction with the business domain can be enabled via the required trust relationship

Workgroup limitations

A workgroup, or peer-to-peer network, is a low-cost option commonly used for small business networks. In this model, computers directly communicate with each other and do not require a domain controller to manage network resources. In general, a peer-to-peer network is most appropriate for networks with a small number of computers (say, less than five), all located in the same general area. The computers in a workgroup are considered peers because they are all equal and share resources among each other without requiring a server. Users determine which data on their computer will be shared with the network. Sharing common resources allows users to print from a single printer, to access information in shared folders, and to work on a single file without transferring it to a floppy disk.

The main disadvantages of workgroups are:

- The requirement to manually configure user accounts on all participating nodes
- The low security protocol used for authentication between nodes

Inter-domain trusts

Inter-domain trusts are used to allow users on one domain to access resources on a different domain. Windows NT domains use explicit trusts; Windows 2000 Server and Windows Server 2003 have trust relationships called transitive trusts. By default, all domains within a Windows 2000 domain have two-way trusts enabled. This dramatically simplifies trust relationship management, but may provide more access than is desirable.

Limiting inter-domain trust

It is important to limit inter-domain trust, that is, not to trust other domain users to log on unless absolutely necessary. Best practice is not to have any trusts between the process control network and business network domains. If trusts are necessary then only have the trusts that are required. Use a one-way trust if possible. Note that this does not prevent users from the business domain making Station connections if they provide credentials (user name and password) that are valid on the Experion PKS server in the process control network domain.

If Stations do reside on the same domain as the Experion PKS server then single signon for operators is possible; that is, Station will be able to automatically connect to Experion PKS using the same credentials as those used when the operator logged onto the Station computer. For more information, see “Single signon” on page 105.

Users, groups, and organizational units

The following Microsoft terms are important when understanding security concepts and configuration. Good definitions can be found in the Glossary of the Windows 2000 Resource Kit:

`http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp`

- access control list (ACL)
- access mask
- access token
- global group
- group
- group memberships
- Group Policy
- Group Policy object (GPO)
- local group
- organizational units (OU)
- permission
- privilege
- universal group
- user account
- user rights

Securing access to the Windows operating system

10

Access is gained to the Windows operating system by logging onto the system using a user account name and password. This is true for both local and remote terminal services access. Because user accounts may be well known or easily guessed within an organization, the password becomes the prime vehicle for authentication. A password policy is therefore an important security measure.

Setting password and account policies

The most popular technique for breaking into a system is to guess user names and passwords. Consequently, it is essential that passwords are difficult to guess and that they are changed often.

You can apply system-wide control of passwords by means of Group Policy. Alternatively, you can apply individual control to each account. The following settings are suggested.

Attention

- Care needs to be taken with the account lockout setting described below as the use of this option can lead to a denial of service for the lockout duration; that is, a valid user will not be able to log on for up to the lockout duration after a number of failed logon attempts.
- It is essential that the password for the Administrator account be changed from the default set at installation.

Parameter	Setting	Comment
Maximum password age	45 to 90 days[i]	Forces the choice of a new password after this time.
Minimum password age	1 to 5 days	Prevents too rapid a cycling of passwords.
Minimum password length	8 characters	Improves encryption and makes guessing harder.
Password uniqueness	8 to 13 old passwords	Prevents reuse of the same password too quickly.
Account lockout	5 attempts	Prevents continual password guessing by disabling account
Lockout duration	4 hours	As above. (Note that the administrator may re-enable the account.)

i More frequent aging of the Administrator account is recommended.

User accounts and passwords: best practices

As a general rule you should:

- Review user accounts on a regular basis.
- Disable or delete all unused accounts

Other best practices for user account and password policies are described below.

Strong passwords

Enforce strong passwords. Weak passwords that are easy to guess provide an opportunity for unauthorized access.

Best practice recommends the use of a pass phrase, for example, “the cow jumped over the moon” rather than a password. The extra characters dramatically increase the difficulty for a hacker attempting to crack the password; it is also much easier to remember than a random collection of letters, numbers, and other characters. This is an alternative way of increasing password complexity.

Experion PKS operator accounts

Experion PKS operator accounts should be set up as follows:

- Enable them to log in only to operator Stations.
- Do not use a shared operator account if individual accountability is required.
- Consider disabling the Windows account lockout feature, which temporarily disables a user account if too many failed logon attempts are made. Lockout is recommended to prevent repeated password cracking attempts, but may lead to denial of service when an authorized user is unable to log on.

  The configuration of the account lockout feature depends on the type of account and the type of domain.

  For more information about the account lockout feature, see the Microsoft white paper “Account Lockout Best Practices - White Paper” (Account Lockout Best Practices.doc) available from:

  `http://www.microsoft.com/downloads/details.aspx?familyid=8c8e0d90-a13b-4977-a4fc-3e2b67e3748e&displaylang=en`
- Use Signon Manager to modify user credentials without loss of view.

Non-operator interactive user accounts

Accounts for engineers and others who need access to server nodes for maintenance activities should be set up as follows:

- Enable them to log in to all process control nodes
- Ensure that they use a secure password: that is, one consisting of at least 8 characters including one numeric.

New accounts

To prevent the use of default passwords, new accounts should have the “User must change” password option set until their first logon.

Where Experion PKS operator-based security is configured, similar care must be taken in choosing passwords. More information about operator based security can be found in the topic “System Administration” in the chapter “Administering users” of the *Server and Client Administration and Startup Guide*.

Administrator accounts

The Administrator account cannot be locked out and is therefore vulnerable to continual attacks with random passwords. A suggested practice is to use Group Policy to modify the user name.

Attention

Renaming the local Administrator account does not provide complete protection from attack as there are tools that attempt to break into the server using the security identifier (SID) of the Administrator account. The SID of the local Administrator account cannot be changed.

Guest accounts

All guest accounts should be disabled.

Service and server accounts

Windows 2000 and COM servers should run under an account with the lowest possible set of privileges. The account should not have the “Logon Interactively permitted” permission set.

The following classes of accounts are suggested in order of preference:

- “Local Service” account (valid on Windows XP and Windows 2003 only)
- Local accounts with minimum rights. Most Experion PKS services run under the local account `mngr`.
- Domain accounts with minimum rights
- “Network Service” account (valid on Windows XP and Windows 2003 only)
- Local or domain user belonging to the Local Administrators group
- “Local System”

Running services under “Local System” should be avoided if at all possible as compromised processes running under this account have rights to “act as part of the operating system” and can do anything they wish on the computer.

Honeywell High Security Policy

The Honeywell High Security Policy leverages the Microsoft Windows Group Policy security model to enable you to control how programs, network resources, and the operating system behave for users and computers in your organization. The policy is in the form of a template which specifies attributes for computers and user accounts.

Attention

- You can use the High Security Policy in a domain or a workgroup environment but as you can only implement Windows Group Policy in a domain environment, you cannot install all the components of High Security Policy in a workgroup environment. High Security Policy is therefore best implemented in a domain environment.
- Implementing the High Security Policy in a domain environment allows you to implement security settings at the group level. The security settings then apply to every user in the group regardless of the computer they are logged on to.
- Implementing the High Security Policy in a workgroup environment applies the settings to every user who logs on to the computer regardless of which local groups they belong to. If you are using a workgroup environment, you need to ensure that the Administrator account can still perform administrative functions.

The following table lists the various components associated with High Security Policy and where they are installed.

Component	Installed
Group Policy Objects (GPOs)	A GPO for each user type is created on the domain controller.
Global groups	A global group for each user type is created on the domain controller. These groups are used as filters on the GPOs.
Global accounts	User accounts created on the domain controller
Local groups and users	A local group for each user type is created on each computer when you install the Experion PKS workstation security package.
Local computer policy settings	Created on each computer when you install the Experion PKS workstation security package.
LinkDomainGroups.vbs	A script to link global groups with local groups for computers participating in a domain.
Local user policy template	A local policy for computers not participating in a domain.
Lockdownlocalusers.bat	A script to enable the local policy on computers not participating in a domain.

You should consider re-running High Security Policy if significant changes are made to your system. This will ensure that those changes do not undo or adversely affect the security settings created by High Security Policy.

User security configuration under High Security Policy

The High Security Policy provides an appropriate security configuration for each user type: operator, supervisor, engineer, and so on.

The High Security Policy is based on the Windows security model, but has been optimized for use with Experion PKS and related products with the addition of specialized security templates, accounts, and groups.

For more detailed information about implementing and configuring the Honeywell High Security Policy, see the topic “Using High Security Policy” in the chapter “Configuring security and access” of the *Server and Client Configuration Guide*.

System services

System services are background processes started by the system at boot time to provide functionality independently of any logged on user. While Experion PKS itself runs as a set of these services, many of the system default services are not needed by Experion PKS. They do, however, provide avenues for malicious network attack and should be disabled. This can be performed through the Services tool: choose **Control Panel > Services**.

The following table lists required services on Windows 2000. Depending on your Experion PKS licence options, all other services should be disabled.

Display Name / Core System	Service	Required?	Dependent on?
Computer Browser	browser	Y	lanmanserver, lanmanworkstation
Logical Disk Manager	dmserver	Y	
DNS Client	dnscache	Y	
Event Log	eventlog	Y	
COM and Event System	eventsystem	Y	rpcss
IIS Admin Service[i]	iisadmin	Optional[ii, iii]	rpcss, protectedstorage
Server	lanmanserver	Y	
Workstation	lanmanworkstation	Y	
TCP/IP NetBIOS Helper Service	lmhosts	Y	
MSSQLSERVER	MSSQLSERVER	Y[ii]	
Network Connections	netman	Y	rpcss
Remote Procedure Call (RPC)	rpcss	Y	
Plug and Play	plugplay	Y	rpcss
Protected Storage	protectedstorage	Y	rpcss
Print Spooler	spooler	Y	rpcss
Security Accounts Manager	samss	Y	
System Event Notification	sens	Y	EventSystem
SQLSERVERAGENT	SQLSERVERAGENT	Y[ii]	MSSQLSERVER
Windows Time	w32time	Y	rpcss
World Wide Web Publishing	w3svc	Optional[ii, iii]	IIS Admin
simple mail service (optional for pager)	smtpsvc	Optional[iv]	

Display Name / Core System	Service	Required?	Dependent on?
Windows Management Instrumentation (needed by FTE)	winmgmt	Optional[v]	rpcss
Windows Management Instrumentation Driver Extensions	wmi	Optional[v]	

i After installing Internet Information Services (IIS), ensure that the IIS Locktown Tool is run. The procedures are documented in the *Experion PKS Software Installation and Upgrade Guide.*

ii Not required for client nodes.

iii Required for Event Archiving/Email notification for Alarm Pager.

iv Pager may be configured to use a mail server. This could be SMTP, but other mail servers are possible.

v Windows Management Instrumentation is needed if Fault Tolerant Ethernet (FTE) is in use.

The following table lists services that run on an Experion PKS server. Depending on your Experion PKS licence options, other services may be disabled.

Display Name / Core System	Required?
Experion PKS BOOTP Server	Y
Experion PKS Checkpoint Service	Y
Experion PKS Configuration Studio Information Service	Y
Experion PKS Control Data Access Server	Y
Experion PKS DTLR Server	Y
Experion PKS EMDB Server	Y
Experion PKS ER Server	Y
Experion PKS GCL Name Server	Y
Experion PKS HART Multiplexer	Y
Experion PKS Server Daemon	Y
Experion PKS Server Database	Y
Experion PKS Server Desktop	Y
Experion PKS Server Logger	Y
Experion PKS Server Operator Management	Y
Experion PKS Server Replication	Y
Experion PKS Server System	Y
Experion PKS System Repository	Y
sm-Component Admin Service (cas.exe)	Y
sm-Fte Provider (HeartBeatProvider) (fteprovider.exe)	Y

Display Name / Core System	Required?
sm-Name Service Provider	Y
sm-Remote Configuration Service	Y
sm-System Event Provider (sysevtprov.exe)	Y
IKB	Experion PKS optional[i]
Signon Manager	Experion PKS optional[i]
GUS TimeSyncClerk Service	Installed for ESVT[ii]
TDC Emulators Service	Installed for ESVT[ii]

i If installed, should not be disabled.

ii Only required on an Experion PKS TPS server (ESVT) accessing TPS data and alarms.

The following table lists services that run on an Experion PKS Console Station: other services may be disabled.

Display Name / Core System	Required?
Experion PKS Console Station Daemon	Y
Experion PKS Console Station Database	Y
Experion PKS Console Station Desktop	Y
Experion PKS Console Station Logger	Y
Experion PKS Console Station Operator Management	Y
Experion PKS Console Station Replication	Y
Experion PKS Console Station System	Y
Experion PKS Control Data Access Server	Y
Experion PKS GCL Name Server	Y
Experion PKS System Repository	Y
sm-Component Admin Service (cas.exe)	Y
sm-Fte Provider (HeartBeatProvider) (fteprovider.exe)	Y
sm-Name Service Provider	Y
sm-Remote Configuration Service	Y
sm-System Event Provider (sysevtprov.exe)	Y
IKB	Experion PKS optional[i]
Signon Manager	Experion PKS optional[i]

Display Name / Core System	Required?
GUS TimeSyncClerk Service	Installed for EST[ii]
TDC Emulators Service	Installed for EST[ii]

i If installed, should not be disabled.

ii Only required on an Experion PKS TPS Station (EST) accessing TPS data and alarms.

File system and registry protection

Windows protects objects, including files, directories and registry keys, with Access Control Lists (ACLs). An ACL is a list of user accounts and groups, each entry specifying a set of allowed, or disallowed actions. In the case of a file, actions include open, read, write, modify permissions, and so on. When applied to a directory, the permissions are, by default, inherited by all subordinate files and directories. The inheritance can be broken if required.

When installed, Windows applies default ACLs to its system directories and registry trees to prevent malicious or accidental damage. Similarly, the Experion PKS installation will apply ACLs to its directories and registry tree. New directories, files, or registry keys will inherit ACLs from their parent node.

If the inheritance is broken, or a new directory is created under the root, there will be no ACLs and hence no protection. It is then up to the site to apply appropriate protection. ACLs are discretionary in that they need not exist for an object, but once they do exist, all access to the object will be subject to the access control specified.

Managing file system ACLs

To manage file system ACLs:

1. In Windows Explorer, select the file or directory.
2. Right-click and select **Properties > Security**.

   This will show a list of users and groups for which access is specified.
3. Selecting a specific user will show their access permissions. You can change these if necessary.

As installed, the file system ACLs will provide good security, with access to the `\program files\Honeywell\Experion PKS` subtree being set up as follows:

- Users are given “read only” permission
- Power Users are given “read/write” access
- Honeywell Administrators are given full access.

Attention

A site may wish to tighten these permissions by applying more specific ACLs to files and directories, but should do so under Honeywell’s guidance. Incorrect permissions may prevent Experion PKS from operating correctly.

Managing registry ACLs

Caution

Incorrect changes to the registry may create problems or cause severe damage to your system. Changes made to the Windows registry happen immediately, and no backup is automatically made.

Before making changes to the registry, you should back up any valued data on your computer. For detailed information about backing up and restoring system data like registries, see the topic "Backups and recovery" in the *Server and Client Administration and Startup Guide*.

To manage registry ACLs:

1. Using `regedt32`, select the registry key that you want to protect.
2. Right-click it and select **Permissions**. A dialog box similar to that provided by Windows Explorer will appear.

Managing file shares

File shares should also be protected. By default, any directory which is made available for network access will give "read access" to the Everyone group, that is, anyone on the network can read any file under the shared directory tree. This is generally too permissive.

Experion PKS uses file shares as follows:

- Distributing reports to Station users requires read access by Station users
- Distributing display pages requires:
  - "read" access by Station users
  - "write" access if users need to build displays
- Configuration Studio uploads and downloads require "write / file create" access by plant engineers.

Thus Experion PKS file shares should be set up to give the Honeywell Administrators group (engineers) "change access" and the Station users group "read access".

Other Microsoft services

Experion PKS relies on the presence of several complex Microsoft services. These must also be configured securely.

Internet Information Services

Internet Information Services (IIS) is needed for some functionality of Experion PKS (Event Archiving System Displays, Alarm Pager option (e-mail notification)) and eServer. In setting up and maintaining the IIS:

- Keep the number of virtual directories to a minimum. These are the access points used by the outside world, and will therefore be the target for hackers.
- Do not place executable `.asp` files and read only `.html` files in the same directory:
  - Directories containing HTML should have read-only permission
  - Directories containing ASP files should have execute-script permission only
- Never have network share directories within a virtual directory tree. If a user can write an `.html` or `.asp` file within a virtual directory, then that page can be executed by a browser and, with the help of scripting, can do untold damage to the system; for example they can delete files. File and directory permissions may be further contained with NTFS security options. IIS will compare its own permissions with those of NTFS and use the most restrictive.
- Where possible do not allow anonymous connections, since there is no indication who is calling. Where access is intranet, that is, from trusted domains, enable NT challenge/response so that IIS can determine the callers identity. Mixed mode connections can be allowed by enabling both anonymous and NT challenge connections and using NTFS to prevent access to those directories requiring client identity checking.

Attention

It is strongly recommended that you run the following tools if using IIS:

- The IIS Lockdown Tool, available as a free download from Microsoft
- Microsoft Baseline Security Analyzer (see “Microsoft Baseline Security Analyzer” on page 88)

SQL Server

Security concepts related to SQL Server are well discussed in publicly available literature. The following information will therefore concentrate on Experion PKS requirements. If other databases are hosted by the Experion PKS SQL Server, then their own security model must also be applied.

Experion PKS requirements

Where possible a user should not have access to multiple databases.

Experion PKS processes use integrated authentication to access the SQL database through the Honeywell Administrators group account.

Attention

- It is recommended that you run Microsoft Baseline Security Analyzer (see "Microsoft Baseline Security Analyzer" on page 88) on your SQL Server.
- Although Experion PKS does not use the SQL Server account `SA`, it is strongly recommended that you change the default password for this account as quickly as possible.

Securing Windows Terminal Services

Windows Terminal Services allows you to run Microsoft Windows-based programs on a server and display them remotely on client computers connected to the LAN. This can be a useful facility for remote administration, engineering and monitoring activities, but does provide an additional avenue for attack.

Several levels of protection are available which are detailed in Microsoft documentation. The fewer people given Terminal Services access the better, and logon rights should be removed as soon as access is no longer needed. Communications should be set to be encrypted.

The easiest way of allocating Terminal Services access to users is to place all such users in a special group and use the Terminal Services session manager to give that group, rather than the "Everyone" group, Terminal Services logon rights.

Securing RAS

The Remote Access Service (RAS) allows remote workstations to establish a dial-up connection to a LAN and access resources on the LAN as if the remote workstation were on the LAN; that is to provide "terminal services" like functionality over a dial-up line.

It is important to secure RAS if it is available and configured in your system. RAS can be used to allow dial-up access for engineers running a remote Station, or for an administrator when performing remote diagnostics, but can also be a significant security risk.

Follow these guidelines:

- Only give dial-in access to those users who need it.
- Revoke this right as soon as the need has passed.
- Ensure that their passwords are strong, and are changed frequently.
- Configure RAS to use encrypted authentication to prevent password stealing.
- If the computer is connected directly to a modem, consider limiting the valid TCP/IP ports available for connection.

Limiting access to the SMS Network Monitor

The SMS Network Monitor is a very useful tool which intercepts and displays network packets. Access to the tool should be controlled by password. In addition, both Windows 2000 servers and workstations have a Network Monitor agent which allows a remote monitor to intercept packets to or from that computer. The agent should also be password-protected using the Monitor Agent panel applet.

Miscellaneous settings

Windows 2000 has many registry settings that can be used to increase the overall security of a system. This section will discuss the more obvious options. For further information see Microsoft's white paper, *Solution for securing Windows 2000 Server*.

Desktop policy

Windows 2000 has an option to display a pre-canned banner when someone logs on. A typical message would be:

```
It is an offence to continue without proper authorization
```

Historically legal prosecutions of intruders have failed because no such warning was displayed. The banner can be defined using Group Policy or the local registry.

By default, Windows 2000 displays the name of the last user to log on in the logon dialog box. This saves time if the same user is logging on again, and provides a quick indication if an unauthorized logon has been attempted, but provides useful information to a would-be attacker: they only have to guess the password. Group policy or the local registry may be used to hide the last user's name.

By default, Windows 2000 allows anyone with access to the system console (whether logged on or not) or a Terminal Services session to shut down the system without trace. This feature should be disabled, either through the computer's Group Policy if part of a Windows 2000 domain, or through the local registry.

If the system console is not locked away with the server, then the option for the Recovery Console (an option used when troubleshooting a booting problem) should be configured to disable automatic Administrator logon. Without this change it would be possible for anyone with physical access to reboot the system and obtain Administrator access.

A password-protected desktop screen saver should be configured with a short timeout (say 10 minutes) so that unattended logged-on sessions cannot be high-jacked. In a control room with dedicated stations this may not be desirable, an alternative method is to configure Station idle timeouts to reduce the Station level to "view only".

Disable unused subsystems

Windows 2000 provides support for running executables intended for Windows, POSIX (UNIX) and OS/2 environments. The POSIX and OS/2 support is not required and should be disabled as they offer an increased attack surface to malicious users. These subsystems can be disabled with local registry settings. See Microsoft Knowledge Base article 320869, *How to Prevent Windows from Loading the Optional OS/2 and POSIX Subsystems*.

Restrict anonymous logon

By default, anonymous NetBIOS connections can be made to the server and used to obtain information about domain accounts, computer names, file shares, and so on. Although it does not directly allow the computer to be compromised, it provides valuable information which can be used for other attacks.

See the registry key `HKLM\system\CurrentControlSet\control\lsa` for details on disabling anonymous logon.

Caution

Incorrect changes to the registry may create problems or cause severe damage to your system. Changes made to the Windows registry happen immediately, and no backup is automatically made.

Before making changes to the registry, you should back up any valued data on your computer. For detailed information about backing up and restoring system data like registries, see the topic "Backups and recovery" in the *Server and Client Administration and Startup Guide*.

Where file share connections need to cross insecure networks, such as into the DMZ or across the Level 3/Level 4 boundary (see “Supported topologies” on page 53), consider enforcing the digital signing of SMB packets. This will prevent packet spoofing or session hijacking, at the expense of up to 15% CPU overhead. This option may be set either through the computer’s Group Policy (if the computer belongs to a Windows domain) or through the local registry.

Use NTLM Version 2

In a Windows NT 4 or mixed mode domain, the NTLM protocol will be used for authentication. Provided that all computers are at NT 4 SP6a or later, a more robust version (NTLMv2) may be used. This uses stronger encryption for credential exchange. For maximum security, both server and clients should be set to accept and transmit NTLMv2 only.

Caching of previous logons

Windows remembers the credentials of previous logged on users so that in the event of the domain server being unavailable, those users can continue to log on. Some security experts recommend that this caching be disabled to prevent sensitive information remaining in memory and hence being vulnerable to attack. This can, however, lead to a denial of service. Should the control room become disconnected from the domain server, no more user logons will be possible until re-connection occurs.

Harden TCP stack

Windows supports a number of options to help TCP/IP defend itself from well-known network attacks. Although it is recommended that these options be set for maximum protection, care must be taken to allow for the characteristics of individual LANs. Details can be found in the Microsoft Knowledge Base article: Q315669: *How To Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000.*

System monitoring

11

If all the steps outlined in this document are followed, then a secure system should result. However, there is always the possibility that an attacker will succeed in circumventing all the safeguards and break in. In this case it is important to discover the break in and prevent further damage as rapidly as possible. The more evidence that can be captured, the less the damage is likely to be and the greater the chances of identifying the intruder.

Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (MBSA) is a tool that you can run on Windows-based computers to check for common problems with security configuration. MBSA checks the operating system as well as other installation components such as Internet Information Services (IIS) and SQL Server. It also checks whether or not security updates are current.

MBSA is freely available for download from the Microsoft Web site. When run, MBSA attempts to connect to the Microsoft Web site in order to download the latest information on hotfixes, service packs, and so on. It only takes a few minutes to run and generates a series of reports on the security health of a system.

Analyzing the audit log

If there is a suspicion that the system is being misused, then Windows auditing provides a useful tool to track who has done what and when.

To enable auditing:

1. Log on as the Local Administrator.
2. Start the User Manager tool.
3. Select **Policies > Audit** and enable options of interest.

The most useful options are likely to be:

- Logon and Logoff - success and failure
- Process Tracking - success and failure
- Object access - success and failure

This enables the auditing of file system and registry access. It is then necessary to choose the objects of interest and the user (or groups) whose actions are to be audited. Note that since it is necessary to specify an identity to audit, and by definition, it is not known who the intruder is, specify the group “Everyone”.

For files:

1. Go to Windows Explorer and select the directory or file of interest.
2. Select **Properties > Security > Advanced > Auditing**.
3. Then add a user, for example, “Everyone” and the access to be audited; for example, “Open failure”.

The process is similar for registry keys:

1. Run `regedt32`.
2. Select the key for which you want to set up auditing.
3. Select **Permissions > Advanced > Auditing** and add users as above.

Obviously, there is no point in collecting audit information if it is not reviewed. When auditing is enabled, a responsible person should review the log frequently and take action if unexpected activity is seen.

Attention

The default action is to halt the system if the security log becomes full. This is to prevent activity occurring without any traceability. However, it also provides an opportunity for a denial of service attack.

To prevent this, either increase the log file size and review the log before it fills up, or set one of the overwrite options, and check the log frequently enough to prevent loss of events.

Start the Event Viewer tool, select **Log > Security** and then select **Log > Log Settings** to view the log settings. Change either the Maximum Log Size, or the Event Log Wrapping options.

If you give the mngr account “generate security audits” rights before starting the database service, and enable audit object access, then any attempt by an executable to open the Experion PKS database will also generate a security log message.

Detecting network intrusion

Network Intrusion Detection Systems (NIDS) can take many forms. They can be a dedicated server on the same network branch, freeware software available under GNU or similar licences (most of these are aimed at the UNIX world), or commercial products aimed specifically at Windows systems. Their purpose is to scan incoming network packets and look for unusual traffic or for specific malformed packets known to be associated with attacks. If anomalies are found NIDS take action such as raising alerts or even disconnecting the computer from the network. The latter is a dangerous option which causes its own denial of service while preventing damage from occurring to the system, by closing network ports, and so on.

Other forms of intrusion detection will search event logs looking for unusual events, or will compare the current file system to a known good image. Care must be exercised when running such tools to prevent them using too many resources and interfering with the control system.

Event response team

An event response team should be ready to handle any security breach as it occurs. Their role is to identify the attack, prevent further damage, recover from the damage and capture evidence which could be used in prosecutions. In many instances the IT department will already have such a team; they simply need to be made aware of any specific requirements of the control system.

Many Government and industry bodies and computer vendors have published good papers on this topic, which should be reviewed when building the team.

Useful references include:

- `http://www.microsoft.com/technet/security/guidance`
- `http://www.sans.org/resources/`
- `http://csrc.nist.gov/`

Experion PKS security features

12

This chapter describes security features specific to Experion PKS.

Experion PKS security is based on *operators* and *assets*:

- Operators are individual users or users grouped by role. Operators are assigned various degrees of access to assets through access levels. These allow restrictions varying from “view only” to “full control”.
- In the context of this chapter, the term “assets” refers specifically to the Experion PKS assets that comprise your Experion PKS asset model.

The following sections expand on these concepts.

Windows and Experion PKS user accounts

Experion PKS users fall into several roles, which can be reflected in the Windows user groups to which their account belongs. The main roles are: operators, plant engineers, system administrators, and in some cases, application developers. Each role needs different account characteristics and privileges.

On installation, Experion PKS adds a number of local groups and accounts to existing Windows groups and accounts. These include:

Account name	Description
mngr	A local account under which the Experion PKS processes run. For more details, see “Changing the Windows mngr password” on page 94 and “Requirements for the Windows mngr account” on page 95.
Honeywell Administrators	A local group to which engineers, administrators and developers must belong. Membership of this group gives direct access to the Experion PKS database, file system sub-tree containing Experion PKS executable and data files, and to the Experion PKS registry keys.
Engineering Repository Administrators	A local group giving permission to administer the engineering repository database. The `mngr` must belong to this group.
Engineers	A local group, created for convenience, which may be used to group plant engineers. If single signon (see “Single signon” on page 105) is required, this should be changed to be a domain group.

Changing the Windows mngr password

The `mngr` account is used by all Experion PKS core processes, by certain Experion PKS Windows services, and by certain Experion PKS COM servers. The `mngr` account is also used for DSA node authentication and by Console Stations.

Because the configuration of these services and COM servers involves specifying the `mngr` password, changing this password cannot be done lightly.

Attention

- If the `mngr` password is changed on a DSA node, then this account’s password must also be changed to the new value on all other DSA nodes.
- Similarly, the Experion PKS server and all Console Stations synchronized with that server must have the same `mngr` password.

Since best practice requires frequent password changes, the password utility `pwdutil.exe` is available for ensuring that the change is made consistently. For information about using `pwdutil.exe` see the topic "Changing the Windows mngr account password" in the *Administration and Startup Guide.*

The system administrator should run this periodically but with care as an invalid password could prevent Experion PKS operating correctly.

Requirements for the Windows mngr account

The Windows `mngr` account has a number of specific requirements:

- Password should never expire (incorrectly changing the password for `mngr` can result in the system failing to start)
- The following settings should be applied:
  - Deny logon locally
  - Deny logon through terminal services
  - Logon as a batch job
  - Logon as a service
  - Replace a process token

Attention

- Where a DSA environment is geographically compact it may be possible to have all the computers in a single domain. The `mngr` account must, however, be a local account rather than a domain account.
- To prevent access from external DSA systems it is necessary to change the Windows `mngr` account password as described above.

Requirements for the Honeywell Administrators group

The Honeywell Administrators group should be given the following privileges:

- Debug programs
- Profile single process
- Shut down the system

Experion PKS group key

Caution

Incorrect changes to the registry may create problems or cause severe damage to your system. Changes made to the Windows registry happen immediately, and no backup is automatically made.

Before making changes to the registry, you should back up any valued data on your computer. For detailed information about backing up and restoring system data like registries, see the topic "Backups and recovery" in the *Server and Client Administration and Startup Guide*.

Experion PKS restricts access to its database by placing ACLs on various securable shared objects which it creates (these include shared memory segments, semaphores, Mutexes and other kernel objects). These ACLs grant access to one or more user groups nominated in the following registry key:

```
LOCAL_MACHINE\software\Honeywell\Experion pks server\group
```

By default the Honeywell Administrators group is given access. There would not normally be any need to change the default group names.

You can specify multiple account groups by separating them with semicolons (;). This allows several user groups to access Experion PKS but have different access permissions to other areas of the server. The group specified must be a local group, not a global group, that is, it must be defined on the Experion PKS server, not a domain server.

User accounts and Experion PKS user roles

The users in your Experion PKS system generally fall into one of the four following user roles:

- Engineers
- Programmers
- Administrators
- Operators

The user account and access requirements of each role is described below.

Engineers

Engineers need access to configuration tools such as Configuration Studio, HMIWeb Display Builder, and Display Builder. They also need to view the system log and to run Station. This requires an account with more flexibility than the operator.

In addition, if they need to stop and start the Experion PKS services, or run utilities with direct access to the database such as `trace` or `dct`, then their Windows user account must be part of the Honeywell Administrators group.

If a site wishes to change the name of this group, or to give additional groups direct access to the database, then the following registry key may be changed (see the instructions in "Experion PKS group key" on page 96 for changing or adding user groups to a registry key):

```
HKLM/software/Honeywell/Experion pks server/group
```

You can reduce the management load if all engineers use the same logon. However, this is not recommended as it becomes impossible to trace an individual's activities in audit trails.

Programmers

Programmers should not develop on the live system because of the risk of disruption due to the excessive use of resources (CPU, memory, and disk throughput), and because of problems associated with untested code.

Development should occur on a second computer, and new executables should only be allowed on the live system after they have been thoroughly tested.

Sensitive sites may use file permissions to prevent changes and additions to the executables in the `run` directory by anyone other than an authorized administrator. Anyone who adds or removes processes running under the Experion PKS umbrella must belong to Honeywell Administrators group. Typically, they also belong to the Power Users group.

Administrators

Administrators generally have two roles. They are expected to perform backups, and to undertake performance monitoring, diagnostic investigation and software configuration tasks for the Experion PKS system. They must belong to Honeywell Administrators group and the Backup Operators group for these activities.

They are also expected to manage user accounts, perform audits, undertake operating system upgrades and so on, for which they must belong to the Windows Administrators group.

Best practice requires that administrators have two accounts, and that they only use the account belonging to the Windows Administrators group when absolutely necessary. This reduces the risk of accidental damage, and of leaving a highly privileged account logged on and liable to hijacking.

Operators

While every user logging onto a Windows computer needs their own Windows user account, it may not be necessary to configure individual operator accounts in Experion PKS. Depending on the Experion PKS security model you choose, operators may be:

- Defined only within the Experion PKS database, or
- A member of a Windows group, or
- A separate Windows account.

For more information, see “Station security” on page 99 and “Integrated accounts” on page 104.

Station security

In deciding on the kind of Station security to implement you need to consider the following:

- What type of Station security do you want to use:
  - Operator-based security, or
  - Station-based security?
- If you choose operator-based security, do you want to use:
  - Traditional operator accounts?
  - Integrated accounts using either domain-based Windows accounts or local Windows accounts?
  - Windows group accounts using either domain-based Windows groups or local Windows groups?
  - Electronic signatures?
  - Single signon?
- What type of access do operators require within Experion PKS?
- How do you want to implement Windows security?
- What type of Windows accounts do you require?
- Do you want to use the Honeywell High Security Policy?

To learn more about	Go to:
Station-based security	page 100
Operator-based security	page 101
Group accounts	page 106
Integrated security	page 104
Honeywell High Security Policy	page 73

Station security choices

Experion PKS offers two types of security:

- Station-based security
- Operator-based security

This allows you to configure security levels, control levels, and asset assignments for individual operators (or groups of operators) or alternatively for individual Stations.

About Station-based security

Station-based security works as follows:

- Station starts without prompting users to enter any form of operator ID or password.
- The initial security level setting allows users to perform the basic operating functions associated with the user level of `Oper` (for example, acknowledging alarms and controlling points).
- Users only need to use a password if they want to change to a higher level of security (that is, to `Supv`, `Engr`, or `Mngr`).
- Asset assignment applies to the Station, not to the operator.

The security levels and their associated functions are described in "About security levels" on page 107.

Attention

If you opt for the Station-based security method, it is recommended that the default passwords for `Engr`, `Supv`, and `Mngr` security levels (that were installed as part of the Experion PKS installation process), be changed as soon as possible after installation.

The `paswrd` utility used for this change may be run by anyone belonging to the Honeywell Administrators group. Additional file system ACLs may be used to further constrain the use of this tool.

About operator-based security

Operator-based security provides a higher level of security than Station-based security. In general, operator-based security with traditional operator accounts works as follows:

- You assign a specific security level to each user.
- Users cannot access any Station functions unless they enter a valid user ID and password.
- To access a higher security level than the one they are currently using, users need to sign off and then sign on again as a different operator who has the higher security level.
- Assignable assets are assigned to the operator, irrespective of which Station they are currently logged on to.

Operator-based security is appropriate if you need to specify each user's access and control rights, or where an operator remains at the Station throughout a shift.

Attention

You must use operator-based security if you want to use:

- Single signon
- Electronic Signatures

Operator-based security variations

If you choose operator-based security, there are several alternatives that you can use:

Account type	Description
Traditional operator account	An account whose definition exists in the Experion PKS server database. Authentication and authorization is done by the Experion PKS server.
Integrated account	A combination of a Windows user account and an Experion PKS operator account. Authentication is done by Windows, authorization is done by the Experion PKS server.
Windows group account	An integrated account that allows you to add multiple users by adding the Windows group to the Experion PKS server. Authentication is done by Windows, authorization is done by the Experion PKS server.

There are two aspects to operator-based security: authentication and authorization. Authentication is the process of verifying that a user is known to the system, while authorization controls what a known user can do within the system. Accounts are used to restrict access and authority within Station.

- For traditional operator accounts, authentication of the user is done by the Experion PKS server against credentials stored in Experion PKS. Authorization is also controlled by Experion PKS using security levels and, if applicable, assignable assets.
- For integrated accounts and Windows group accounts, authentication of the user is done by Windows on the server computer against the Windows user account. Authorization is then controlled by the Experion PKS server using security levels and, if applicable, assignable assets.

By using Windows group accounts you can add multiple users to Experion PKS simply by adding the Windows group. All users within the Windows group can then log on to Station in the same manner as traditional operator accounts or integrated accounts.

You can further restrict operator authority by restricting the level of access to assets (see “Assets” on page 110). Access to assets uses a separate set of security levels (see “Control levels” on page 108).

Disabling an operator account

If you want to remove access to Experion PKS for a particular operator but want to keep the operator account, you can disable the operator access rather than deleting the operator account. For detailed procedures, see the topic “Disabling an operator account” in the chapter “Configuring security and access” in the *Server and Client Configuration Guide*.

About traditional operator passwords

For security reasons:

- An operator password consists of a minimum of 5 alphanumeric characters and is stored using one-way encryption.
- Operators may change their own passwords, but a new password cannot be the same as the last 10 passwords used in the previous 3 months. The validity period for passwords defaults to one month, but this setting can be configured as required.

- When signing on, three unsuccessful attempts will lock the operator out for a configurable lockout period. Note that making the retry count too small, or the lockout time too great could lead to a denial of service if a malicious person attempts numerous consecutive failed logons.
- Once logged on an operator can log off at any time, or they will be automatically logged off after a defined period of inactivity. This will result in the same page, or if configured, an idle page, being displayed in view only mode. Any attempt to change pages, or perform data entry, will cause a logon dialog box to appear.

For more information, see the topic “Changing passwords” in the chapter “Configuring security and access” in the *Server and Client Configuration Guide*.

Integrated accounts

You can control operator access to Experion PKS using an integrated account. An integrated account is a combination of a Windows user account and an Experion PKS operator definition. The security credentials stored in the Windows user account are used to authenticate the user, while the security details in the Experion PKS operator definition are used to control the authority the user has within Experion PKS.

Using integrated accounts enables you to:

- Use existing enterprise-wide security policies
- Use single signon
- Minimize the number of accounts required for operators
- Use Windows auditing to track user activities

The benefits and impact of integrated accounts vary depending on your logical network configuration. For guidance, see the detailed scenarios in the topic "Using Integrated Security" in the chapter "Configuring security and access" in the *Server and Client Configuration Guide*.

Considerations and prerequisites

When deciding how to implement integrated accounts, consider the following:

- You need to set up a Windows user account, so that the user can be authenticated, and then create an operator definition in Experion PKS, so that the user's authority can be controlled.
- You need to decide what type of Windows user accounts you use: either local or domain accounts. Different account types will suit different site requirements.
- You need to decide if your system will use single signon.
- You then need to add the Windows accounts to the appropriate Honeywell Experion PKS Windows group, that is, add accounts for operators to the Honeywell Experion PKS Users group. If the operator also needs to use configuration tools such as Configuration Studio, add the Windows account to the Honeywell Administrators group.

Converting traditional operator accounts to integrated accounts

If you already have traditional operator accounts, you can convert these accounts to integrated accounts. For detailed procedures, see the topic "Converting traditional operator accounts to integrated accounts" in the chapter "Configuring security and access" in the *Server and Client Configuration Guide*.

Single signon

If you are using integrated accounts you can set up single signon. Single signon enables operators to log on to the Station computer and start Station by providing their operator ID and password only once when they log on to the computer. This is a configurable option that requires the use of operator-based security integrated with Windows accounts.

Signon Manager

Signon Manager is an application that provides a point of single signon on a particular computer to applications that use this facility. Users can:

- Sign on to any applications that are “Signon aware” through Signon Manager.
- Change the current user without having to shut down and restart any applications or the computer.
- Temporarily override the current user security credentials without having to shut down and restart any applications or the computer.

Signon Manager is optional and can be used with Station if the security type is operator-based and integrated with Windows accounts.

The benefit of using Signon Manager is that operators can sign on and off without losing view of the plant or critical processes. When a different user signs on to Signon Manager, any instances of Station that are running receive notification of the change of user. The Experion PKS server then verifies the authority of the user in the normal manner and changes to the appropriate security level for the user who is currently signed on.

Sample scenario

An operator is logged on to Signon Manager and is running multiple instances of Station on their workstation. At the end of the shift, the next operator needs to sign on with their security credentials. The operator for the next shift calls up Signon Manager and enters their user name and password. All instances of Station are notified of the change of operator and the new operator is now effectively logged on to all Stations with the correct security credentials.

Windows group accounts

If you are using integrated Windows and Experion PKS accounts (see “Integrated accounts” on page 104), and you have also set up Windows group accounts, you can add Windows group accounts to Experion PKS. This enables all members of that Windows group to log on to Station.

The benefits of using Experion PKS Windows group accounts are that you:

- Only have to configure one account in Station for every Windows group, and therefore reduce the number of accounts required in Experion PKS.
- Can leverage any existing Windows security policies and settings.
- Can apply any Experion PKS security and access restrictions at the group level.

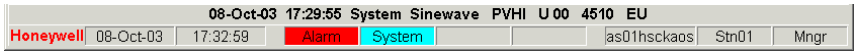
The Windows group can be a local Windows group or a domain Windows group. For information about the use of local or domain Windows groups, see the topic “Using Integrated Security” in the chapter “Configuring security and access” in the *Server and Client Configuration Guide*.

For more information about using Windows group accounts in Experion PKS, see the topic “Adding an Experion PKS Windows group account” in the *Server and Client Configuration Guide*.

About security levels

The current security level of a Station is displayed in the status line (lower right-hand side). If no operator is signed on to the Station, this part of the Station status line is blank.

Figure 2 Status line showing the current security level setting (“Mngr”)



You can use up to six different security levels in Experion PKS. These levels are shown in the following table in ascending order of access.

Table 10 Security levels

Default Security Level Acronym	Default Meaning
View Only previously called Lvl1 (Available with operator-based security only)	View-only mode
Ack Only previously called Lvl2 (Available with operator-based security only)	Alarm acknowledgement mode
OPER	Operator mode
SUPV	Supervisor mode
ENGR	Engineer mode
MNGR	Manager mode

If you have configured a Station to use operator-based security:

- The Station prompts you to sign on, and you cannot access any Station functions until you have successfully signed on.

If you have configured a Station to use single signon (available only if you are using Windows accounts):

- The Station starts with the credentials of the current Windows account if the equivalent operator definition exists in Experion PKS.

If you have configured a Station to use Station-based security:

- The Station starts at a security level of `Oper`, but you need to enter a password if you want to access a higher level of security.

The security levels `Oper` through `Mngr` can be assigned to server functions. In order to use the function, the current security level used to run Station must be equal to or greater than the security level assigned to the function. For example, a push button on a display might be assigned a security level of `Supv` when a custom display is built. In order for an operator to use the push button, the Station security level must be either `Supv` or `Mngr`.

For a detailed listing of actions permitted at each security level, see the topic "Actions permitted at each security level" in the *Server and Client Configuration Guide*.

Setting security levels for enabling or disabling channels and controllers

Security levels are also used to define which level of security is required to enable or disable hardware items.

For detailed procedures, see the topic "Enabling and disabling channels and controllers" in the chapter "Configuring controllers" in the *Server and Client Configuration Guide.*

Attention

This enable/disable security level setting applies to every Station in your system.

Setting security levels for downloading from Configuration Studio

As an option, security levels can also be used to control who can upload and download changes to the engineering database made via Configuration Studio. An Experion PKS global setting requires that the Configuration Studio user is running under a Windows account known to Experion PKS (that is, using an integrated account) and configured to have mngr access level.

Control levels

Operator-based security provides up to 255 control levels to further refine operator control access to individual items of plant and equipment. Any control action to a given point is only allowed if the control level configured in the operator or profile exceeds the level assigned to the point. Any actions initiated by an operator are logged in the Event database against an operator identifier.

Display page security

The data that can be viewed with a display page is primarily controlled by assigning to operators the assets that contain the data. Values can be seen if the access level is View or higher. Values can be changed if the access is `Oper` or higher. However, additional constraints can be defined for an individual page.

- A page may be assigned to an asset, so that the operator has to have View access to that asset in order to call up the display page at all.
- An individual database link can have data entry permissions set. Data entry can be totally prevented, that is, the field is read only, or a security level may be applied, allowing an operator with lower level to see the data, but not modify it. This technique is used on many system pages to restrict data entry to Admin level only.

ODBC client authentication

ODBC clients using the Experion PKS data source are authenticated when they first establish a connection. Asset assignments are used to limit access to data, unless the user has `Mngr` access level. An operator name may be specified as part of the data source definition, or may be supplied via a dialog box on connection. Authentication can be as a traditional operator, a Windows integrated account or group. Single signon will take effect if permitted.

Assets

In Experion PKS *assets* are database entities that represent a physical part of a building or a particular process. Assets can represent entities such as fixed plant equipment, materials, facilities, and buildings.

An Experion PKS asset model provides an organizational structure that enables you to engineer your Experion PKS system around your key entities and provides a hierarchical structure that resembles your organization.

About assignable assets

Within an asset model you can define assignable assets in order to restrict access to parts of the system, process, or individual pieces of equipment.

By configuring assignable assets (and profiles) you can restrict access to:

- Points, that is, to points associated with a particular asset, and to points found in a particular asset sub-tree.
- Alarms so that operators will only see alarms emanating from points that fall within their profile.
- Flex Stations, Consoles, and Console Stations. With Station-based security, a Flex Station, Console, or Console Station is assigned to a particular asset or profile, and can only access points, custom displays and reports that are assigned to that profile. (See “About Station-based security” on page 100.)
- Specific operators (providing you use operator-based security). (See “About operator-based security” on page 101.)
- Custom displays
- Reports

For more information, see “Using assignable assets to define scope of responsibility” in the *Server and Client Configuration Guide*.

Access levels

Asset assignments therefore limit operator or Station access to graphics, alarms and point data to assigned assets, thus providing effective plant partitioning. The limitation of asset assignment can be further refined to define access as “View only”, “View and acknowledge”, or “Full access”. These access levels are used in conjunction with the existing operator-based or Station-based security.

As a configuration option, the system will require that both the operator and Station have appropriate asset access prior to granting control. This enhances safety by preventing an operator with broad access from operating equipment from an unsafe location.

Individual operator details, including security levels, control levels and asset assignments, are activated when operators sign on to the system. In addition, profiles (see "About profiles" on page 111) can be created enabling plant items and similar assets to be enabled or disabled for control, between certain time and date criteria.

For example, the asset, `Precipitator`, and all child assets and points associated with the `Precipitator` asset are viewable by Stations or operators that have had the `Precipitator` asset assigned to them, with an access level of at least "View only". If a Station or operator does not have the `Precipitator` asset assigned with at least "View only" access, they cannot view child assets or points associated with the `Precipitator` asset.

For detailed procedures on using assignable assets to control access to the system, see the chapter "Configuring your Enterprise Model" in the *Server and Client Configuration Guide*.

About profiles

Within an asset model Experion PKS also uses profiles as a means of further refining the restriction of access. A profile consists of an asset list containing one or more assets, and a time period. If you are using operator-based security, you can set up profiles to provide:

- Additional security by assigning assets only for specified times
- A method of giving an operator additional access at specified times; for example, after-hours monitoring from a central location.
- A quick way of assigning assets to operators

For more information

To learn about	Go to:
Planning your asset model	The chapter "Assets and asset models" in the *Server and Client Planning Guide*
Configuring assets and asset model	The chapter "Configuring your Enterprise Model" in the *Server and Client Configuration Guide*. See also the *Enterprise Model Builder User's Guide*
Configuring asset lists, time periods, and profiles	"Configuring profiles for scope of responsibility" in the chapter on "Configuring security and access" in the *Server and Client Configuration Guide*.

Restricting access to operating systems and non-Station software

To prevent an operator from accessing the operating system and software other than Station software, you can configure the computer as a "secure" Station. This is an appropriate action for dedicated or static Stations.

Setting up a secure Station involves securing the operating system and non-Station software as well as securing Station. The procedures for securing Station described in this section can be used in conjunction with the Experion PKS High Security Policy.

To restrict access to the operating system and non-Station applications, you need to:

- Set up a secure Station. See "Setting up a secure Station" on page 112.
- Remove access to the operating system and applications other than Station. See "Locking Station in full screen and disabling menus" on page 113.
- You should also remove the link from the System Menu display to Knowledge Builder as Knowledge Builder uses Internet Explorer. When Internet Explorer is open operators can gain access to other files.

Setting up a secure Station

Locking down (that is, securing) Station involves the following tasks.

Attention

- If you want an operator to print, you need to set up access to the printers for the operator before you complete the tasks in this section.

1. Creating a batch file which starts Station automatically.
2. Specifying the batch file as a logon script to the user account.
3. Preventing operators from shutting down their computer.
4. Removing access to applications via Task Manager and Windows Explorer.
5. Setting up automatic logon (optional).

   If you set up automatic logon, to log on as Administrator you need to press the Shift key to prevent automatic logon.
6. Preventing users from locking the computer.

For detailed instructions on completing each of these tasks, see the section on setting up a secure Station in the chapter “System administration” in the *Server and Client Administration and Startup Guide*.

Locking Station in full screen and disabling menus

You can restrict access to non-Station software on a computer by changing the Station command line.

If you want to completely restrict access to the Station computer, use the procedure in the section “Restricting access to operating systems and non-Station software” on page 112 and use the High Security Policy.

Changing the Station command line allows you to:

- Lock the Station window in full screen so that users cannot resize the window or access operating system functions and non-Station applications.
- Disable the **Exit** menu choice so users cannot close down this Station.
- Disable the **Setup** menu choice so that users cannot change the connection or display settings for this Station.
- Disable the **Connect** menu choice so that users cannot attempt to connect to a different server and disconnect from the current server.

For detailed instructions, see the topic “Changing the Station command line” in the chapter “System Administration” in the *Server and Client Administration and Startup Guide*.

Access to Intranet and Internet sites is disabled by default on Station. For information on enabling full or restricted access see the topic “Web access” in the chapter “Configuring Stations and printers” in the *Server and Client System Configuration Guide*.

Electronic signatures

The Experion PKS Electronic Signatures option is specifically designed to support users (such as the pharmaceutical industry) that must meet the requirements of 21 CFR Part 11. However, it is also useful to any user requiring the ability to absolutely trace all operator actions.

You can configure operator actions, such as acknowledging a message or controlling a point, to require one or two electronic signatures before the action is performed. You can also require a reason to be specified before the action is performed.

Electronic signatures are the legally binding equivalent of an operator's handwritten signature. Each time such an action is performed, an event records the name of the operator(s) who initiated the action, the specified reason and the date/time.

A set of reasons must be configured so that the operator can select from this set at the time of signing. A reason set can contain up to 32 reasons.

Events recording the names of the operators responsible for the action, date, time and reasons are generated and stored in the events database. These events can be viewed in the Event Summary. If an operator partially completes signing an action and then cancels the action, an event is also generated. Operator actions are not complete if:

- The user name or password provided by the operator is invalid.
- The operator cancels the Electronic Signature dialog box.
- A timeout has been set for the action and the time has been exceeded before the signing was complete.
- The operator does not have the appropriate security level required for the action.

Prerequisites

Electronic Signatures require the use of operator-based security integrated with Windows accounts. For more information about integrated accounts see "Integrated accounts" on page 104 of this guide, and also the topic "Using integrated security" in the chapter "Configuring security and access" in the *Server and Client Configuration Guide*.

For more information

For more information about electronic signatures, see the chapter "Configuring electronic signatures" in the *Server and Client Configuration Guide*.

Glossary

Access Control List

A list of user accounts and groups, each entry specifying a set of allowed, or disallowed actions. When applied to a firewall, an ACL is a list of node addresses and ports that may (or may not) pass through the device.

ACL

The abbreviation for “Access Control List.”

asset

In an Experion PKS asset model, an asset is a representative entity such as fixed plant equipment, materials, and buildings.

asset model

The Experion PKS Asset Model provides an organizational structure to enable you to engineer your Experion PKS system around your key entities. It provides a hierarchical structure that is intended to resemble your organization.

Because of this, the Asset Model can help operators more easily identify particular parts of the plant or specific pieces of equipment without having to remember obscure names. For example, you have a point that represents a flow controller; the unique identifier for the flow controller is FC123. The Asset Model enables you to give the point a more intuitive name such as FlowController.

The Asset Model also provides an intuitive way of allowing or restricting access to parts of the plant, process, or equipment with the use of assignable assets.

assignable assets

An asset that can be assigned to an operator or Station for the purposes of controlling what an operator or Station can view or control in the Experion PKS system.

authentication

When a user logs on to a system the authentication process verifies that a user is known to the system. See also “authorization”.

authorization

When a user logs on to a system, the authorization process controls what a known user can do within the system. See also “authentication”.

business network

A collective term for the network and attached systems at Level 4. See also "Levels 1 through to 4."

Configuration Studio

Configuration Studio is an Experion PKS tool that provides a central location from which you can configure your Experion PKS system. Configuration Studio presents a customized list of tasks that you are required to complete to configure your system. The list of tasks is automatically generated based on your licence details. When you click a task, the appropriate tool is launched so that you can complete the task.

Console

A logical grouping of Console Stations and Console Extension Stations.

Console Extension Station

A Flex Station that is connected to a Console Station rather than to the server.

Console Station

A Station that has direct access to Process Controllers in addition to the server. Consequently, there is no loss of view of critical process data if the server fails.

Compare with a Flex Station.

controller

Generic term for a device that is used to control and monitor one or more processes in field equipment. Controllers include Programmable Logic Controllers (PLCs), loop controllers, bar code readers, and scientific analyzers.

demilitarized zone

A demilitarized zone (or DMZ), is an area with some firewall protection, but which is visible to the outside world. This is where public servers for Web sites, file transfers and email are located. More sensitive, private services such as internal company databases, intranets and so on are placed behind a further firewall and have all incoming access from the Internet blocked. You can also create an effective DMZ with just one firewall by setting up access control lists (ACLs) that let a subset of services be visible from the Internet.

Distributed Systems Architecture

An option that enables multiple Experion PKS systems to share data, alarms, and history.

DMZ

The abbreviation for "demilitarized zone."

DSA

The abbreviation for “Distributed Systems Architecture.”

electronic signature

A combination of a user ID and password which are used as the legally binding equivalent of a handwritten signature.

Emergency Repair Disk

One of the options available with the Microsoft Windows Backup utility is the creation of an Emergency Repair Disk that can help you to fix damaged system files or repair a computer that will not start.

ERD

The abbreviation for “Emergency Repair Disk”.

FIM

The abbreviation for “Fieldbus Interface Module”.

firewall

A firewall is a software or hardware barrier that sits between two networks, typically between a LAN and the Internet. A firewall can be a standalone network appliance, part of another network device such as a router or bridge, or special software running on a dedicated computer.

Firewalls can be programmed to block all network traffic from coming through except that which has been configured to be allowed. By default, a firewall should block all 65,000 ports and then open up only the ports you need. So, if you need to browse the web, then it should allow “outgoing” traffic on port 80. If you would like DNS lookups to work for you then you would need to open up port 53 for “outgoing” traffic. If you want to access your internet mail server through POP3, then you would open up port 110 for outgoing traffic. Firewalls are directional, that is, they pay attention to where the traffic originates, that is, whether it is “incoming/inbound” and “outgoing/outbound”.

Quite frequently you will not want any unsolicited inbound traffic unless you have specific reasons (for example, you might have a web server that you want people to be able to access). However, in most cases, a web server would probably be located outside your firewall and not on your internal network. This is the purpose of a “demilitarized zone.”

The following Microsoft reference is a useful source of information about well known TCP/IP ports:

```
http://support.microsoft.com/default.aspx?scid=kb;en-us;832017
```

Flex Station

A Station that is generally installed on a computer other than the server computer, and which is connected to the server using either a static or rotary connection.

Compare with a Console Station.

FTE

The abbreviation for “Fault Tolerant Ethernet,” the control network of Experion PKS.

GUS

The abbreviation for “Global User Station,” a TPS node.

IP

The abbreviation for “Internet Protocol.”

Knowledge Builder

An online library that contains the complete Experion PKS documentation set.

LAN

The abbreviation for “Local Area Network.”

Levels 1 through to 4

The location of a node within an Experion PKS network and attached systems are often categorized in terms of a series of levels.

- Level 1 is where real time control takes place
- Level 2 is where supervisory control takes place
- Level 3 is where advanced control and advanced applications reside
- Level 4 is where the business network resides

Levels 1 to 3 inclusive constitute the “process control network.” Between Levels 3 and 4 you might have a demilitarized zone to help restrict unauthorized access to the process control network.

locking down

The procedure whereby a given user is given access to only one or a few specific programs is known as “locking down” a desktop or computer.

MAC

The abbreviation for “Media Access Control,” the lowest level LAN protocol layer under the IEEE 802.11-1997 standard. MAC can also be an abbreviation for “Message Authentication Codes”, a cryptographic hash added to a message to enable the detection of tampering.

MES

The abbreviation for “Manufacturing Execution Systems.”

MRP

The abbreviation for “Manufacturing Resource Planning.”

NAT

The abbreviation for “network address translation.”

network address translation

This is a protocol that enables networks to access the Internet by translating private IP addresses.

node

A node is a processing location within a network. It can be a computer or some other device, such as a printer.

PHD

An abbreviation for “Process History Database,” the Experion PKS history node.

port

A port is a logical endpoint on a network node used for communications. There are approximately 65,000 ports on which any one IP address can communicate. Some are dedicated to specific well-known services; some are used by application services; and some will be dynamically allocated to clients as they connect to remote services. A service listens on a known port for client connections, if the connection is accepted then the client will address messages to that port, the server will send responses to the dynamically allocated client port.

PCN

The abbreviation for “process control network.”

Process Controller

Experion PKS’s controller, which can handle all possible control requirements—whether for continuous processes, batch processes, discrete operations, or machine control needs. The term is used to refer to all control hardware (chassis, power supply, Control Processor, and ControlNet bridge) as a single entity.

Points on a Process Controller are called *process points*.

process control network

A collective term for the network and connected systems at Levels 1 through to Level 3. See also “Levels 1 through to 4.”

redundant server

In a redundant server system, the backup server is actively linked to the primary (running) server, so that it can take immediate control if the primary server fails or is shut down. When synchronized, any change made to the primary's database will be automatically reflected in the backup's database.

subnet

A group of hosts that form a subdivision of a network.

subnet mask

A subnet mask identifies which bits of a IP address are reserved for the network address. For example, if the IP address of a particular node is 192.168.2.3 with a subnet mask of 255.255.255.0, this subnet mask indicates the first 24 bits of the address represent the network address and the last 8 bits can be used for individual node addresses on that network.

switch

A switch is a multi-port device that moves Ethernet packets at full wire speed within a network. A switch may be connected to another switch in a network. Switches direct packets to a destination based on their MAC address. Each link to the switch has dedicated bandwidth (for example, 100 Mbps).

Station

The Experion PKS operator interface.

TCP/IP

The abbreviation for Transmission Control Protocol/Internet Protocol.

terminal server

A terminal server allows you to connect several controllers and Stations to a network even though they only have serial or parallel ports. Most terminal servers also provide a range of serial connection options, such as RS-232, RS-422 and RS-485.

TPS

The abbreviation for TotalPlant® Solutions.

unassigned item

In the Experion PKS asset model, an unassigned item is an item that has not been associated with an asset. For example, if you build a point but do not associate the point with an asset, when you download the point, the point is considered to be an unassigned item. Likewise, if you delete an asset but retain the points associated with the asset, those points become unassigned items.

uninterruptible power supply

For a process control network, reliable power is essential, so it is important to provide an uninterruptible power supply (UPS). If the site has an emergency generator, the UPS battery life may only need to be a few seconds; however, if you rely on external power, the UPS probably needs several hours supply.

uplink

Any interface that connects switches to switches or switches to routers.

UPS

The abbreviation for “uninterruptible power supply.”

WAN

The abbreviation for “Wide Area Network.”

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Honeywell

Honeywell Process Solutions
2500 West Union Hills
Phoenix AZ 85027
USA