Honeywell

Experion PKS
Network and Security Planning Guide

EPDOC-XX75-en-431A
February 2015

Release 431

Honeywell

Document	Release	Issue	Date
EPDOC-XX75-en-431A	431	0	February 2015

Disclaimer

Contents

1 About this guide

This document contains networking and security-related information applicable to Experion. It provides information about the recommendations to assist you in planning, setting up, and maintaining a secure environment for your system.

Revision history

Revision	Date	Description
A	February 2015	Initial release

2 Introduction

This guide contains networking and security information applicable to Experion. It documents the recommendations to assist you in planning, setting up, and maintaining a secure environment for your system.

Related topics

"Assumptions and prerequisites" on page 10
"How to use this guide" on page 11
"Related documents" on page 12

2.1 Assumptions and prerequisites

This guide is primarily intended for engineers, system administrators, and other technical staff who are responsible for planning the configuration and maintenance of an Experion system. Therefore, it is assumed that the user must have technical knowledge and familiarity with the following:

- Microsoft Windows operating systems
- Networking systems and concepts
- Security issues and concepts

Attention

As you derive a security program for your process control system you must be aware that detailed information, if not protected, can fall into the hands of organizations that could cause harm to your control system or process operations.

Important terminology

You must be familiar with the Microsoft terms listed in the following table to understand the concepts of security and configuration.

Microsoft terms	
access control list (ACL)	local group
access mask	organizational units (OU)
access token	permission
domain	privilege
global group	universal group
group memberships	user account
group policy	user rights
group policy object (GPO)	workgroup

You can find the definitions for the terms listed in the table on the following Microsoft web site.

http://www.microsoft.com/resources/glossary/default.mspx

2.2 How to use this guide

If you have specific security concerns such as protecting your Experion system against viruses or preventing unauthorized access, refer to the section “Security Checklists” on page 13.

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

For Information About:	Refer to
Developing a security program.	“Developing a Security Program” on page 21
A strategy for backups and recovery.	“Disaster Recovery” on page 29
The physical security of your system.	“Physical and Environmental Considerations” on page 35
Measures for keeping security related software up to date	“Microsoft Security Updates and Service Packs” on page 41
Antivirus measures	“Virus Protection” on page 47
Network planning	“Network Planning” on page 57
Network port access connections through firewalls	“Network Security” on page 85
Securing wireless devices	“Securing Wireless Devices” on page 139

2.3 Related documents

The following documents complement this guide.

Document	Description
Overview	Provides a comprehensive overview of Experion, including basic concepts and terminology.
Server and Client Planning Guide	Contains high-level planning and design topics for Experion servers and clients, as well as for controllers other than Process Controllers.
Server and Client Configuration Guide, and *System Administration Guide*	Contains detailed configuration information about Experion security.
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.
Windows Domain and Workgroup Implementation Guide. For planning information, refer to Windows Domain and Workgroup Planning Guide. For operation system migration information, refer the appropriate operating system-specific implementation guide Windows Domain Implementation Guide for Windows Server 2008 R2/Windows Domain Implementation Guide for Windows Server 2012.	Provides information about installing and configuring domain controllers and Windows workgroups.
Software Installation User's Guide	Describes how to perform a clean install of Experion servers and station nodes.
Experion Mobile Access User's Guide	Describes planning and security considerations, installation and configuration procedures, and operating instructions for Experion Mobile Access.

3 Security Checklists

This chapter provides a number of checklists which help you analyze the security issues that must be considered for your site.

The checklists cover some of the main threats that may exist on a process control network and the steps that can be used to mitigate against them. They also provide an alternative way of navigating through this document, depending on your key concerns.

Related topics

“Viruses and other malicious software agents” on page 14

“Unauthorized external access” on page 15

“Unauthorized internal access” on page 16

“Accidental system change” on page 17

“Protecting Experion system components” on page 18

“System performance and reliability” on page 19

3.1 Viruses and other malicious software agents

This threat encompasses malicious software agents such as viruses, spy ware (trojans), and worms.

The intrusion of malicious software agents can result in the following:

- Performance degradation
- Loss of system availability
- The capture, modification, or deletion of data
- Loss of prestige if the external access becomes public knowledge

Mitigation steps

√	Mitigation steps	For more information, refer to
	Ensure that your virus protection and Microsoft security hot fixes are up to date on all nodes in your process control network and the systems connected to it.	“Virus Protection” on page 47
	Ensure that there are no e-mail clients on any nodes of your process control network	“Prohibit email clients on the process control network” on page 55
	Use a firewall and DMZ for the business network to process control network interface	“Connecting to the business network” on page 91
	Use Honeywell's High Security Network Architecture	“High Security Network Architecture” on page 86
	Lock down the nodes in your system.	“Honeywell High Security Policy” on page 167

3.2 Unauthorized external access

This threat includes intrusion into the process control system from the business network and possibly an intranet or the Internet.

Unauthorized external access can result in the following:

- Loss of system availability
- Incorrect execution of controls causing damage to the plant, or theft or contamination of product
- Loss of prestige if the external access becomes public knowledge

√	Mitigation steps	For more information, refer to
	Use a firewall/DMZ for the business network to process control network interface to restrict access from the business network to process control network.	“Connecting to the business network” on page 91
	Set the minimum level of privilege for all accounts, and enforce a strong password policy.	“Windows user accounts and passwords” on page 164
	Monitor system access.	“System Monitoring” on page 151
	Use Honeywell's High Security Network Architecture	“High Security Network Architecture” on page 86
	Securing wireless devices	“Securing Wireless Devices” on page 139
	Lock down the nodes in your system	“Honeywell High Security Policy” on page 167
	Use the firewall on Windows 7 and Windows Server 2008 machines	“Use the firewall on Windows 7 and Windows Server 2008 machines” on page 177

3.3 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.

Unauthorized internal access can result in the following:

- 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	For more information, refer to
	Ensure Station security.	“Station security” on page 185
	Use physical security for process control network systems.	“Physical and Environmental Considerations” on page 35
	Do not allow the use of unauthorized removable media (for example, CDs, floppy disks, and memory sticks) on any node in (or connected to) your Experion system.	“Protecting against unauthorized system access” on page 37
	Use strong passwords on network equipment.	“Securing network equipment” on page 114
	Monitor system access	“System Monitoring” on page 151
	Prevent the use of unauthorized laptops on the process control network (PCN).	“Connecting other nodes to the process control network” on page 113
	Use and enforce a strong password policy	“Windows user accounts and passwords” on page 164
	Lock down the nodes in your system	“Honeywell High Security Policy” on page 167
	Ensure strong access controls are in place on the file system, directory, and file shares	“File system and registry protection” on page 170
	Securing wireless devices	“Securing Wireless Devices” on page 139

3.4 Accidental system change

This threat encompasses inadvertent changes to executables or configuration files.

Accidental system change can result in the following:

- Loss of system availability
- Loss of data

Mitigation steps	For more information, refer to
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	“Windows user accounts and passwords” on page 164
Lock down the nodes in your system	“Honeywell High Security Policy” on page 167
Ensure strong access controls are in place on the file system, directory, and file shares	“File system and registry protection” on page 170

3.5 Protecting Experion system components

The tables in this section list the steps you can take towards securing the following Experion.

- Server(s), Stations, and domain controller
- Process control network components (including routers, switches, and firewalls)

Experion server

Protection measure	For more information, refer to
Take steps to implement and enforce physical security.	"Physical and Environmental Considerations" on page 35
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	"Windows user accounts and passwords" on page 164
Ensure that your virus protection and Microsoft security hot fixes are up to date on all systems.	"Virus Protection" on page 47
Lock down the nodes in your system	"Honeywell High Security Policy" on page 167

Experion Station

Protection measure	For more information, refer to
Take steps to implement and enforce physical security.	"Physical and Environmental Considerations" on page 35
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	"Windows user accounts and passwords" on page 164
Ensure that your virus protection and Microsoft security hot fixes are up to date on all systems.	"Virus Protection" on page 47
Lock down the nodes in your system	"Honeywell High Security Policy" on page 167
Ensure Station security.	"Station security" on page 185

Domain controller

Protection measure	For more information, refer to
Take steps to implement and enforce physical security.	"Physical and Environmental Considerations" on page 35
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	"Windows user accounts and passwords" on page 164
Ensure that your virus protection and Microsoft security hot fixes are up to date on all systems.	"Virus Protection" on page 47

Network components

Protection measure	For more information, refer to
Take steps to implement and enforce physical security.	"Physical and Environmental Considerations" on page 35
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	"Windows user accounts and passwords" on page 164

3.6 System performance and reliability

Protection measures	For more information, refer to
Do not allow port scanning within the process control network (PCN).	“Port scanning” on page 121
Do not automatically schedule full system antivirus scans on Experion nodes.	“Configure active antivirus scanning” on page 50

4 Developing a Security Program

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

Related topics

“Forming a security team” on page 22
“Identifying assets to be secured” on page 23
“Identifying and evaluating threats and vulnerabilities” on page 24
“Creating a mitigation plan” on page 25
“Implementing change management” on page 26
“Planning ongoing maintenance” on page 27
“Security response team” on page 28

4.1 Forming a security team

While forming a team you must perform the following:

- Define executive sponsors. It is 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 (for example, the process control network administrator)
  - Business applications
  - IT system administration
  - IT network administration

4.2 Identifying assets to be secured

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.

Consider the following while identifying assets that are at risk.

- 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 computing equipment (databases) and other intellectual property

4.3 Identifying and evaluating threats and vulnerabilities

You must 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.

The following potential threats must be considered.

- 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.

The potential vulnerabilities that must 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 can also use failure mode analysis to assess the robustness of your network architecture.

4.4 Creating a mitigation plan

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

You must also perform risk assessments on your process control system equipment. A full inventory of your assets helps in identifying threats and vulnerabilities. Risk assessment helps you decide whether you can ignore, mitigate, or transfer the risk.

4.5 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 must 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 may also be required.

4.6 Planning ongoing maintenance

Constant vigilance of your security position must involve the following:

- 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 (refer to “Implementing change management” on page 26).
- The creation of an Incident Response Team (refer to “Security response team” on page 28).

Additional security resources

You must also be proactive about security by reviewing additional security resources, for example:

Resource	Location
Honeywell Process Solutions (HPS) web site	http://www.honeywellprocess.com (In the **Quick Links** column select **Security & Other Updates**. Now click **Microsoft Security Updates**.)
Microsoft	http://www.microsoft.com/technet/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	http://www.isa.org Choose Standards. Then choose *ISA99 Security Guidelines and User Resources for Industrial Automation and Control Systems, 3nd Edition*.

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.

4.7 Security response team

The responsibilities of a security response team (SRT) might include:

- Monitoring the Microsoft and Honeywell software update sites.
- Monitoring the antivirus software updates.
- Assessing risk for each security update, antivirus update, and any other update, 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 hot fixes 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 SRT determines that an update is so important that you cannot wait for Honeywell's verification cycle and so, you must verify and install it early on all of your systems.
- Ensuring the deployment of qualified security updates on the Experion servers and dedicated (control room) Station clients. Note that the corporate IT policy for updating Windows computers must be sufficient for the rotary Station and engineering computers.
- Checking that Microsoft Baseline Security Analyzer is run periodically to ensure that security updates have not been missed. For details, refer to "Using Microsoft Baseline Security Analyzer" on page 125.
- Reviewing network infrastructure patches and configuration changes that help to secure the network against the latest methods of attack.

5 Disaster Recovery

This chapter describes planning considerations for backup and restore policies and the tools that are supported for backing up and restoring your Experion system.

Related topics

“Formulating a disaster recovery policy” on page 30
“Backup and recovery tools for Experion” on page 31
“About Experion Backup and Restore” on page 32
“Planning considerations for Experion backup and restore” on page 33

5.1 Formulating a disaster recovery policy

As part of your security strategy, you must define a comprehensive backup and restore policy for disaster recovery purposes. Consider the following for formulating this policy.

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

5.2 Backup and recovery tools for Experion

To back up your Experion system, you must use the Experion Backup and Restore (EBR), a separately licensable Experion option.

For detailed information about backup strategies and specific instructions for backing up your Experion system using these tools, refer to the *Experion Backup and Restore Guide*.

5.3 About Experion Backup and Restore

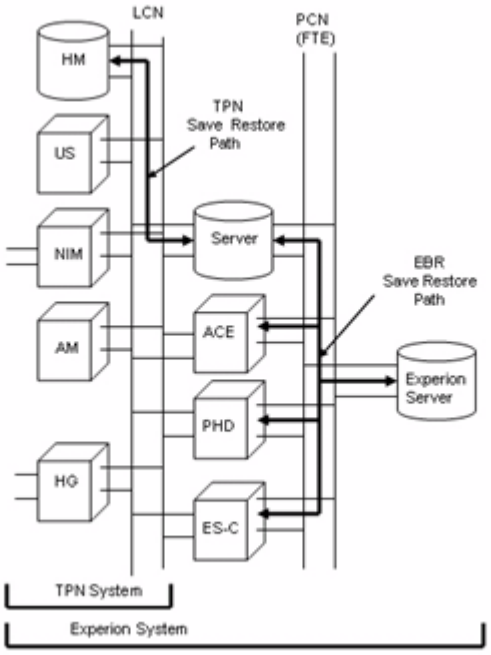
A key feature of the Experion Backup and Restore option is the ability to provide an image-based backup while the node is operational. The backup image can then be the basis for a rapid node recovery.

With Experion Backup and Restore, you can perform partial or total restore of your disk images as required by your system condition. Experion Backup and Restore can also be used to restore individual folders and files. The backup image can be used to return your computer to a previous working state with the operating system, applications, and data files intact.

With Experion Backup and Restore, you can perform the following tasks.

- Select nodes and databases that are part of the Experion Backup and Restore backup and restore environment.
- Determine what is backed up on a node and where the backup image is stored in the Experion system.
- Configure backups, backup schedules, and options.
- Manually perform a backup.
- Monitor the status of backup jobs.
- Manage the backup repository.
- Archive/export backup images to CD, DVD, or a network drive to allow you to store backup images and data in a secure temperature controlled location.
- Restore drive images, files, and folders.
- Restore archived images from CD, DVD, or a network drive.

The following image is a simplified diagram that illustrates the relationship between the Experion System, and the Experion Backup and Restore save, and restore path. In this illustration, the information from the Experion nodes is backed up onto a server. Using the Experion Backup and Restore tool, you can specify the drive images of the Experion nodes that are stored in the Experion server.



5.4 Planning considerations for Experion backup and restore

When planning the implementation of Experion Backup and Restore, ensure that the following rules and guidelines are followed.

- The network location used as the destination for the backup images must not be an Experion server or PHD server.
- Experion Backup and Restore must be installed on both the servers of a redundant pair to be backed up. In the event of a failure, a backup created on one of the servers cannot be used for recovering the other server. A license is required for each of the server machines to be backed up.
- Experion Backup and Restore supports only Honeywell nodes and Windows domain controllers used for an Experion platform. If you need to back up non-Honeywell nodes, purchase separate Acronis Backup and Recovery licenses.
- Do not use separately licensed versions of Acronis Backup and Recovery to back up and restore Honeywell nodes. While Experion Backup and Restore is based on Acronis Backup and Recovery technology, it includes additional components and is tested to ensure backup integrity of Honeywell nodes. Honeywell does not support directly purchased versions of Acronis Backup and Recovery (which are not part of EBR) as they do not have additional components required for Experion.
- The License server manages Acronis licenses. When installing an Acronis software package, specify the license server. The installer fetches licenses from the Acronis License Server. Acronis Backup and Recovery agent connects to Acronis License Server every time the agent service starts and every few days, as specified in the agent configuration parameters.
- Install the Experion Backup and Restore Manager on a dedicated server machine. Experion Backup and Restore Manager is not recommended on a domain controller, Experion server, PHD server or APP node. Instead, Honeywell recommends EBR Manager to be installed on a file server that is also the repository for the backup images.

Backing up TPN systems

If your system contains Local Control Network (LCN) nodes, you must use the TPN Save Restore tool to back up the LCN History Module (HM) to an LCN-connected server as illustrated in the image in section “About Experion Backup and Restore” on page 32. The back up of LCN History Module (HM) must be done before you use Experion Backup and Restore to back up the remainder of the system. Using the TPS/TPN Save Restore tool as the first part of your backup strategy ensures that you have a complete backup of your system.

The TPS/TPN Save Restore tool can perform automatic check pointing before the tool begins backing up the HM to ensure that you have the latest information. For a description of the TPN Save Restore tool, refer to the *TPS/TPN Backup and Restore User's Guide*.

6 Physical and Environmental Considerations

Although the security issues for Experion 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) is rendered inoperable.

Related topics

“Physical location” on page 36
“Protecting against unauthorized system access” on page 37
“Control room access” on page 38
“Network and controller access” on page 39
“Reliable power” on page 40

6.1 Physical location

It is important to consider the environmental factors for addressing the security needs of your system and data.

For example, if a site is dusty, you must place the server and network equipment 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. And if vibration is likely to be a problem, you must mount the server on rubber to prevent disk crashes and wiring connection problems. In addition, you must provide stable temperature and humidity for the server and network equipment, as well as, for network 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 must be chained to the furniture, and the case locked and closed.

If computers are readily accessible, and 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 must also consider disabling or physically protecting the power button to prevent unauthorized use. For maximum security, the server must be placed in a locked area and the key must be protected. Network equipment must be placed in a cabinet or locked closet to protect against unauthorized access to the power, console ports, and network ports.

If you are required to connect an Experion USB dongle (security key) to a server, protect it from being removed. If the server, or control room Stations have any unused USB ports, disable them to prevent memory sticks or other uncontrolled devices from being connected to the system. Such devices may be used to introduce virus or other malware.

6.2 Protecting against unauthorized system access

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

If there is an 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 of critical importance in relation to the nodes in your process control network that you prevent the use of all unauthorized removable devices and media such as CDs, DVDs, 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.
- Disabling USB ports and other ports capable of being used for memory sticks and other portable storage devices.
- Group policy may be used to prevent certain drive letters (floppy drive and CD drive) from being visible to Microsoft Windows Explorer. For instructions on how to do this, refer to the Microsoft article 231289 "*Using Group Policy Objects to hide specified drives*". Note, however, that this policy does not prevent users from using other programs to gain access to local and network drives or prevent users from viewing and changing drive characteristics by using the Disk Management snap-in.

6.3 Control room access

Providing physical security for the control room is essential to reduce the potency of many threats. Frequently, control rooms 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 also often contains 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.

6.4 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 and network equipment must 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 must be duplicated and laid in separate hardened cable runs.

6.5 Reliable power

Reliable power is essential, so you must 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.

Note that where you have redundant equipment such as redundant servers or redundant switches, you must also ensure that each unit in a redundant pair is on a different UPS or power source.

7 Microsoft Security Updates and Service Packs

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.

At the same time, it is important to bear in mind that 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.

Related topics

“Security updates” on page 42
“Honeywell's qualification of Microsoft security updates” on page 43
“Installing service packs” on page 44
“Distributing Microsoft updates and virus definition files” on page 45

7.1 Security updates

Microsoft releases a range of security updates and other operating system and software updates. Note that only Honeywell-qualified Microsoft updates are supported. Therefore, you must wait until Honeywell has validated Microsoft updates before installing them (refer to the section “Honeywell's qualification of Microsoft security updates” on page 43). It is also recommended that you implement a controlled system for the distribution of all updates (refer to the section “Distributing Microsoft updates and virus definition files” on page 45).

Timely information on security updates can be obtained by subscribing to the Microsoft Security Bulletin Summary at http://www.microsoft.com/technet/security/current.aspx

Attention

- If you have PHD nodes in your Experion system, you can (and must) install security updates and hot fixes on those nodes as soon as they are available.
- Before installing security updates on the critical nodes in your process control network, you should refer to Honeywell's Solution Support On-Line site (refer to the section “Honeywell's qualification of Microsoft security updates” on page 43 for instructions on navigating to the site). This site provides information on the status of qualified updates and hot fixes for Honeywell Process Solutions (HPS) products (that is, Experion , TPS, and Uniformance). For non-HPS products, you must refer to the supplier's security update rules.

7.2 Honeywell's qualification of Microsoft security 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 security updates and other updates for operating systems, Internet Explorer, and SQL Server products within a short period of time but generally only qualifies updates denoted as "Critical".

Contact your local Honeywell Technical Assistance Center (TAC) for Microsoft security updates, or go to the Honeywell Process Solutions (HPS) web site for a list of Microsoft security updates that have been qualified by Honeywell.

To access the Honeywell Process Solutions website

1. In a web browser, type the following URL.
   https://www.honeywellprocess.com/support

   The **Product Support** page appears.
2. If you are a new user, register at this website. Click **Register**, and follow the on-screen instructions.
3. If you are already registered, type your user name and password, and click **Login** to logon.
   Your account logon name appears in the top-right of the page.

To download and install hotfix

- In **Search Support Documentation**, type **hotfix**.
  The hotfixes and other non-security updates are displayed. These are the latest hotfixes from Microsoft that are approved for use in Experion.

  Attention
  To download the latest Experion patches, refer to the spreadsheet available at the following link http://www.honeywellprocess.com/library/support/software-downloads/Experion/experion-update-matrix.zip.

- Honeywell's **Microsoft Security Information** web page also provides links to a number of Microsoft sites that have information related to security hot fixes.
  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 following Microsoft web site is a prime source of information on current and past hot fixes.

  http://www.microsoft.com/technet/security/current.aspx

7.3 Installing service packs

A service pack is a tested, cumulative set of all security and other 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.

Honeywell's qualification of Microsoft service packs

Microsoft performs full integration testing of their service packs against the operating system and their own applications. Honeywell follows that with system integration testing of the service pack which in most cases are a part of a scheduled and planned release.

Note that only Honeywell-qualified Microsoft service packs are supported, and therefore wait until Honeywell has qualified the service pack prior to your own qualification testing.

Contact your local Honeywell Technical Assistance Center (TAC) for Microsoft security updates, or go to the Honeywell Process Solutions (HPS) web site for a list of Microsoft security updates that have been qualified by Honeywell.

To access the Honeywell Process Solutions website

1. In a web browser, type the following URL.
   https://www.honeywellprocess.com/support
   The **Product Support** page appears.
2. If you are a new user, register at this website. Click **Register**, and follow the on-screen instructions.
3. If you are already registered, type your user name and password, and click **Login** to logon.
   Your account logon name appears in the top-right of the page.

To download and install hotfix

- In **Search Support Documentation**, type **hotfix**.
  The hotfixes and other non-security updates are displayed. These are the latest hotfixes from Microsoft that are approved for use in Experion.

  Attention
  To download the latest Experion patches, refer to the spreadsheet available at the following link http://www.honeywellprocess.com/library/support/software-downloads/Experion/experion-update-matrix.zip.

- In any case you must 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.

7.4 Distributing Microsoft updates and virus definition files

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

It is, however, not best practice to distribute Microsoft security updates 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 an update manager and an antivirus server be located in the DMZ (refer to “The demilitarized zone” on page 92). 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 Microsoft update and antivirus 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 antivirus product that is supported by the process control equipment vendor is not the same as the antivirus product supported by the corporate IT department.

Attention

Honeywell qualifies Microsoft security updates and other updates. It is strongly recommended that Microsoft updates are not implemented until this qualification has been carried out (refer to “Honeywell's qualification of Microsoft security updates” on page 43 and Honeywell's qualification of Microsoft service packs).

8 Virus Protection

Related topics

8.1 Choose supported antivirus software

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

The following antivirus components have been qualified by Honeywell:

- **McAfee**
  - McAfee AV + VirusScan Engine + patch (8.7i + Engine 5400 + Patch3)
  - ePolicy Orchestrator + patch + Agent (ePO 4.5.0 + Patch1 + Agent 4.5.0.1270)
- **Symantec**
  - Symantec Endpoint Protection 11; Release Update 6a, supersedes RU6

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

Attention
Virus scanners other than McAfee VirusScan and Norton Anti-Virus may not be supported and may not work on Experion. For more information contact your Honeywell service center or TAC.

8.2 Installing antivirus software on process control nodes

Install antivirus software on every node in the process control network must include the following:

- In an Experion system:
  - Experion Stations (Flex Stations, Console Stations and Console Extension Stations, LCN-connected Stations)
  - Experion Server, LCN-connected servers, eServers
  - Application Control Environment (ACE) node
  - SIM-ACE and SIM-C300 nodes
  - Application Server (EAS)
  - APP node (E-APP)
- In a TPS system:
  - GUS nodes
  - Application Processing Platform (APP) nodes
- Other nodes:
  - Process History Database (PHD) servers
  - Advanced control nodes
  - Honeywell and third party application nodes
  - Non-Windows nodes
  - Subsystem interface nodes (for example, tank gauging).

It is recommended that you set up special servers for the controlled distribution of antivirus signature files to the process control network (PCN) as outlined in section “Distributing Microsoft updates and virus definition files” on page 45.

8.3 Configure active antivirus scanning

It is recommended that you adopt an active virus scanning strategy. For guidance on antivirus measures go to the Honeywell Process Solutions (HPS) web site.

In the HPS web site you find information about the following:

- Antivirus software that has been qualified by Honeywell
- Recommended antivirus strategies

The recommended strategies include ensuring that:

- Virus scan reports are regularly reviewed
- Antivirus software is configured to:
  - Scan the boot sectors of all floppy disks.
  - Move infected files to a quarantine directory and notify the user that an infected file was found. The user should be allowed to clean up the infection.

To access the Honeywell Process Solutions website

1. In a web browser, type the following URL.
   https://www.honeywellprocess.com/support

   The **Product Support** page appears.
2. If you are a new user, register at this website. Click **Register**, and follow the on-screen instructions.
3. If you are already registered, type your user name and password, and click **Login** to logon.
   Your account logon name appears in the top-right of the page.

To apply the latest antivirus notification

1. Use the **Search** toolbar to locate the latest notifications.
   Or

   In the **Latest Support Files**, click **Latest Notifications** link.

   The **All Notifications** page is displayed. This page lists the latest notifications.
2. If the notifications cannot be located in the list displayed, you can search using the **Search** toolbar.
3. To search with **Advanced** link, click the **Advanced** link in the **Search** toolbar.
   The **Advanced Support Document Search** page is displayed.
4. Type the details of the notification and click **Search**.
   The list of notifications with the required information is displayed.
5. Locate the required notification and click to open.

8.4 Tune the virus scanning for system performance

To formulate your virus scanning strategy, consider the potential impact on critical system resources.

For example, if your Experion is experiencing problems due to low system resources, you must perform the following:

- Ensure that the antivirus software (and other third party applications) is run only when system resources on the node are adequate to meet system needs.
- Consider limiting the system resources that are used by antivirus software during scanning. 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%.

To find the proper balance between server performance and virus protection you must make configuration choices such as disabling scanning on reading of files and changing the default process-based scanning to per-process scanning.

For more information about virus-scanning and system performance, refer to the section “About virus scanning and system performance”.

Attention

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

- Impact the ability of operators to respond to a situation, or
- Result in execution cycle overruns on an ACE node

Directories excluded from scanning

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

- *\Program Files(x86)\Honeywell\Experion PKS\Engineering Tools\system\er*
- *\Program Files (x86)\Microsoft SQL Server\MSSQL11.MSSQLSERVER*
- *\ProgramData\Honeywell*
- *\Program Files(x86)\Honeywell\Experion PKS\client\System*

The following table describes the list of Honeywell folders/files that do not support the custom installation path.

Media/package	Installation path	Comments
Init Media folder	*C:\ProgramData\Honeywell\Install \Init Media*	This folder is created by Experion System Initialization media, and is used for maintaining logs and configuration files. These files are only created during install time, not accessed during runtime.
Shared Software	*C:\Program Files(x86)\Common Files*	Common files shared across the software.
ErrLog1.txt	*C:\ProgramData\Honeywell\Experion PKS\ErrLog_1.txt*	Refer to the **ErrLog(s)** maintained at the custom installation path location.
TraceUI	*C:\ProgramData\Honeywell\TraceUI \DotNetSysMgmtDsp.txt*	Log for System Management Display tracing tool.
Crystal Report merge module folders	• *C:\css* • *C:\html* • *C:\images* • *C:\jss* • *C:\prompting*	These folders are created for Crystal reports during runtime.

About virus scanning and system performance

The Experion 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.

When tuning antivirus software, 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 antivirus scanners allow you to set maximum CPU usage. The default installation of antivirus software generally meets the demands of most customers. However, for systems with extremely high CPU usage and input/output demands, the default installation of antivirus software may impose system limitations. Please refer to your antivirus software documentation for specific procedures on how to limit CPU utilization.

If your system is experiencing continued resource-related performance problems, there are further steps that you can take to limit the resources consumed by antivirus software. For up-to-date and specific information, look up the web-site for your antivirus software.

8.5 Ensure frequent updates to antivirus signature files

Non-directed virus and worm attacks are common attacks on a control system. A virus that is deemed low risk for corporate systems may pose a high risk to a control system if it causes a denial of service. It is therefore essential to update antivirus signature files frequently by:

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

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.

For recommendations on distributing antivirus updates, refer to “Distributing Microsoft updates and virus definition files” on page 45.

8.6 Test the deployment of antivirus signature files

It is important to test antivirus signature files offline before deploying them. This helps to ensure that the signature file does not break the antivirus 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

In line with the best practice of minimizing communication between the business network and the process control network, it is recommended that updates to antivirus signature files be distributed from a server located in a DMZ as outlined in section “Distributing Microsoft updates and virus definition files” on page 45.

When implementing the automatic deployment of signature files, it is also important to:

- Stagger automatic deployment to eliminate the potential for common cause failure. For example, deploy to no more than three or four nodes per hour.
- Follow the recommendations of your antivirus software vendor for distribution server/services.
- Stage the distribution on a test system.

8.7 Prohibit email clients on the process control network

Do not install email clients on any node connected to the process control network. Honeywell does not support email clients on the process control network.

Viruses and email

Many viruses and similar malware propagate through 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, which may prevent the timely delivery of controls and alarms.

Instant messaging

An emerging trend is the use of instant messaging (IM) as a transport mechanism for malware. Targeting MSN clients in particular, the malware sends messages to all contacts on an infected machine, thereby increasing network traffic uncontrollably. This message itself, apparently from a trusted source, tells the recipient to browse to a malicious web site which then download more serious malware, opening back doors or otherwise allowing takeover of the machine. It is possible that IM replaces email as the prime carrier of malware in the near future.

Honeywell strongly advises against supporting instant messaging on nodes within the process control network (PCN).

8.8 Spyware

An increasingly common threat is that posed by spyware, also known as "bots." These are typically small modules that do not in themselves cause damage, but record keystrokes and other user actions, and then transmit this information to a remote host, where passwords, account, and other information can be extracted.

Conventional antivirus checkers do not look for spyware. Like viruses and other malware, spyware can be propagated through email or inadvertently downloaded in the course of Internet access.

Note that Honeywell does not support internet and email access from the PCN.

9 Network Planning

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

- *Overview* describes the basic concepts and terminology as well as the capabilities of an Experion process control network.
- *Server and Client Planning Guide* contains planning information for Experion, including information about distributed systems architecture (DSA), server redundancy, and data exchange. Refer to the "Networks" section in the *Server and Client Planning Guide*.
- *Experion Mobile Access User's Guide* contains planning information for networks using Experion Mobile Access.
- Windows Domain and Workgroup Implementation Guide. For planning information, refer to Windows Domain and Workgroup Planning Guide. For operation system migration information, refer the appropriate operating system-specific implementation guide Windows Domain Implementation Guide for Windows Server 2008 R2/Windows Domain Implementation Guide for Windows Server 2012. contains information and recommendations to assist you in setting up a domain controller and workgroups for your Experion system.

10 Planning EtherNet/IP implementation

Starting with Experion R430, an efficient EtherNet/IP interface has been introduced. The EtherNet/IP (EIP) interface facilitates a comprehensive integration between the C300 controllers and the EtherNet/IP-compatible nodes and I/O devices, which are installed on the network. It also provides an efficient integration between the C300 and the ControlLogix Control system. EIP is only supported in high capacity topology or deployment of Experion.

In addition to the "Related documents" on page 12 section, refer to the following documentation resources before you start the planning and design activities:

- The *Overview* document and the *Control Building User's guide* for more information about the integration between C300 and EtherNet/IP-compatible I/O devices.
- *C300 Controller User's guide* for more information about the planning and design activities of the C300 Controller.

Additionally, the following sections provide more information to help you plan and design an EtherNet/IP interface for the integration between C300 and the EtherNet/IP-compatible devices:

- "Network requirements" on page 60
- "EtherNet/IP implementation architecture and topology" on page 63
- "Tofino firewall configuration" on page 76
- "Configuring the Stratix switch for EtherNet/IP integration" on page 68

Related topics

"Network requirements" on page 60
"EtherNet/IP implementation architecture and topology" on page 63
"Configuring the Stratix switch for EtherNet/IP integration" on page 68
"Switch Maintenance" on page 75
"Tofino firewall configuration" on page 76
"Software and hardware requirements for Tofino firewall configuration" on page 77
"Configuring the Tofino firewall" on page 78

10.1 Network requirements

The following table lists the hardware and software components required for the EtherNet/IP implementation.

Hardware components

Component	Supported type/version	Description
CISCO switches	2960 and above	Level 2 CISCO switches For more information about configuring Level 2 CISCO switches, see *Fault Tolerant Ethernet Overview and Implementation Guide*.
Tofino security appliance	TSA 100 For more information about the required hardware and software requirements for Tofino firewall configuration, see “Software and hardware requirements for Tofino firewall configuration” on page 77.	The Tofino Industrial Security Solution helps in providing a secure communication on the industrial control network. It is a distributed network security solution. The Tofino security appliance is a security device, which is connected to the Level 2 CISCO switches and the Stratix Switch. For more information about the Tofino firewall and configuring the Tofino firewall, see: • “Tofino Security” • “Tofino firewall configuration” on page 76
Stratix switch	Stratix 8000	• The Stratix switch is used for connecting the EtherNet/IP-enabled devices to the C300 controller through the Tofino firewall and the CISCO switches. • The Stratix switch is also used for connecting the ControlLogix PLC and the C300 controller. For more information about Stratix switches, see the “Rockwell Literature Library”. For more information about configuring Stratix switches, see “Configuring the Stratix switch for EtherNet/IP integration” on page 68
ArmorPoint adapter	ArmorPoint 1738-AENT adapter	For more information about installing and configuring the ArmorPoint 1738–AENT adapter, see the “Rockwell Literature Library”.

Component	Supported type/version	Description
ArmorPoint I/O modules	• ArmorPoint 1738-IB4DM12 • ArmorPoint 1738-IB8M12 • ArmorPoint 1738-IE2CM12 • ArmorPoint 1738-IE4CM12 • ArmorPoint 1738-IR2M12 • ArmorPoint 1738-IT2IM12 • ArmorPoint-1738-OA2M12AC3 • ArmorPoint 1738-OB2EPM12 • ArmorPoint 1738-OB8EM12 • ArmorPoint 1738-OE2CM12 • ArmorPoint 1738-OE4CM12	• For more information about the supported I/O modules of the ArmorPoint family, see EtherNet/IP device configuration in the *Control Building User's Guide*. • For more information about installing and configuring the EtherNet/IP-compliant ArmorPoint I/O devices, see the "Rockwell Literature Library".
ArmorBlock I/O modules	• ArmorBlock 1732E-IB16M12DR • ArmorBlock 1732E-IF4M12R • ArmorBlock 1732E-IR4IM12R • ArmorBlock 1732E-IT4IM12R • ArmorBlock 1732E-OF4M12R	For more information about installing and configuring the EtherNet/IP-compliant ArmorBlock I/O devices, see the "Rockwell Literature Library".
PowerFlex Drives	PowerFlex 755	For more information about installing and configuring the PowerFlex 755 drive, see the "Rockwell Literature Library".
Adapter for E3 and E3 plus relays	193-DNENCATR	For more information about installing and configuring the 193-DNENCATR adapter, see the "Rockwell Literature Library".
Relays	E3 and E3 plus	For more information about installing and configuring the E3 and E3 plus relays, see the "Rockwell Literature Library".
ControlLogix PLC	5572 and 5555	For more information about installing and configuring the ControlLogix PLC, see the "Rockwell Literature Library".
EtherNet/IP Tap (ETAP)	1783–ETAP	The 1783 ETAP can be used as a Ring Supervisor and also as a non-supervisor. For more information about installing and configuring the 1783 ETAP, see the "Rockwell Literature Library".
Drive Explorer		The DriveExplorer is an easy-to-use application, which is used for online configuration of PowerFlex drives and communication adapters. It is also used for monitoring purposes. For more information about DriveEplorer, see: • "Rockwell Literature Library" • "DriveExplorer"
Allan Bradley OPC Server from MatrikonOPC		The MatrikonOPC Server for Allen Bradley PLCs enables data interchange between OPC clients and Allen Bradley-compliant devices. For documentation about installation and configuration, see *MatrikonOPC Server for Allen Bradley PLCs Online Help*.

Attention

Ensure that there are no duplicate IP nodes on the network. If the IP address of an existing EtherNet/IP I/O on the network is assigned to another EtherNet/IP I/O device, which is connected to the Uplink port of the L2 switch, the existing EtherNet/IP I/O device loses its communication with the C300.

10.2 EtherNet/IP implementation architecture and topology

Starting with Experion R430, the C300 controller supports EtherNet/IP (EIP). The EtherNet/IP supportability facilitates the following:

- Integration between C300 and the ControlLogix control system
- Communication between C300 and the EtherNet/IP-compatible third-party devices, such as I/Os, drives, and relays

Supported topologies

The EtherNet/IP-I/O devices, drives, and relays can be set up in one of the following network topologies:

- Ring topology — The nodes of the network are connected in a circular mode, forming a ring.
- Linear bus topology — The nodes of the network are connected to a common communication media.
- Star topology — The nodes of the network are connected to a central hub.

The topology can also be a hybrid setup with a combination of star, linear bus, and ring topologies.

A Device-level ring topology is recommended because it provides a network that is single-fault tolerant.

In an EtherNet/IP implementation setup, the ring network includes the following components:

- EtherNet/IP-compatible I/O devices, drives, and relays
- Ring supervisor
- ETAP modules for single port devices

One of the 1783 EtherNet/IP TAP (ETAP) is configured as the Ring supervisor, which is connected to the Stratix switch. The Ring supervisor is an important component on the ring network because it is used as the connection media between the EtherNet/IP-compatible devices and the Stratix switch. Therefore, if the connection between the Ring supervisor and the Stratix switch is lost, the connection from the I/O devices to the C300 controller will be lost.

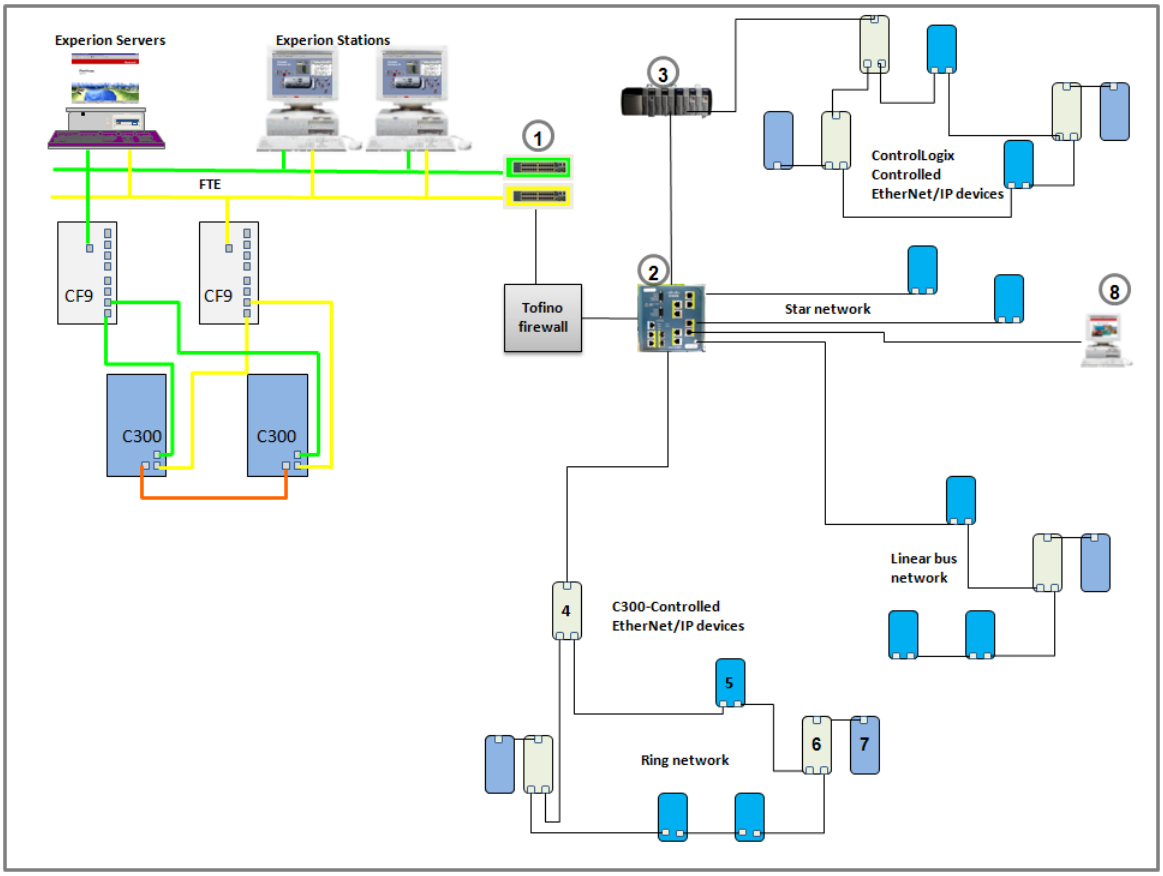
The 1783-ETAP modules are also used to connect single-port devices on the ring and linear bus network.

Attention

Experion SCADA access for ControlLogix tags using Matrikon OPC server will also work in this topology. Matrikon OPC requires the Allen Bradley via Ethernet/IP driver for communication. Refer to the SCADA access guide.

EtherNet/IP implementation architecture and topology

The following figure depicts the EtherNet/IP implementation architecture:



Item	Graphic	Description
2		Stratix Switch
3		ControlLogix Controller
4		Ring Supervisor – ETAP configured as ring supervisor
5		Dual port EtherNet/IP device
6		ETAP

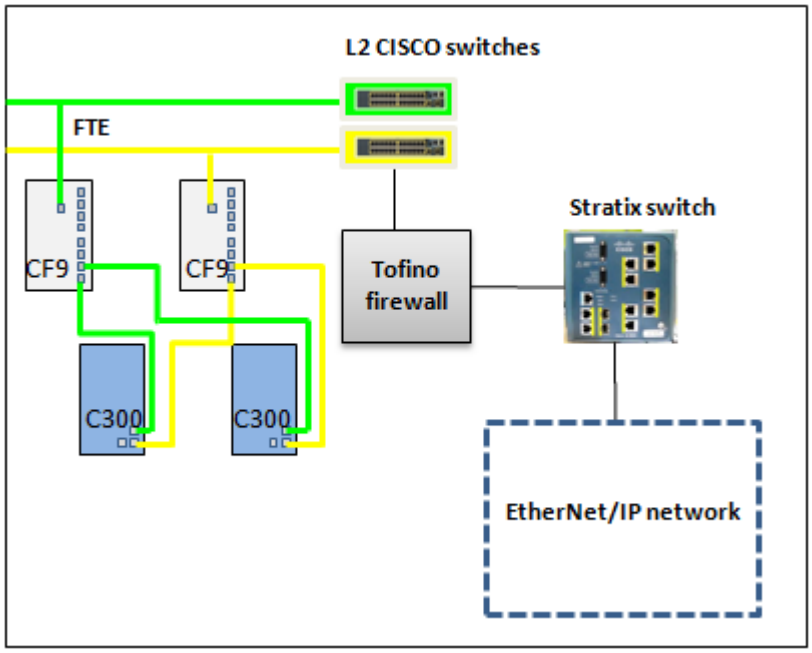
Item	Graphic	Description
7		Single port EtherNet/IP device
8		Computer with Third party software installations

The preceding graphic represents the following entities on the network:

- The Experion system on the FTE network
- The C300 controllers and the Level1 switch
- Tofino firewall
- Stratix switch
- The EtherNet/IP I/O devices on an EtherNet/IP network
- The ControlLogix PLC on an EtherNet/IP network
- Computer to install third-party tools

The following components on the EtherNet/IP network help in the integration of C300 with the EtherNet/IP-compatible I/O devices and the integration of C300 with the ControlLogix PLC:

- Level 2 CISCO switches — The level 2 CISCO switches provide a connectivity medium for C300 and the EtherNet/IP-compatible I/O devices on the EtherNet/IP network.

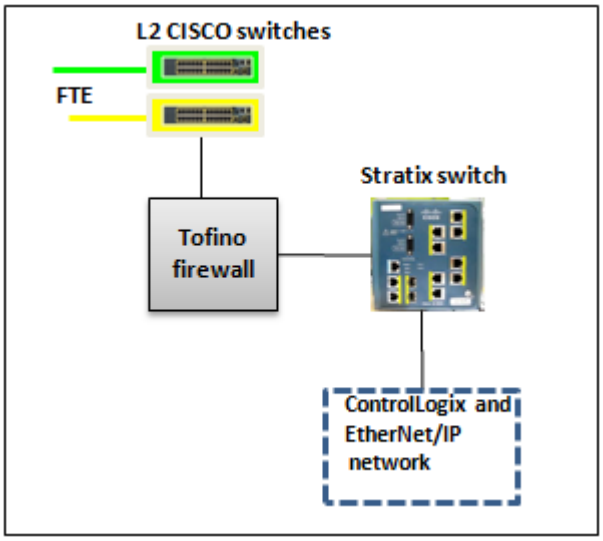


The EtherNet/IP network must be connected to the yellow CISCO switch. The components are connected as follows, as shown in the figure:

– C300 controllers are connected to CF9
– The CF9 devices are connected to the CISCO switches on level 2
– Additionally, the connections from the EtherNet/IP-compatible I/O devices connected to the Stratix switch converge to the CISCO switch through the Tofino firewall.

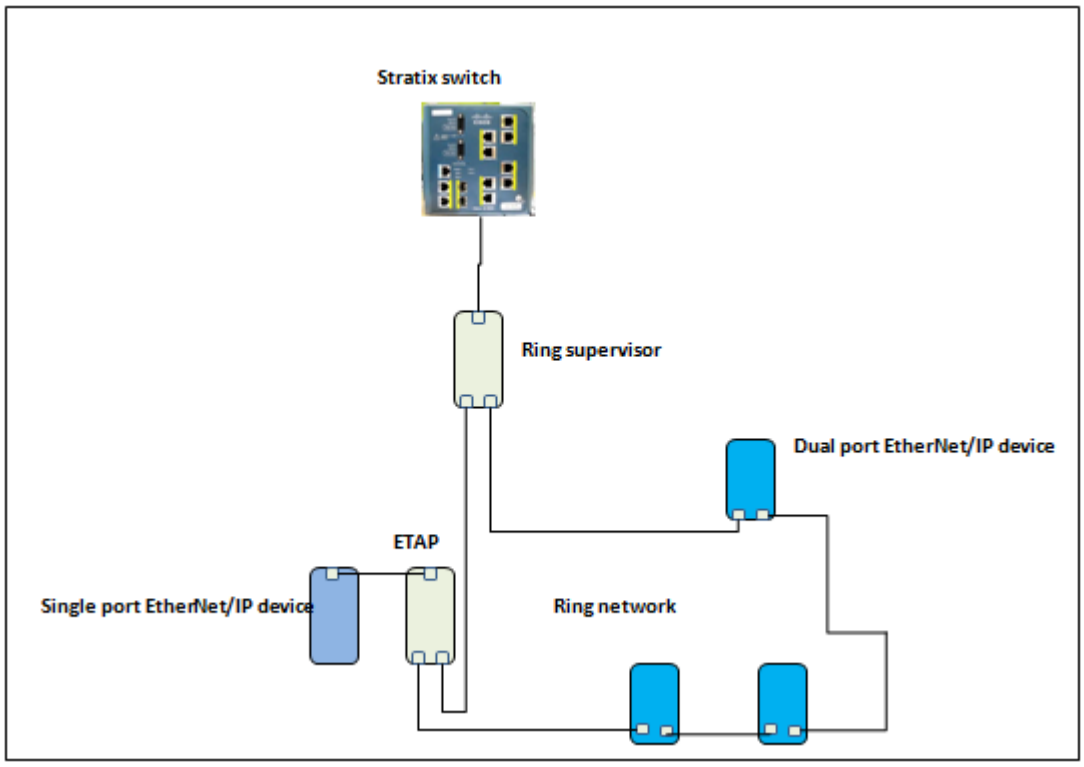
For more information about configuring the Level 2 CISCO switches, see *Fault Tolerant Ethernet Overview and Implementation Guide*.

- Tofino firewall — The Tofino firewall is used as a security solution to ensure a secure communication on the network. The Tofino security appliance is added to allow only the EtherNet/IP traffic to and from the L2 Switches. You can define firewall rules, specify the devices that are allowed to communicate, and specify the protocols that can be used. The Tofino firewall is connected to the Stratix switch. For more information about Tofino firewall configuration, see “Tofino firewall configuration” on page 76
- Stratix switch — The Stratix switch is used for connecting the EtherNet/IP-compatible I/O devices and the ControlLogix PLC to the C300 controllers. It connects to the C300 through the level 2 CISCO switches. The following components are connected to the Stratix switch:



  - The I/O devices, drives, and relays
  - The ControlLogix PLC
  - Computer in which third-party tools are installed

  For more information about the Stratix switch configuration, see “Configuring the Stratix switch for EtherNet/IP integration” on page 68.
- Ring Supervisor — The Ring supervisor is a part of the EtherNet/IP devices. The Ring supervisor connects to the Stratix switch. The Ring supervisor is an important component on the ring network because it is used as the connection media between the EtherNet/IP-compatible devices and the Stratix switch.



- ETAP— The 1783-ETAP modules are used to connect single-port devices to a ring or linear bus network.
- Computer to install third-party tools — You can use the computer to install third-party tools that are required. For example: DriveExplorer, and web access to EtherNet/IP I/O devices.

ControlLogix-controlled EtherNet/IP devices — The EtherNet/IP IO devices controlled by the ControlLogix must not be directly connected on the Stratix switch. These devices must be configured under the Control Logix chassis through a downlink EtherNet/IP module. For more information about configuring EtherNet/IP devices for the ControlLogix PLC, see the ControlLogix documentation in the “Rockwell Literature Library (http://literature.rockwellautomation.com)” .

10.3 Configuring the Stratix switch for EtherNet/IP integration

Stratix switch 8000 with IOS firmware revision 15.0 is used for connecting the EtherNet/IP-compatible I/O devices and the ControlLogix PLC to the C300 controllers. For more information about Stratix 8000, see Rockwell Literature Library

Perform the following tasks to install the switch configuration files to the node, and configure the Stratix switches for EtherNet/IP integration. Use the command line interface of the switch and the correct switch startup configuration file to perform the following tasks.

Prerequisites

Before beginning the procedures in this section, ensure that you verify the following:

- You have an RS-232 cable configured, as required by the switch vendor, to connect the computer's serial port to the communication port of the switch.
- You have downloaded HyperTerminal and Telnet is enabled on the operating system used as the interface to the switch.
- You have reviewed the Stratix switch documentation at Rockwell Literature library.

To configure the Stratix switch for EtherNet/IP integration

1. Connect to the switch. See "Connecting locally to the switch" on page 68.
2. Verify the Stratix switches have the IOS version qualified by Honeywell as listed in the SCN for your release. See "Checking the version of the switch IOS" on page 69.
3. Configure the switch. See "Configuring switch interface options" on page 70
4. Load the switch configuration file. See "Loading the switch configuration file" on page 73

Related topics

"Connecting locally to the switch" on page 68
"Checking the version of the switch IOS" on page 69
"Accessing switch configuration files" on page 69
"Configuring switch interface options" on page 70
"Loading the switch configuration file" on page 73

10.3.1 Connecting locally to the switch

Perform the following procedure to connect to the switch and start HyperTerminal.

Attention
Do not turn on the switch until instructed to do so.

To connect locally to the switch

1. Connect the RS-232 cable to the communication port of the switch and the computer's serial port.
2. Click **Start** > **All Programs** > **Accessories** > **Communications** > **HyperTerminal**.
3. On the **Connection Description** dialog box, specify a name that describes the connection and click **OK**.
4. In the **Icon** box, click the appropriate icon, and click **OK**.
5. On the **Connect To** dialog box, select the serial port used by the computer from the **Connect Using** box and click **OK**.
6. From the **Connect To** dialog box, select the serial port being used by the computer and click **OK**.

7 From the **Properties** page, configure the following port settings:
- Bits per second: 9600
- Data bits: 8
- Parity: NONE
- Stop bits: 1
- Flow control: NONE

8 Click **OK**.

Results

The switch is connected.

10.3.2 Checking the version of the switch IOS

Switches with unqualified IOS have unpredictable performance. Therefore, perform the following procedure to check the IOS version. Stratix 8000 is tested and qualified for EtherNet/IP with IOS firmware revision 15.0.

Prerequisites

Ensure that you have downloaded and installed the HyperTerminal application.

To check the version of the Stratix switch IOS

1 Open Hyper Terminal and log in to the switch.

2 Run the following command to check the IOS version:

```
show boot
```

If the IOS version is not qualified by Honeywell as listed in the SCN, contact Honeywell Network Services for the procedure to upgrade the IOS.

Results

The version of the IOS is displayed.

10.3.3 Accessing switch configuration files

Switch configuration files are packaged with the FTE driver and are copied to the following location when you run the FTE driver installation package.

\Honeywell\FTEDriver\SwitchConfigurationFiles\stratix 8000

If you have not installed FTE, access the switch configuration files from the Experion PKS Installation media at the *Media Drive:\FTEDriver\SwitchConfiguration* location. After connecting to the switch, use the command line interface (CLI) of the switch to configure the switch options. If the switch does not respond, press ENTER and wait for the prompt (>) to appear. The following table lists the conventions used in the switch configuration procedures and examples.

Convention (Example)	Description
`Enter host name [Switch] :`*`Stratix_EIP`*	Text in the terminal display appears in the following font: `commands`
`Stratix_EIP#`**`config t`**	Values that are entered by the user are in **bold**.
`Stratix_EIP(config)#`**`int`** *`vlan1`*	Arguments for which the user provides the required inputs are **bold** and *italicized*.

Convention (Example)	Description
`Press RETURN to get started! <ENTER>`	Non-printing characters, such as passwords or Enter key are in angle brackets (<>).

10.3.3.1 Switch configuration files for the Stratix 8000 switch

The following are the Stratix switch configuration files, which are located at: *\Honeywell\FTEDriver\SwitchConfigurationFiles\stratix 8000*

Stratix switch configuration file	Port information
eip_stratix8000_1u_8.txt	This file is for the Stratix 8000 switch, which contains 8 ports. • 1 uplink port configuration • 2 ETAP port configurations • 5 ports are configured for connecting EIP IO Devices
eip_stratix8000_1u_16.txt	This file is for the Stratix 8000 switch, which contains 16 ports. • 1 uplink port configuration • 2 ETAP port configurations • 13 ports are configured for connecting EIP IO Devices
eip_stratix8000_1u_24.txt	This file is for the Stratix 8000 switch, which contains 24 ports. • 1 uplink port configuration • 2 ETAP port configurations • 21 ports are configured for connecting EIP IO Devices

10.3.3.2 Stratix switch port and connection speeds

The following table summarizes the switch port and connection speeds for the Stratix switch.

Switch port	Requirement	Comment
EtherNet/IP IO devices ports	• Port fast spanning tree is enabled • Speed is set to auto with full duplex	• Helps in connecting EtherNet/IP devices • Helps in quick reconnection
EtherNet/IP ETAP ports	• Port fast spanning tree is enabled • Speed is set to auto with full duplex	• Helps in connecting ETAP for making a Ring or a Linear bus network • Helps in quick reconnection
Uplink ports	• Spanning tree is enabled. • Speed is set to 100 Megabit and full duplex.	• Helps in connecting the downlink port of the Tofino firewall • Helps to connect to another EtherNet/IP Stratix switch

10.3.4 Configuring switch interface options

The procedures in this section describe how to enable the configuration dialog and set the basic management setup in the switch. Additionally, it also describes how to set up the switch IP address. Establishing an IP address allows you to use Telnet and FTP sessions to save and restore configuration options.

Attention

The procedures in this section contain multiple instances of switch display for reference. The text in the switch display instances are formatted as follows:

- The commands and some of the options in the switch display instances are formatted bold. Therefore, the text in bold should be typed as it appears.
- Sample inputs that must be provided by the user are formatted bold and italicized (For example: ***Stratix_EIP***). Ensure that you specify an appropriate value that matches your requirement.
- Press the Enter key after you type the required command or option.

To configure the switch interface options

1 When the following display appears, specify the required values.

```
Would you like to enter the initial configuration dialog?
[yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: y
Configuring global parameters:
```

The host name is unique for each switch. The following values are used as examples in this procedure:

Option	Example
host name	Stratix_EIP
enable secret	Stratix_EIP1
virtual terminal password	EIP1
enable password	Stratix_EIP1

2 When the following display appears, specify the required details.

The following is an example for your reference. Press the Space bar to advance the display when it pauses.

```
Enter host name [Switch] :Stratix_EIP

The enable secret is a password used to protect access to privileged EXEC and configuration
modes. This password, after entered, becomes encrypted in the configuration.
Enter enable secret: Stratix_EIP1

The enable password is used when you do not specify an enable secret password, with some older
software versions, and some boot images.
Enter enable password:EIP1

The virtual terminal password is used to protect access to the router over a network
interface.
Enter virtual terminal password: Stratix_EIP1

Configure SNMP Network Management? [no]: N
```

3 After the configuration display is complete, the switch dialog appears. Specify the required values.

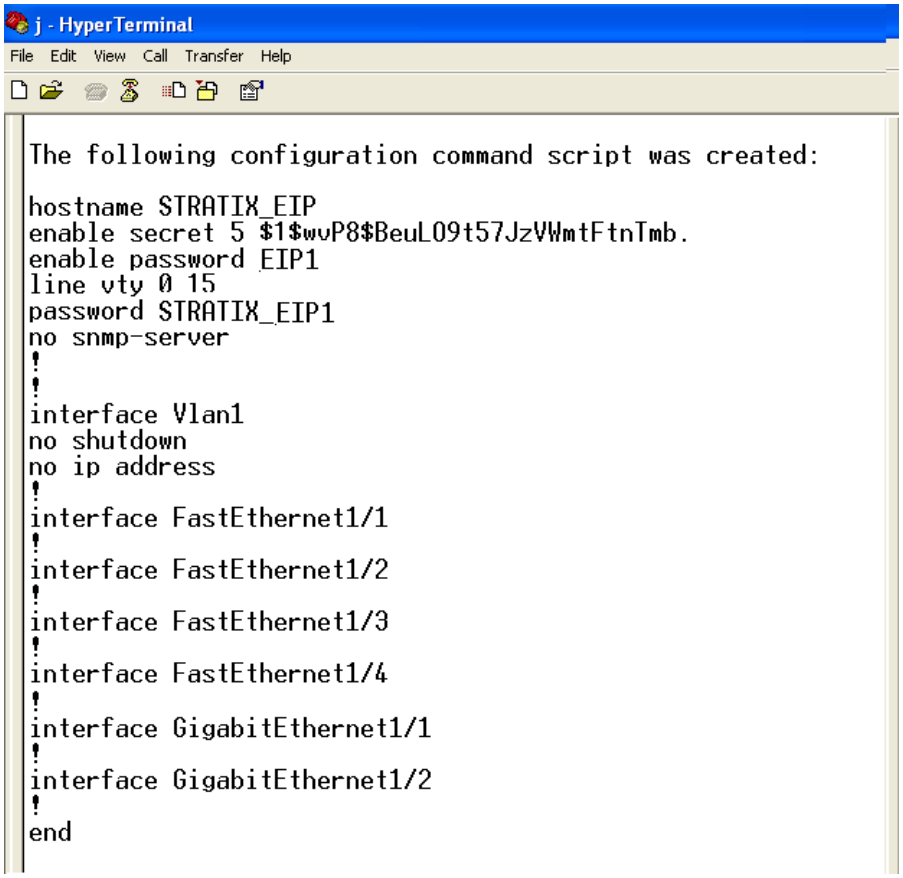
```
Enter interface name used to connect to the management network from the above interface
summary :vlan1

Configuring interface Vlan1:

Configure IP  on this interface ? [yes/no]: N

Would you like to enable as a cluster command switch? [yes/no]: N
```

The following is an abridged example of what displays after the VLAN1 configuration. Press the SPACE BAR to advance the display when it pauses.



4 After the configuration display is complete, the following switch dialog appears. Type 2 and press ENTER to save the switch configuration.

```
[0] Go to the IOS command prompt without saving this config
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
```

Setting up the IP address for the switch

1 Use the enable command and the enable secret string that was established earlier, in the procedure. Stratix_EIP1 is used in the following example. Specify the required values.

```
Press RETURN to get started! <ENTER>

Stratix_EIP>enable
Password: Stratix_EIP1

Stratix_EIP#config t

enter configuration commands, one per line. End with CNTL/Z
```

2 If you have to use VLAN 101, initialize VLAN 101 by performing the following additional steps:

1. Type the following:

   ```
   vlan 101
   ```

2. Type the following:

   ```
   exit
   ```

Otherwise, go to the next step.

3 To enable Telnet and FTP, run one of the following commands:

- To configure VLAN1, type:

  ```
  int vlan1
  ```

- To configure VLAN101, type:

  ```
  int vlan101
  ```

```
Stratix_EIP(config)#int vlan1
```

4 The following is used for the IP address and subnet mask in the following switch display.

```
10.1.4.253 255.255.255.0
```

```
Stratix_EIP(config-if)#ip address10.1.4.253
255.255.255.0
Stratix_EIP(config-if)#no shutdown
Stratix_EIP(config-if)#exit
```

5 Type **exit** and type **write**.

The switch option configuration is complete. You can now download the appropriate switch configuration file.

10.3.5 Loading the switch configuration file

The following procedure uses the Xmodem file transfer utility of Hyperterminal to transfer the correct switch configuration file to the switch. After downloading the switch configuration file, write the configuration back to the switch memory.

To determine the most appropriate switch configuration file for your system, see “Switch configuration files for the Stratix 8000 switch” on page 70

To load the switch configuration files

1 Initiate the transfer in the switch by using the copy command. Type all values that appear in bold.

```
Stratix_EIP#copy xmodem: system:running-config
```

2 To initiate the transfer from the Hyperterminal, select **Transfer** > **Send File**.

3 Click Browse and navigate to the Switch Configuration folder in one of the following locations:

- C:\Program Files\Honeywell\FTEDriver\SwitchConfigurationFiles\stratix 8000\
- Media Drive:\Packages\FTE_Driver\Switch_Configuration_Files\

- Location you saved the files

4 Select the correct switch configuration file and click **OPEN**.

5 Select **Xmodem** under Protocol.

6 Click **Send** to start the file transfer.

> **Attention**
> If there is an existing file with the same name, type y to overwrite the file. If there is a problem during the transfer, error messages are displayed, fix the problem with the switch configuration file and perform steps 2 to 7.

A message indicating that the file is copied is displayed.

7 Write the basic switch configuration file and the switch configuration file you downloaded back to the switch memory by running the following command:

```
Stratix_EIP#write
```

8 Run the following command to view the switch configuration options:

```
Stratix_EIP#sho run
```

The options are displayed based on the switch configuration file. For example,

- 1 uplink
- 2 ETAP ports
- Remaining ports for EIP I/O devices

Results

The switch configuration file is loaded.

10.4 Switch Maintenance

During a maintenance or upgrade process, to move the Ethernet/IP cable (TOFINO Downlink) from the yellow L2 switch to the green L2 switch. perform the following tasks.

To move the Ethernet/IP cable from the yellow L2 switch to the green L2 switch

1. Disconnect the Stratix cable (EtherNet/IP Uplink) from the yellow switch.
2. Disconnect the cross-over cable between the yellow and green L2 switches.
3. Connect the Stratix cable (EtherNet/IP Uplink) to the green switch.
4. Reboot the yellow switch for maintenance or upgrade purpose.
5. Connect the cross-over cable between the yellow and green L2 switches.
6. Move the Stratix cable (EtherNet/IP Uplink) to the yellow switch.

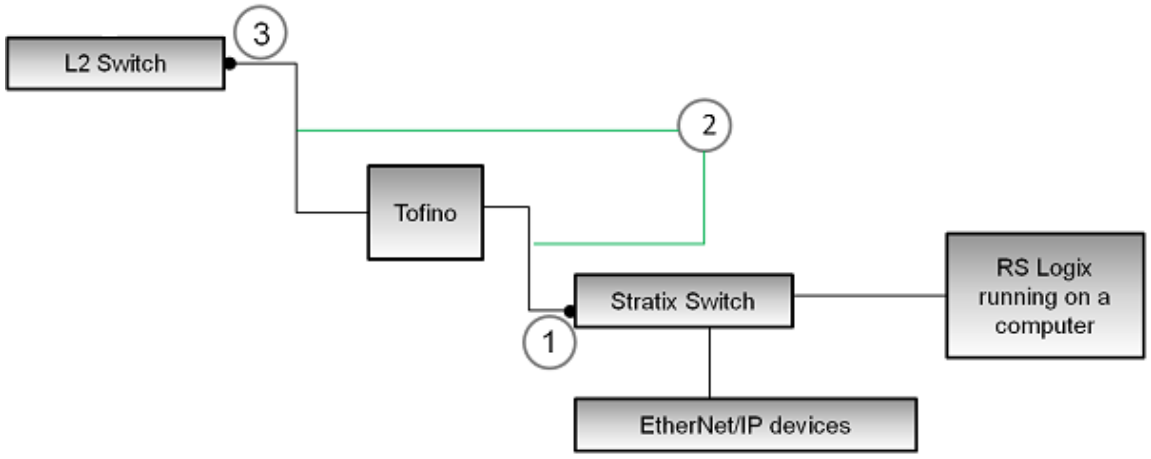
10.5 Tofino firewall configuration

The Tofino Industrial Security Solution helps in providing a secure communication on the industrial control network. It is a distributed network security solution. To ensure a secure communication, you can define firewall rules, specify the devices that are allowed to communicate, and specify the protocols that can be used. The Tofino security appliance is added to allow only the EtherNet/IP traffic to and from the L2 Switches. The Tofino Industrial Security Solution consists of the following components:

- The Tofino Security appliance
- Loadable Security Modules (LSM)
- Tofino Central Management Platform (CMP)

For more information about the Tofino Industrial Solution and its components, see Tofino Security Products.

The following figure highlights the port specifications and the cable details in a Tofino firewall configuration:



Item	Description
1	Up–link port configured to 100TX-FD, No MDIX
2	Straight EtherNet cables
3	Any L2 port configured to 100TX-FD, No MDIX

Attention
The Tofino security appliance must be connected to the yellow level 2 CISCO switch.

10.6 Software and hardware requirements for Tofino firewall configuration

The following table provides the required licenses, hardware, and software components to setup a Tofino firewall module. For more information about the components listed in the table, see “Tofino Security Products”.

Component	Part number	Description	Requirement	Quantity
Hardware	TSA 100	The Tofino Security Appliance is the firewall hardware module.	Required	1 hardware module
Software	FA-CMP-100-D	The Tofino Central Management Platform (CMP) tool is used to configure the firewall rules. The installer for the CMP tool is available on a DVD. CMP is a software component, which provides coordinated security management for all the Tofino Security Appliances from one workstation or server.	Required	1 software DVD
Firmware	LSM-FW-100	The Tofino Industrial Security Solution provides individual security functions in a firmware module, which is referred to as a Loadable Security Module (LSM). Tofino Firewall is an LSM, which is used to check communication on the control network by using the defined firewall rules. This is a licensed module.	Required	1 license
	LSM-LOG-100	The Tofino Event Logger is an LSM, which is used for event logging. Events in Tofino can be saved to a log file on the server. This is a licensed module. This is an optional module.	Optional	1 license
	LSM-SAM-100	Tofino Secure Asset Management is an LSM, which is used for securely managing the Tofino security appliances and other network equipments. This is a licensed module. This is an optional module.	Optional	1 license

10.7 Configuring the Tofino firewall

The Tofino security appliance is added to allow only the EtherNet/IP traffic to and from the L2 Switches. To facilitate the EtherNet/IP devices to communicate with the C300 controller (which is connected to the L2 switch) through the Tofino firewall, you must configure the Tofino firewall with specific firewall rules.

Prerequisites

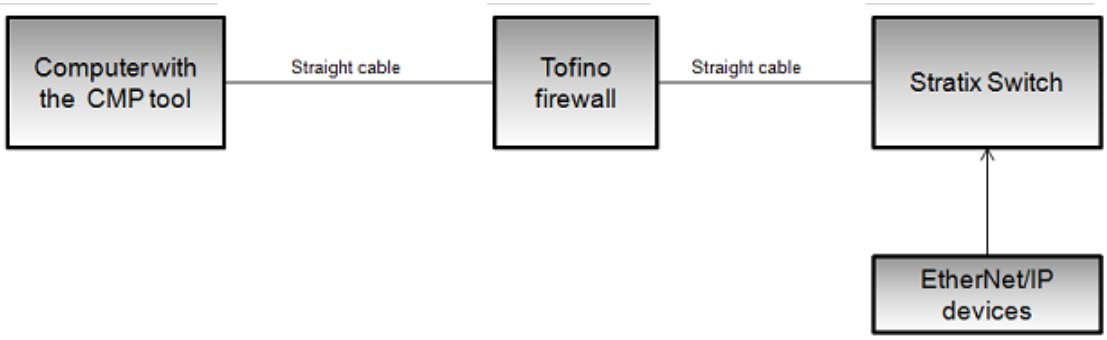
Refer to the Tofino documentation and perform the following tasks:

- Set up the hardware - For more information about the hardware setup specifications, see the following:
  - Tofino Installation and Troubleshooting Guide
  - “Software and hardware requirements for Tofino firewall configuration” on page 77
- Install the Tofino CMP — Central Management Platform (CMP) tool - For more information about installing and configuring the Tofino CMP tool, see Tofino CMP Installation and Upgrade Guide.

> **Attention**
> Run the Tofino CMP installer to generate the Export Request File. Send this file to activation@tofinosecurity.com to receive a Grant File. Import the grant file into the Tofino CMP tool, provide the required key, and create a login account.

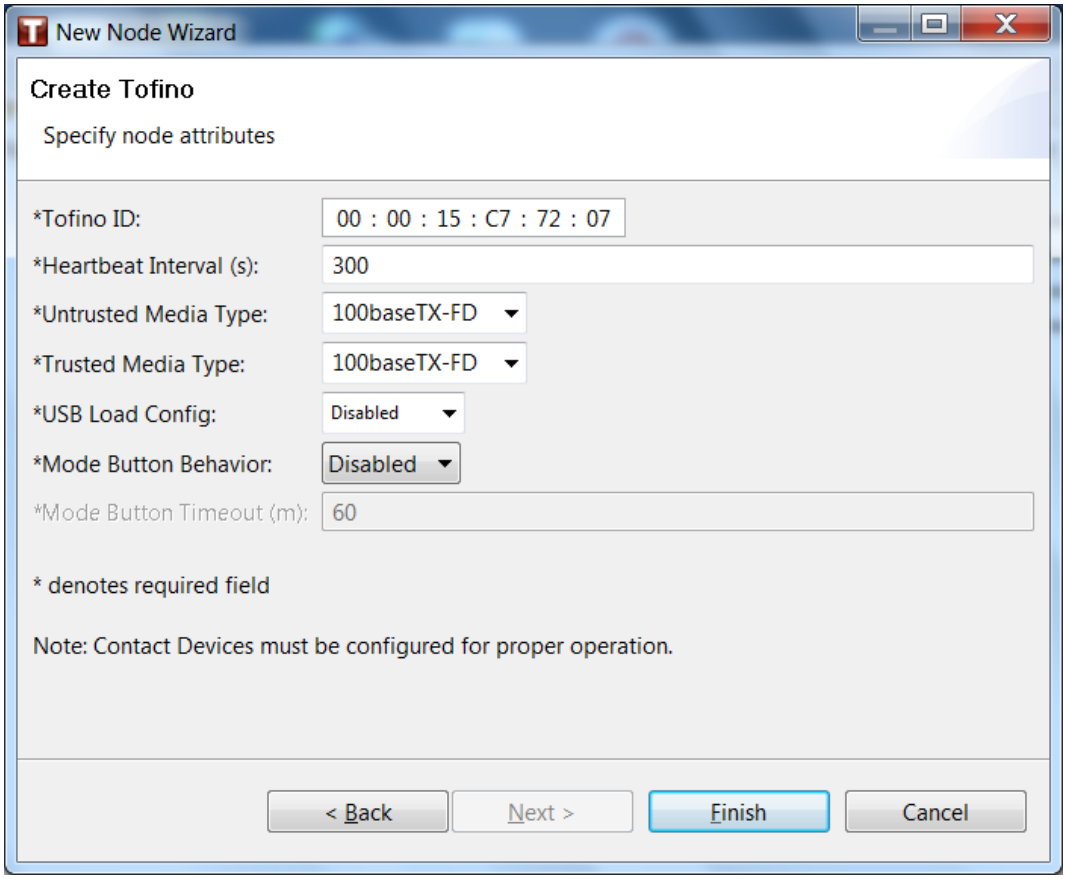
To configure the Tofino firewall

1. Connect straight Ethernet cable between the computer, which has the CMP tool installed to the Up-Link port (Upper port) of the Tofino firewall hardware module.
2. Configure an Up-Link port on the Stratix switch to 100TX-FD, No MDIX
3. Connect a straight Ethernet cable from Down-Link port (bottom port) to the configured Up-Link port on Stratix switch.



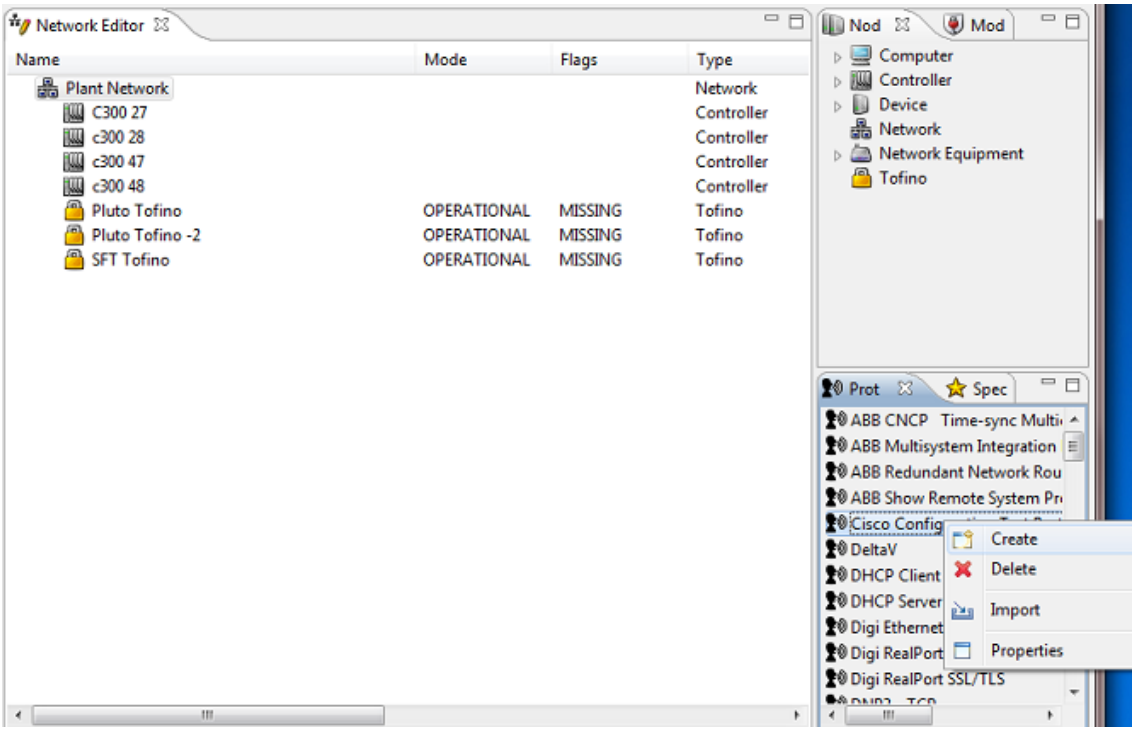
4. Ensure that ICMP ping is possible from the computer, which has the CMP tool to any EtherNet/IP device connected to the Stratix switch.
5. Login to the CMP tool.
6. Start a Tofino Discovery Scan ensuring that the discovery scan includes the IP address of the EtherNet/IP devices, which are connected to the Stratix switch.
7. Drag the discovered Tofino SA from the **Tofino Discovery view** to the **Network Editor** and rename it appropriately.
   The **New Node Wizard** appears.
8. In the New Node Wizard, specify a name, and click **Next**.
9. Specify the following attributes for the node and click **Finish**:

Option	Value
Untrusted Media Type	100baseTX-FD
Trusted Media Type	100baseTX-FD
USB Load Config	Disabled
Mode Button Behavior	Disabled



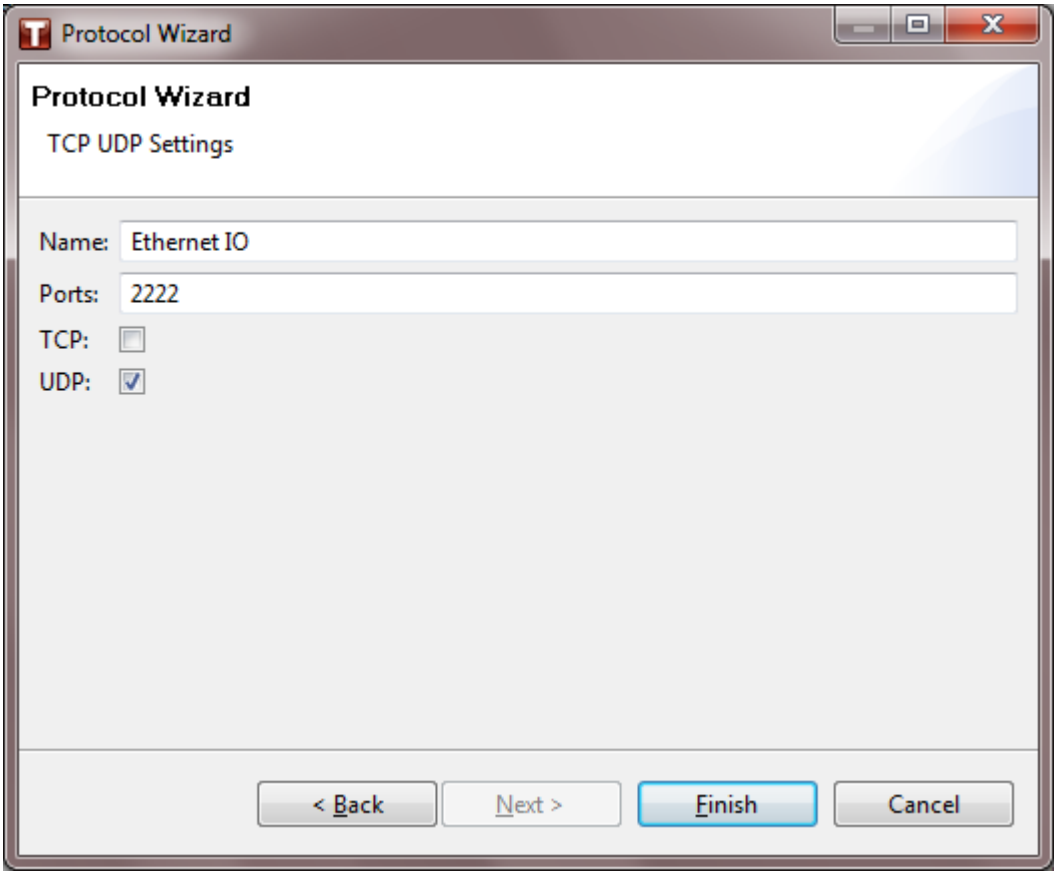
10 Double-click the new Tofino instance in the **Network Editor**. Under the **Modules** tab, select **Firewall LSM** and set the state to **Activated**.

11 Under the **Protocol** tab right-click to create a new protocol.



The Protocol Wizard launches. Follow the on-screen instructions to create the new protocol.

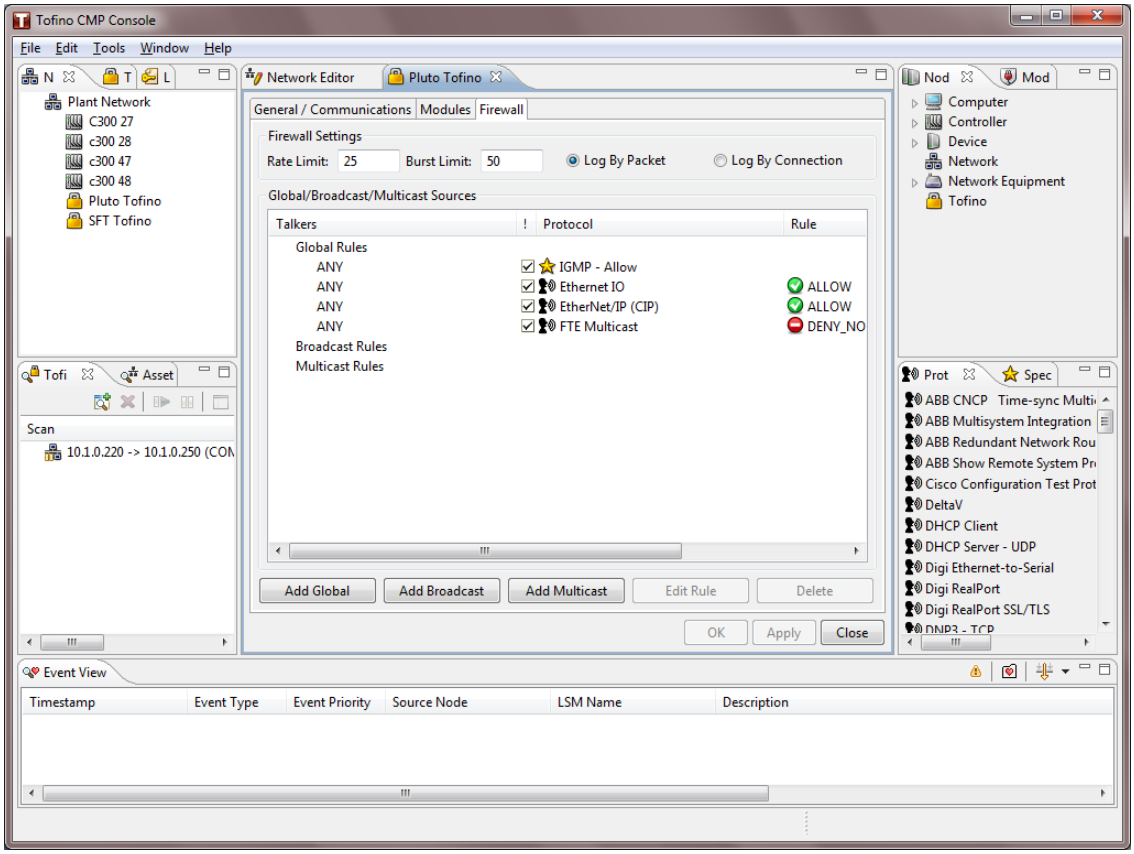
1. On the Choose a Protocol Type page, select **TCP UDP Protocol** as the Protocol type.
2. On the TCP UDP Settings page, specify the following details:
   - Name — Ethernet IO
   - Ports — 2222
   - Select UDP.



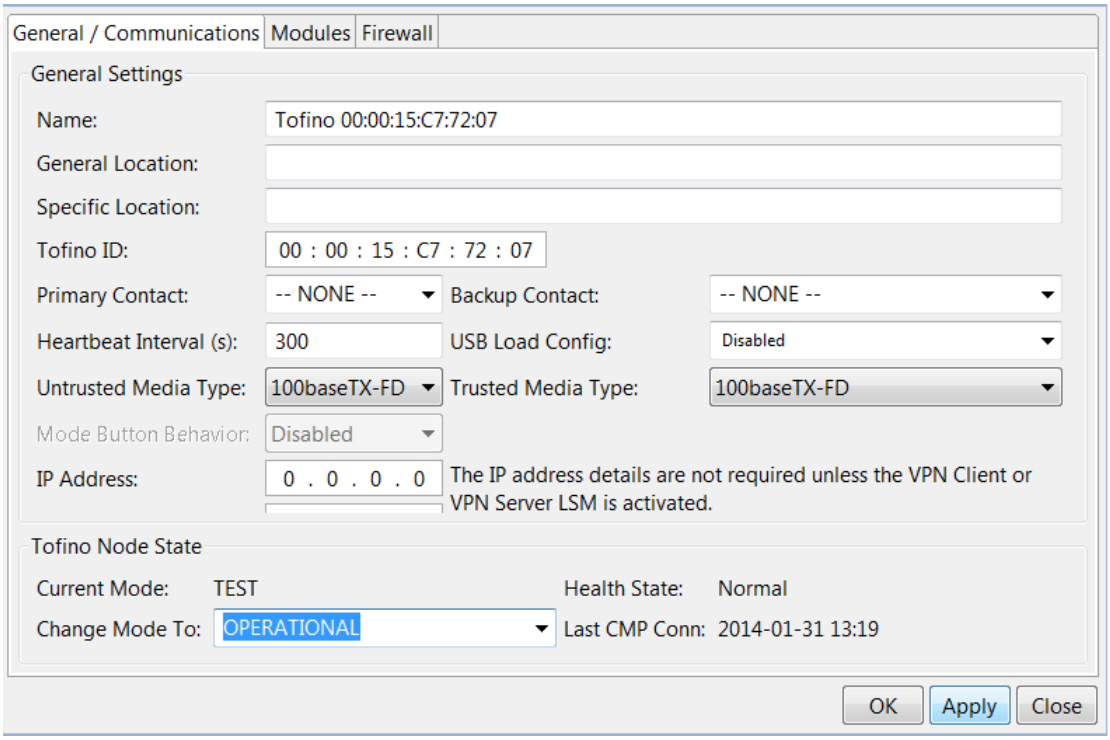
The new protocol named Ethernet IO is created.

12 Double-click the new Tofino instance in Network Editor. Under the **Firewall** tab, add the following global rules. To add the rules, drag the required option to the **Global Rules** section:

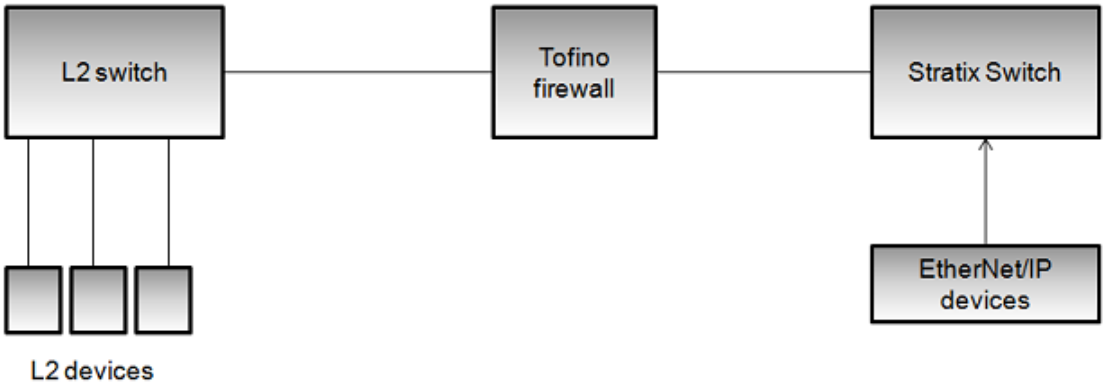
- Drag the **IGMP – Allow** option from the **Special Rules** tab to the **Global Rules** section:
- Drag the **EtherNet/IP (CIP)** option from the Protocols tab to the **Global Rules** section. Select and set the rule as **ALLOW**.
- Drag the **Ethernet IO** option from the Protocols tab to the **Global Rules** section. Select and set the rule as **ALLOW**.
- Drag the **FTE Multicast** option from the Protocols tab to the **Global Rules** section. Select and set the rule as **DENY_NOLOG**.



13 In the **General / Communications** tab, set the Tofino mode to **Operational**.



14 Remove the straight Ethernet cable connected to the computer with CMP tool and connect it to any L2 port on the L2 switch as shown in the following graphic.



15 Configure strategies in the C300 and to write and read the OP, PV values from the EtherNet/IP devices to verify the proper operation of the Tofino firewall.

Note

To modify the Tofino LSM firewall configuration (for example, changing the mode from Operational to Test), ensure that you always connect the straight Ethernet cable directly between the computer with CMP tool and the Up-Link port (upper port) of Tofino hardware module. For more information about troubleshooting other issues related to Tofino please, see the Tofino Troubleshooting guide in the Help menu of the CMP Tool.

CAUTION

Do not modify the Tofino firewall mode of operation by using the computer with the CMP tool connected to L2 switch as this might result in loss of view and loss of control.

Results

You have configured the required rules to facilitate the EtherNet/IP devices to communicate with the C300 controller through the Tofino firewall.

Next steps

In Control Builder verify the input and output modules.

10.7.1 Capturing Tofino diagnostic information

You can capture Tofino-related diagnostic information to a USB storage device.

To create these diagnostic information files you must perform a USB save.

To capture Tofino diagnostic information

1 Insert a USB storage device into one of the USB ports.

2 Press and hold the Config button for 1-2 seconds.(less than 5 seconds)

3 The Fault-Event-Mode LEDs will begin to flash in downward sequence, to indicate the **Save** operation.

4 When the LED flashing sequence stops, remove the USB key.

5 If the save operation was successful, the Tofino SA LEDs will revert to the state they were originally in prior to the saving action.

If the USB Diagnostic Save is successful there will be three or four files on the USB key similar* to the following:

```
00_00_11_8D_95_14_diagnostics.txt
00_00_11_8D_95_14_diagnostics.enc
00_00_11_8D_95_14_kernel_evt.enc
00_00_11_8D_95_14_evt.log
```

The log file (example, 00_00_11_8D_95_14_evt.log will appear only if the Event Logger LSM is installed and activated.)

*The prefix of the file name will be equal to the Tofino ID.

6 Send copies of these files to the technical support team for analysis.

Attention

For more information about troubleshooting issues related to Tofino security appliance and Tofino-related configurations, contact Tofino support or see:

- The Tofino troubleshooting guide in the Help menu of the CMP Tool or contact the Tofino support.
- Tofino documentation

11 Network Security

This section describes the key network security considerations for Experion systems.

Related topics

11.1 High Security Network Architecture

Honeywell's High Security Network Architecture is recommended for Fault Tolerant Ethernet based systems using Experion 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.

To implement Honeywell's High Security Network Architecture, complete the instructions in the following topics in PDF Collection.

- Installation and Upgrades > Fault Tolerant Ethernet Overview and Implementation Guide > Planning a Honeywell FTE Network.
- Installation and Upgrades > Fault Tolerant Ethernet Overview and Implementation Guide > Use of IP Addresses in an FTE Network.

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

11.2 Supported topologies

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

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 access the process control network as well as the business network
Level 4	Business network applications such as Manufacturing Execution Systems (MES) and Manufacturing Resource Planning (MRP) solutions

For small scale networks you can also connect:

- Level 1 and Level 2 devices using a single switch.
- Console Stations directly to the Level 1 switches where the geography of the plant dictates this.

About Level 1

At Level 1, controllers (C300 and 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 is limited to communication with other Level 1 nodes and with the Experion servers and Stations at Level 2. Network traffic on the Level 1 network is also prioritized such that CDA traffic is highest priority.

About Level 2

At Level 2 Experion 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.

- Domain controller can reside on Level 2 or Level 3 depending on your requirement. For more information, refer to the *Windows Domain/Workgroup Implementation Guide*.

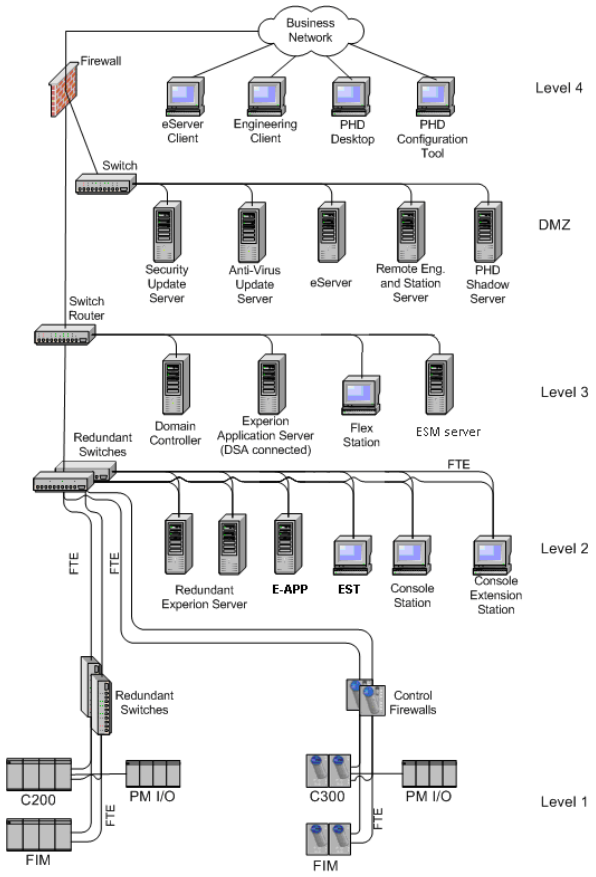
IP subnetting of nodes, priority queuing, and access lists in the switches are used to control network traffic between Level 2 and Level 1 as follows:

- Internal Level 1 traffic has a higher priority than traffic between Level 2 and Level 1 nodes. Peer-to-peer controller communication is not 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.

Attention

Only CF9s provide unicast storm limits. For example, L1 Cisco switches with FTEBs would not have this protection.

The following image illustrates the different levels in an Experion system. Topologies other than the one illustrated in the following images are supported.



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 servers, Stations, and other nodes are connected to a Level 3 router, which may also have 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 have to communicate with the domain controller which should be part of the Level 3 network. Gas measurement systems can reside at either Level 3 or the DMZ.

About demilitarized zones

A demilitarized zone (DMZ) serves as a buffer zone between the process control network and the business network. It is a separate network segment connected directly to the firewall.

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, refer to the section “The demilitarized zone” on page 92.

About Level 4

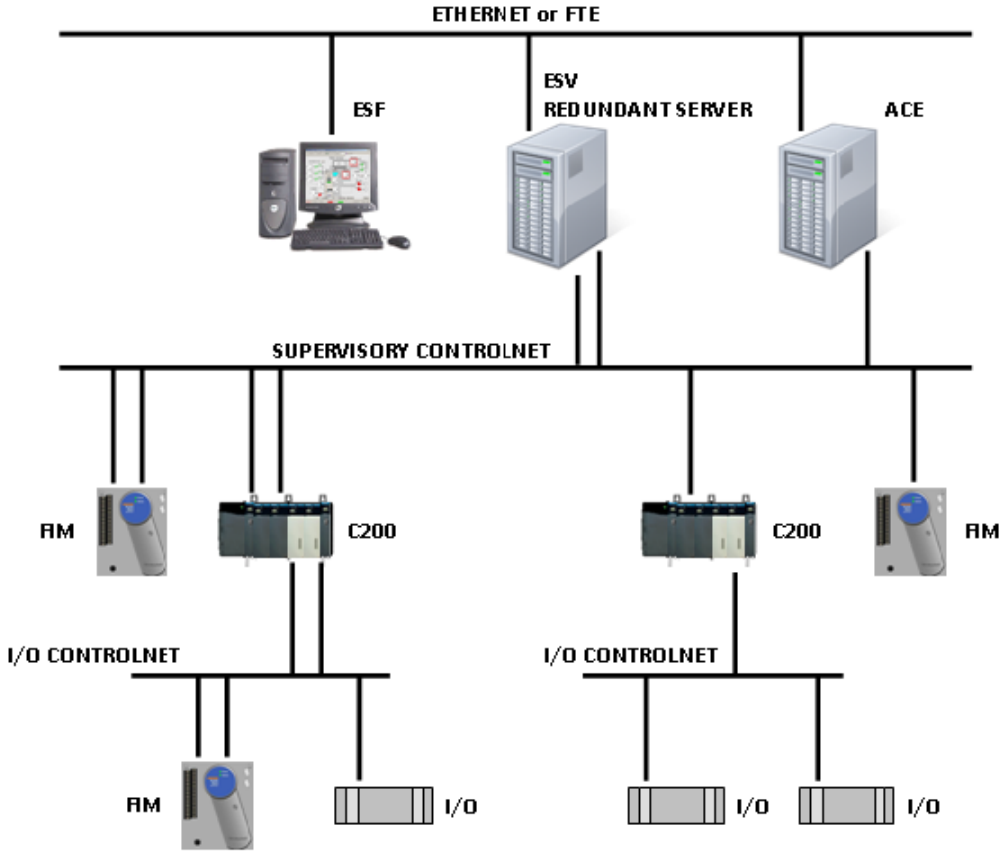
Level 4 is the business network (refer to the section “Connecting to the business network” on page 91). It is generally administered by the corporate IT department and is outside the scope of these guidelines.

11.2.1 Sample FTE Network topology

FTE topology is two parallel tree hierarchies of switches, up to three levels, connected at the top by one crossover cable to form a single fault tolerant network. The separate physical identity of the two trees is maintained by color coding and tagging of cables, switches and FTE node ports.

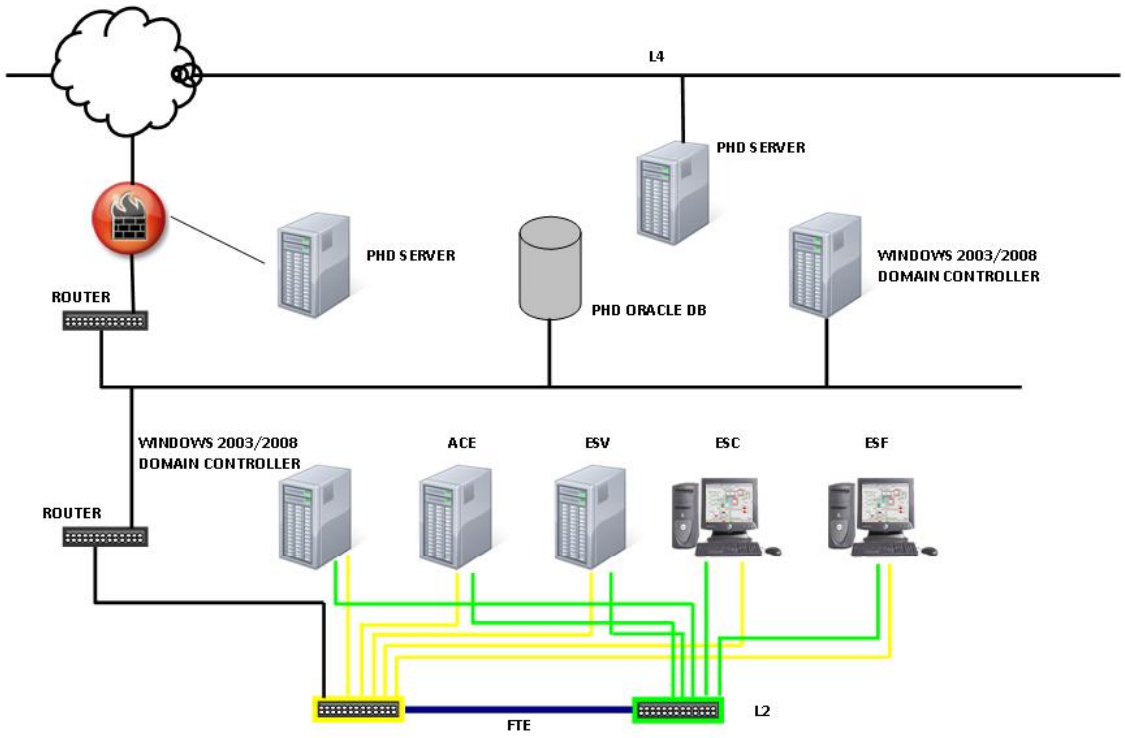
11.2.2 Basic ControlNet topology

The following topology is an example of the ControlNet supervisory network with basic Experion ControlNet components and displays where it is connected in the cluster.



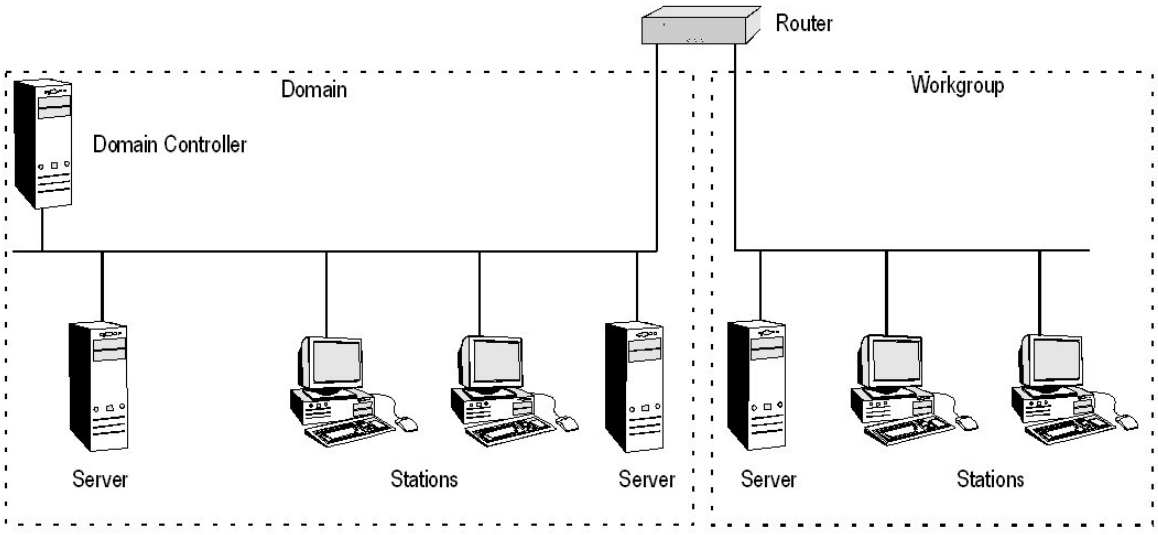
11.2.3 Experion - PHD Integration Topologies

The following topology image illustrates how the PHD Server may fit into the Experion System. Not all possible combinations are displayed, but these examples illustrate the general network schema.



11.2.4 Mixed domain and workgroup topology

If you have a geographically dispersed DSA system, you can use a mixture of domains and workgroups. The following image illustrates how you can use a domain for the centralized servers and a workgroup for the remote server and its Stations.



11.3 Connecting to the business network

The following are the differences in the nature of network traffic on these two networks.

- Internet access, FTP, email, and remote access are 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.

Ideally there must not be direct communication between the process control network and the business network. However, practical considerations often mean that a connection is required between these networks. This is because, the process control network requires data from the business network or because certain business applications need access to data from the process control network.

However, such a connection represents a significant security risk and therefore careful consideration must be given to the design. As a result, it is strongly recommended that only a single connection be allowed and that the connection is through a firewall and a DMZ as described in the section “The demilitarized zone” on page 92.

11.4 The demilitarized zone

A demilitarized zone (DMZ) is a separate network segment that connects directly to the firewall (as illustrated in the image in section) and provides a buffer between the process control network (PCN) and the business network. Servers containing data from the process control system that needs to be accessed from the business network are put on this network segment.

It is recommended that direct access between the two networks is avoided by having each network only access nodes in the DMZ. By eliminating the direct connection between the nodes in the PCN and the business network, the security of each network is increased.

With any external connections the minimum access should be permitted through the firewall. Only identified ports required for specific communication should be opened.

The access required for specific node types is described in section “Configuring the DMZ firewall” on page 93. For more detailed information on firewall configuration, contact Honeywell Network Services.

11.5 Configuring the DMZ firewall

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

Filtering is used to permit only specific nodes on the business network, DMZ and process control network (PCN) to communicate. TCP port filtering should be used to stop denial-of-service attacks to well-known ports.

The topics in this section describe the firewall access and account requirements for an arrangement where nodes on the business network, DMZ, and PCN are separated by a firewall. While other topologies are possible, you must consider their security implications (for example, if a DMZ is not used).

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 topics in this section describe the firewall access requirements for Honeywell-supplied applications. In addition to the requirements documented, access may be required for Windows authentication of accounts and synchronization between domain controllers. The precise access requirements depend upon the following:

- The domain membership of the nodes in the DMZ (business, PCN or other).
- The domain membership of accounts used.
- The location of domain controllers and which, if any, trusts exist between domains.

For more information on:

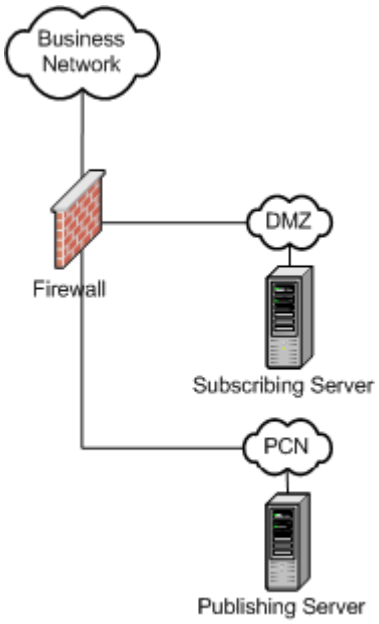
- Domains, refer to the section “Windows Domains and Workgroups” on page 157.
- Firewall filtering requirements; refer to the relevant Microsoft documentation.

11.5.1 Distributed system architecture

This section describes the firewall access and account requirements for Distributed System Architecture (DSA) nodes.

DSA is an option that supports the sharing of information between Experion servers, and is used by a number of the systems described in the following sections.

DSA nodes have publishing and subscribing roles. Publishing servers provide data to subscribing servers. For more details see "Distributed System Architecture" in the chapter "Servers" in the *Server and Client Planning Guide*. The following image illustrates a publishing and a subscribing node. DSA supports networks of nodes, any of which can be publishing, subscribing, or both.



The following table displays the firewall access requirements if both servers are running Experion R310 or later.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Subscribing server	Publishing server	DMZ	12321/UDP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Subscribing server	Publishing server	DMZ	55556/TCP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Subscribing server	Publishing server	DMZ	55563/TCP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Subscribing server	Publishing server	DMZ	55550/TCP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Subscribing server	Publishing server	DMZ	55557/TCP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Subscribing server	Publishing server	DMZ	1433/TCP	This is the default MS SQL server port, required for embedded charts.Client nodes viewing embedded charts over DSA can also be a source host.
Subscribing server	Publishing server	DMZ	2911/UDP	Connection must be configured to use Unicast. Do not use the "Link Supports Multicast Traffic" option.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Publishing server	Subscribing server	PCN	2911/UDP	Connection must be configured to use Unicast. Do not use the "Link Supports Multicast Traffic" option.
Subscribing server	Publishing server	DMZ	50001/TCP	
Subscribing server	Publishing server	DMZ	50003/TCP	
Publishing server	Subscribing server	PCN	50002/TCP	
Publishing server	Subscribing server	PCN	50004/TCP	

If either of the servers is running a release earlier than Experion R310, firewall access needs to be configured as follows.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Subscribing server	Publishing server	DMZ	2911/UDP	Connection must be configured to use Unicast. Do not use the "Link Supports Multicast Traffic" option.
Publishing server	Subscribing server	PCN	2911/UDP	Connection must be configured to use Unicast. Do not use the "Link Supports Multicast Traffic" option.
Subscribing server	Publishing server	DMZ	135/UDP	RPC Endpoint Mapper
Subscribing server	Publishing server	DMZ	1024-65535/UDP	The port range can be restricted by registry settings.
Publishing server	Subscribing server	PCN	135/UDP	RPC Endpoint Mapper
Publishing server	Subscribing server	PCN	1024-65535/UDP	The port range can be restricted by registry settings.

Honeywell strongly recommends that IP to IP access be granted between pre-R300 DSA servers.

Note that the password for the Windows mngr local account must be the same on all servers in a DSA system.

In addition, note that this section refers to Point and Notification DSA traffic and does not include usage of the DSA Alarm Event Report. To use this report, the pre-R300 DSA firewall settings must be configured between servers.

11.5.2 File shares

This section describes the firewall access and account requirements for file shares.

File shares provide access to files for remote systems, such as gas measurement systems, and are used by a number of the systems described in the following sections.

Note that the following directory has a file share configured that is used by the "Alarm and Event DSA" report.

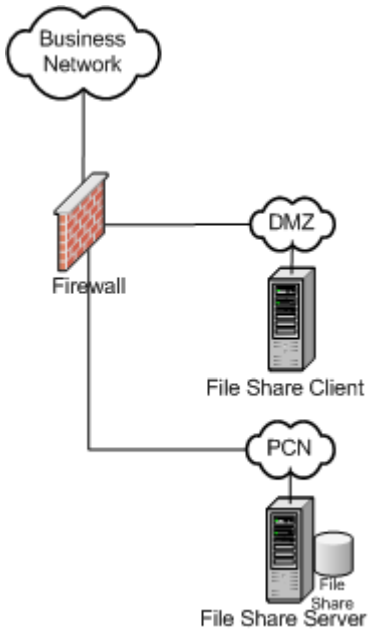
ProgramData\Honeywell\Experion PKS\Server\Data\Report

The file share is used by the "Alarm and Event DSA" report to perform the following:

- Allow the report output to be viewed from a remote Station. Read permissions are granted to the generic Windows Users group for this purpose. If all operator accounts are contained within the same group, then access can be further reduced by only giving that group read access to this directory.

- Allow all temporary information to be retrieved from remote servers when running a report across multiple servers. Read and Write permissions are granted to the Honeywell Product Administrators group for this purpose.

The following image illustrates a server in the DMZ accessing files from a server in the process control network (PCN).



The following table displays the firewall access requirements if both systems are running Windows 2000 or later.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
File share client	File share server	DMZ	445/TCP	

11.5.3 Folder shares and permissions

The following is a list of folder shares and permissions set by the Experion installation.

Share permissions for shares created by Server-Client install

Account Permission	Permission
Local Servers	Full Control
Product Administrators	Full Control
Local Engineers	Change and Read
Local Supervisors	Read
Local Operators	Read
Local Ack View Only Users	Read
Local View Only Users	Read

Shares created by Server-Client install

Name	Location	Nodes	Usage
Abstract	*C:\ProgramData\Honeywell\Experion PKS \Client\Abstract*	Server, Console Station, and Flex Station	Contains users custom displays and is used by File Replication to replicate abstracts to Backup Server, Console Stations and other nodes as configured by user
Checkpoint	*C:\ProgramData\Honeywell\Experion PKS \CheckPoint*	Nodes: Server and Console Station	Used by File Replication to replicate contents to Backup Server and Console Stations
DisplayShare1	*C:\Program Files(x86)\Honeywell \Experion PKS\Client\System\ R431*	Server	Contains the system displays, this share is used by a component in Configuration Studio
DisplayShare2	*C:\ProgramData\Honeywell\Experion PKS \Client\Abstract*	Server	Contains the users custom displays, this share is used by a component in Configuration Studio
EFM	*C:\ProgramData\Honeywell\Experion PKS \server\data\efm*	Server	Contains the exported EFM data for meters. **Attention** The location is configurable; if the location changes, this share might not be used.
GUS Security	*C:\ProgramData\Honeywell\ProductConfig \Security*	• ACE-T • APP • ESC • ESVT	T-node security
HCISecurity	*C:\ProgramData\Honeywell\ProductConfig \Security*	• ACE-T • APP • EAS • ESC • ESCe • Flex • ESVT • ESV • SCE	General security including HCI.
Mapping	*C:\ProgramData\Honeywell\Experion PKS \Server\data\mapping*	Server and Console Station	Contains mapping files for various Point Servers, and is used by File Replication to replicate to Backup Server and Console Stations
Qbfiles	*C:\ProgramData\Honeywell\Experion PKS \Server\user\qbfiles*	Server	Used by Quick Builder for downloads and uploads to the Server

Name	Location	Nodes	Usage
QDB	*C:\ProgramData\Honeywell\Experion PKS \Server\data\qdb*	Server	The Quick Builder database for the server is located in this directory, and is used by File Replication to replicate the QDB file(s) to the Backup Server
Report	*C:\ProgramData\Honeywell\Experion PKS \Server\data\Report*	Server and Console Station	Output from Experion Reports are stored in this directory
Views	*C:\ProgramData\Honeywell\Experion PKS \Server\data\views*	Server and Console Station	Contains view definitions for Alarm, System Alarm, Event, Message, Alert and SOE Summary displays, and is used by File Replication to replicate to the Backup Server and Console Stations

Shares created and permissions created by Experion Tools install

Name	Location	Nodes	Usage	Account	Permissions
HYBRID	*C:\ProgramData\Honeywell \Experion PKS \Engineering Tools*	• Server • Flex Station • Console Station • ACE • SCE • EHG	Used by DBAdmin for database synchronization and replication purposes	EXPSqlSVC	Change, Read
				Product Administrators	FULL, change, Read
CPBASE	*C:\ProgramData\Honeywell \Experion PKS \CheckPointBase*	Server	Checkpoint files are stored here and used during server replication and other checkpoint related tasks	Local Operators	Read and change
				Local Engineers	Read and change
				Local Supervisors	Read and change
				Product Administrators	Full, Change, Read
				Local Ack View only users	Read and change
				Local view only users	Read and change
				EXPSqlSVC	Read and change
Install	*C:\Program Files(x86)\Honeywell \Experion PKS\Install*	• Server • Flex Station • Console Station • ACE • SCE • EHG	Used by Upgrade Tool to analyze Installer files	Product Administrators Local Engineers	Read

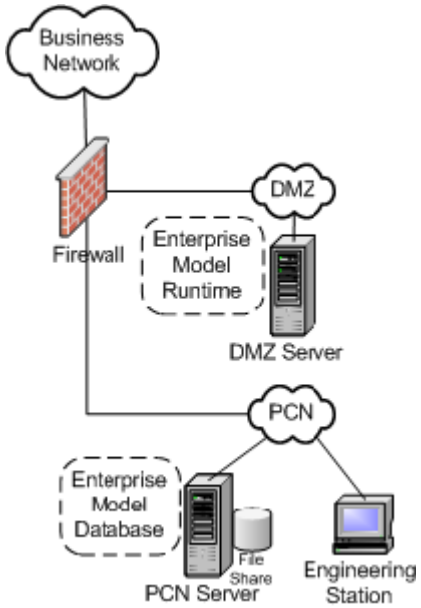
Shares created by custom installation path

Component	Default path	Custom installation path
Experion software	*C:\Program Files (x86)\Honeywell*	%User selected path%\Honeywell
Experion runtime data	*C:\ProgramData\Honeywell*	%User selected path%\Honeywell
Experion SQL logs	*C:\ProgramData\Microsoft SQL Server*	%User selected path%\Microsoft SQL Server

11.5.4 Enterprise model update

The Enterprise Model Builder Database (EMDB) is a system-wide database that stores information on assets, system alarms and alarm groups.

In the following example, the server in the process control network (PCN) stores the Enterprise Model database, but changes are made from an engineering Station in the PCN, and a server in the DMZ uses the Enterprise Model runtime. Changes are made in the offline database and downloaded to servers using the Enterprise Model runtime.



The following firewall access is required to download the Enterprise Model runtime.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Engineering Station	DMZ server	PCN	2909/TCP	
Engineering Station	DMZ server	PCN	2910/TCP	

In addition to this access, the DMZ server needs access to the file share on the PCN server. The DMZ server is the file share client and the PCN server is the file share server. Firewall access requirements are described in section “File shares” on page 95.

Note the following account requirements:

- The Windows mngr local account on the DMZ server and PCN server must have the same password.
- The DMZ server needs to authenticate against the Engineering Station. If the System Wide Settings option Require user name and password for Quick Builder and Control Builder downloads is:
  - Selected

Ensure that both machines have the same account and password configured. The account name must be the same account name that was used to log into Configuration Studio. The account must also belong to the "Product Administrators" group on the DMZ server, and be configured as an Experion operator account with at least ENGR access rights.

– Not selected

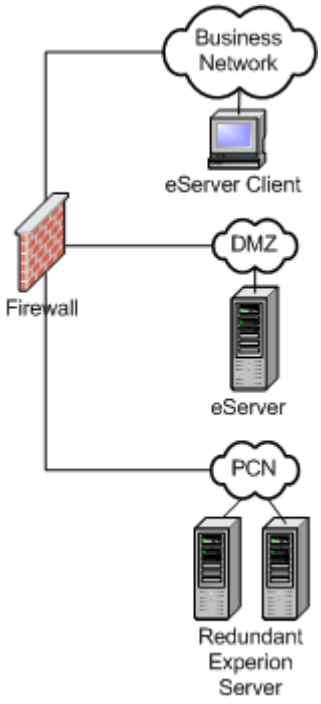
Ensure that the password for the Windows mngr local account is the same on the DMZ and PCN servers

11.5.5 eServer

An eServer provides read-only access to Experion graphics from a web client.

There are two types of eServer clients: Premium Access and Standard Access. Both provide read-only process graphics without the need for any re-engineering. Premium access provides graphics with data that updates as well as active navigation links. Standard Access graphics do not support data updates or any other type of user interaction.

The following image illustrates the eServer client in the business network, connecting to an eServer in the DMZ.



The following table displays the firewall access requirements for eServer.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
eServer client	eServer	Business network	80/TCP	HTTP
eServer client	eServer	Business network	50000/TCP	Premium Access client only

In addition to these access requirements, the eServer is a DSA node that subscribes to the publishing redundant Experion server. Firewall access and Windows account requirements are described in the section “Distributed system architecture” on page 93.

The default eServer configuration allows anonymous access for clients. If authentication is required for access to eServer, the interactive account being used on the eServer client needs to be authenticated on eServer.

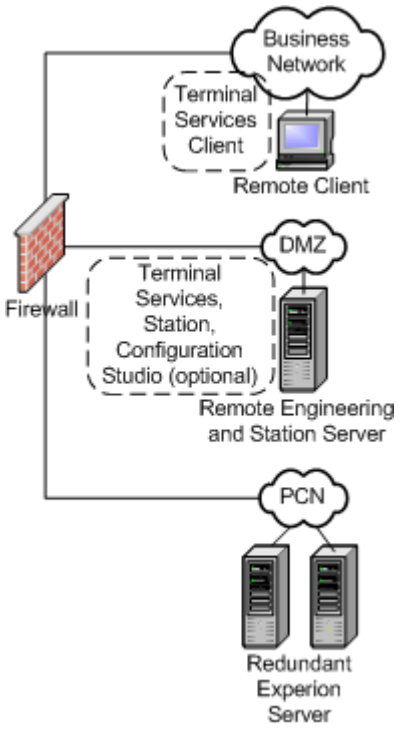
Optionally eServer might use the Enterprise Model runtime, with the Enterprise Model database on the redundant Experion server. Firewall access and account requirements are described in the section “Enterprise model update” on page 99.

11.5.6 Remote access for Station and Configuration Studio

If business network access is required to Configuration Studio or Station, you should set up a Remote Engineering and Station Server and use Microsoft Terminal Services. For information, refer to the section "Configuring Remote Engineering and Station Server" in the *Server and Client Configuration Guide*.

Because of the security risks and firewall access requirements, Honeywell does not support Station or Configuration Studio connected directly to the process control network (PCN) or DMZ. Running Terminal Services directly on the Experion server is also not supported because Terminal Services consumes a significant portion of the fixed size operating system "session space" resource. Exhausting this resource can stop the Experion server from starting correctly.

The following image illustrates a remote client connected to the Terminal Services running on the Remote Engineering and Station Server in the DMZ, which obtains information from a redundant Experion server in the PCN.



The firewall access requirements between the Remote Engineering and Station Server and the remote client are displayed in the following table.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Engineering client	Remote Engineering and Station Server	Business network	3389/TCP	Microsoft Terminal Services

The user on the remote client needs to log on to the Remote Engineering and Station Server with an account that can be authenticated in the Remote Engineering and Station Server's domain.

If Station access is required on the business network, Station runs on the Remote Engineering and Station Server, connecting to the redundant Experion server in the PCN.

If Configuration Studio access is required, both Station and Configuration Studio run on the Remote Engineering and Station Server. The firewall access requirements are described in the following table.

Secure host/network	Destination host/ network	Interface	Ports/service	Comments
Remote Engineering and Station Server	Redundant Experion server	DMZ	12321/UDP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Remote Engineering and Station Server	Redundant Experion server	DMZ	55556/TCP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Remote Engineering and Station Server	Redundant Experion server	DMZ	55563/TCP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Remote Engineering and Station Server	Redundant Experion server	DMZ	55550/TCP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Remote Engineering and Station Server	Redundant Experion server	DMZ	55557/TCP	Required for embedded charts. Client nodes viewing embedded charts over DSA can also be a source host.
Remote Engineering and Station Server	Redundant Experion server	DMZ	1433/TCP	This is the default MS SQL server port, required for embedded charts.Client nodes viewing embedded charts over DSA can also be a source host.
Remote Engineering and Station Server	Redundant Experion server	PCN	40209/TCP	Configuration Studio tasks that invoke some Station displays, such as the DSA configuration display.
Remote Engineering and Station Server	Redundant Experion server	PCN	40200/TCP	Configure Alarm Suppression task within Configuration Studio.
Remote Engineering and Station Server	Redundant Experion server	DMZ	Echo/ICMP	Optionally used to verify which server is currently active. It can be disabled by a configuration option.
Redundant Experion server	Remote Engineering and Station Server	PCN	Echo/ICMP	Optionally used to verify which server is currently active. It can be disabled by a configuration option.
Remote Engineering and Station Server	Redundant Experion server	PCN	1433/TCP	SQL Server access (Configuration Studio only).
Remote Engineering and Station Server	Redundant Experion server	PCN	2909/TCP	
Remote Engineering and Station Server	Redundant Experion server	PCN	2910/TCP	Configuration Studio only.
Remote Engineering and Station Server	Redundant Experion server	PCN	50000/TCP	

If the firewall has been configured to disable ICMP traffic, Station is able to connect to the server unless the "ping" setting in the *station.ini* file has been disabled. For information on changing station.ini file settings, refer to the section "Station.ini" in the chapter "Configuring stations and printers" in the *Server and Client Configuration Guide*.

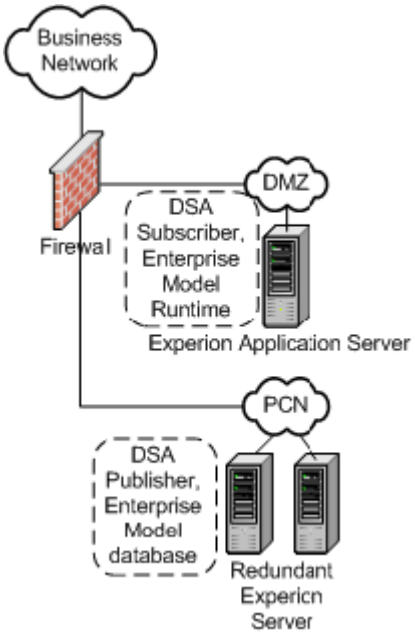
If Configuration Studio is used on the Remote Engineering and Station Server, access to a file share on the redundant Experion servers is required. The Remote Engineering and Station Server is the file share client and the redundant Experion servers are the file share servers. For details on the firewall access requirements, refer to the section “File shares” on page 95.

When users of Configuration Studio connect to Experion, they must use an account that correlates to an operator on that Experion server.

11.5.7 Experion Application Server

When users of Configuration Studio connect to Experion, they must use an account that correlates to an operator on that Experion server.

The following image illustrates an Experion Application Server in the DMZ, getting information through DSA and sharing the Enterprise Model with the Experion server in the DMZ.



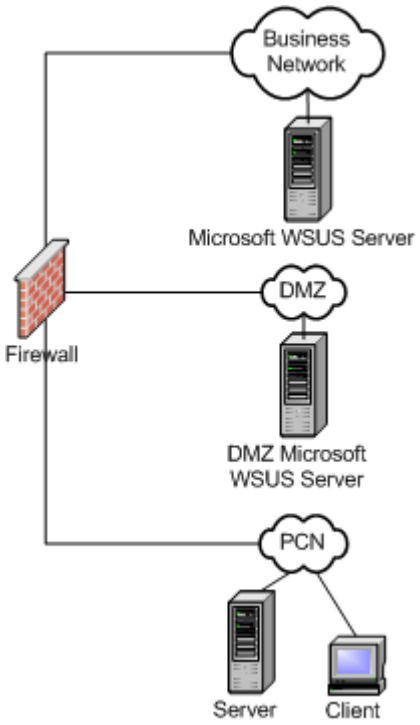
The Experion Application Server is the DSA subscriber to the publishing redundant Experion server. The firewall access and account requirements are described in section “Distributed system architecture” on page 93.

The Experion Application Server uploads the Enterprise Model runtime from the redundant Experion server. The firewall access and account requirements are described in the section “Enterprise model update” on page 99.

11.5.8 Microsoft Windows Software Update Services

A Microsoft Windows Software Update Services (WSUS) server provides Microsoft Security Hot fixes to nodes on the process control network (PCN).

The following image illustrates the Microsoft WSUS in the DMZ. The Microsoft WSUS gets Security Hot fixes from the Microsoft WSUS in the business network, and provides these updates via Windows Update to servers and clients in the PCN. Under no circumstances must the DMZ server access the internet to get the updates to propagate to the PCN.



The following table displays the firewall access required between the Microsoft WSUS server in the business network and DMZ.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
DMZ Microsoft WSUS server	Microsoft WSUS server	DMZ	80/TCP	HTTP

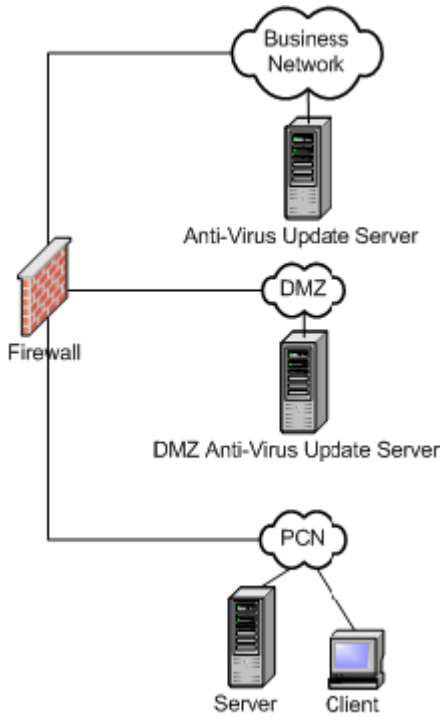
The firewall access required between the Microsoft SUS in the DMZ and the server and client nodes in the PCN is displayed in the following table.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PCN server or client	DMZ Microsoft WSUS server	PCN	80/TCP	HTTP

11.5.9 Antivirus update server

The Antivirus Update Server provides DAT file updates to nodes on the process control network (PCN).

The following image illustrates an Antivirus Update Server in the DMZ. The Antivirus Update Server gets antivirus DAT file updates from the Antivirus Update Server in the business network. In this way updated DAT files are provided to servers and clients in the PCN. Under no circumstances should the DMZ server access the internet to get the updates to propagate to the PCN.



There are two supported methods for distributing the DAT files: FTP and HTTP. You can use either of these methods.

The firewall access required between the Antivirus Update Server in the business network and DMZ is displayed in the following table.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
DMZ Antivirus Update server	Antivirus Update server	DMZ	80/TCP	HTTP
DMZ Antivirus Update server	Antivirus Update server	DMZ	21/TCP	FTP

The firewall access required between the Antivirus Update Server in the DMZ and the server and client nodes in the PCN is displayed in the following table.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PCN server or client	DMZ Antivirus Update server	PCN	80/TCP	HTTP
PCN server or client	DMZ Antivirus Update server	PCN	21/TCP	FTP

11.5.10 PHD

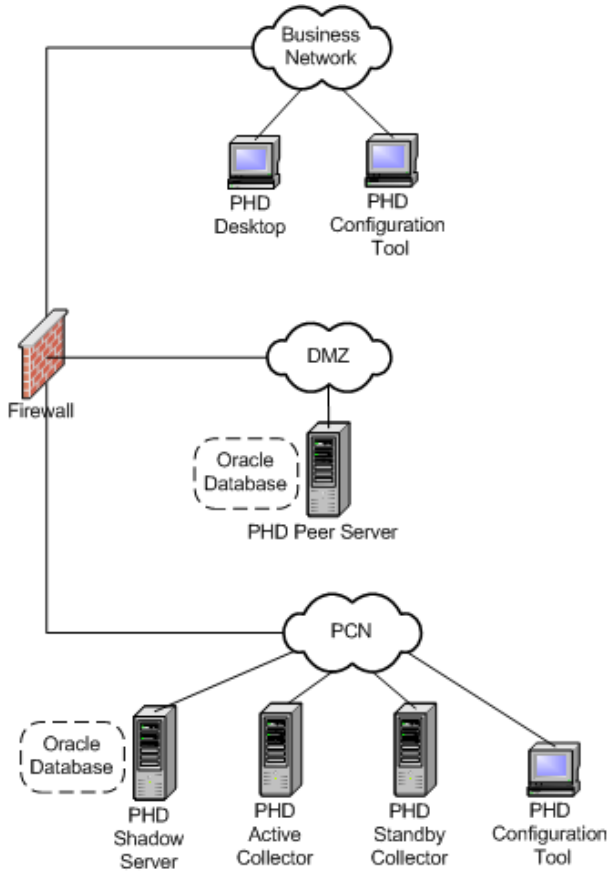
PHD is Honeywell's advanced historian, providing distributed data collection, and data consolidation. PHD supports a wide range of network topologies. This section describes the firewall access and account requirements of two possible topologies with different levels of complexity and security.

The firewall access requirements shown in this section apply to PHD Release 202 and later only. Earlier versions of PHD have different firewall access requirements.

High security configuration: PHD Peer Server in DMZ

The following image illustrates a PHD Peer Server in the DMZ gets data from a PHD Shadow Server in the process control network (PCN). The PHD Peer and PHD Shadow servers each have an Oracle database. A PHD Configuration Tool in the business network is used to configure the PHD Peer Server, while a PHD Configuration Tool in the PCN is used to configure the PHD Shadow Server and Collectors

The firewall access requirements for this configuration are minimal. A less complex topology that balances ease of configuration with somewhat less network security (because more ports need to be opened in the firewall) is shown in “Typical configuration: PHD Shadow Server in DMZ”



The firewall access requirements for communicating with the PHD Peer Server are as follows. The port numbers displayed in the following table indicate the default settings, which can be modified.

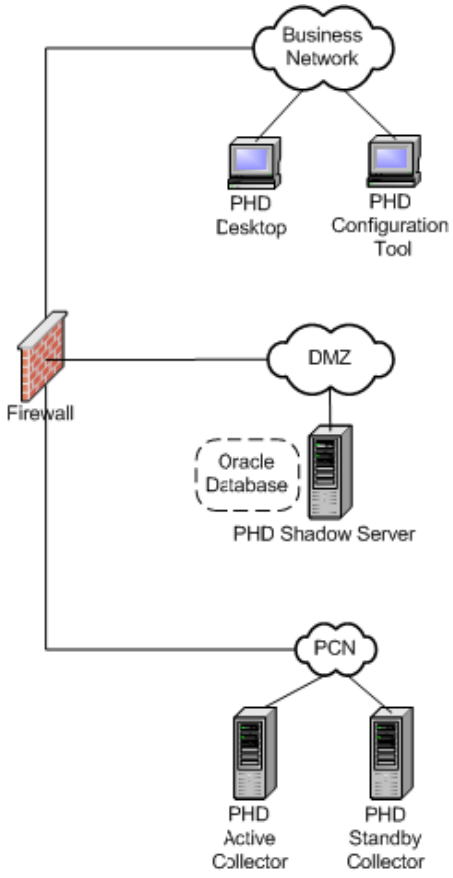
Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Peer Server	PHD Shadow Server	DMZ	49500/TCP	1st RDI. Each RDI has a port
PHD Peer Server	PHD Shadow Server	DMZ	49501/TCP	2nd RDI

The firewall access requirements for the connection between the PHD Desktop and the PHD Peer Server are as follows. The port numbers displayed in the following table indicate the default settings, which can be modified. The exception is port 445, which is fixed.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Desktop	PHD Peer Server	Business Domain	3100/TCP	Process Trend, Automation Object via Standard PHD API
PHD Desktop	PHD Peer Server	Business Domain	3150/TCP	Process Trend, Automation Object via Standard PHD API
PHD Desktop	PHD Peer Server	Business Domain	445/TCP	
PHD Desktop	PHD Peer Server	Business Domain	1521/TCP	Tag Explorer.

Typical configuration: PHD Shadow Server in DMZ

The following image illustrates a Shadow Server in the DMZ gets data from redundant PHD Collectors in the PCN. The PHD Configuration Oracle database is on the Shadow Server. The PHD Configuration Tool is used to configure PHD in the PCN.



This configuration has reduced Oracle database license and system administration requirements relative to the topology displayed in “High security configuration: PHD Peer Server in DMZ”. However, additional ports need to be opened in the firewall to support communication with the Oracle database. Furthermore, tag and user updates from the Shadow to the Collectors require specific NT authentication ports to be open.

The firewall access requirements for the PHD Configuration Tool to do an update are as follows. Ports are required for communication with the Oracle database and for sending tag and user updates from the PHD Shadow server to both the PHD Collectors. The port numbers displayed in the following table indicate default settings, which can be modified. The exception is port 445, which is fixed. Note that port 3100 can be modified but must be the same on the PHD Shadow Server and both PHD Collectors.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Configuration Tool	PHD Shadow Server	Business Network	1521/TCP	Oracle
PHD Configuration Tool	PHD Shadow Server	Business Network	3100/TCP	
PHD Configuration Tool	PHD Shadow Server	Business Network	445/TCP	
PHD Shadow Server	PHD Active Collector	DMZ	3100/TCP	
PHD Shadow Server	PHD Active Collector	DMZ	445/TCP	
PHD Active Collector	PHD Shadow Server	PCN	1521/TCP	Oracle
PHD Shadow Server	PHD Standby Collector	DMZ	3100/TCP	
PHD Shadow Server	PHD Standby Collector	DMZ	445/TCP	
PHD Standby Collector	PHD Shadow Server	PCN	1521/TCP	Oracle

Port 445 is used for many Windows functions, including authentication and Named Pipes. For more information, refer to the *Microsoft Knowledgebase Article Q179442*. Starting with Release 210, PHD can be configured to use either Named Pipes (the default method) or Secure Sockets to pass authentication information. Both methods require communication using port 445. Named Pipes use port 445 for both authentication and data transfer. Secure Sockets use port 445 for authentication.

The firewall access requirements for the connection between the PHD Desktop and the PHD Shadow Server are as follows. The port numbers shown in the following table are default settings, which can be modified. The exception is port 445, which is fixed.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Desktop	PHD Shadow Server	Business Domain	3100/TCP	Process Trend, Automation Object through Standard PHD API
PHD Desktop	PHD Shadow Server	Business Domain	3150/TCP	Process Trend, Automation Object through Standard PHD API
PHD Desktop	PHD Shadow Server	Business Domain	445/TCP	
PHD Desktop	PHD Active Collector	Business Domain	1521/TCP	Tag Explorer (optional)

Two approaches can be used for communication between a PHD Collector and a PHD Shadow Server: the Gateway RDI, which supports peer-to-peer communication, or the Shadow RDI.

- The Gateway RDI firewall access requirements are displayed in the “High security configuration: PHD Peer Server in DMZ”.
- The Shadow RDI is used in conjunction with Robust Data Collection (RDC) as displayed in this topology. The firewall access requirements for the Shadow RDI are as follows. The port numbers displayed in the following table are default settings, which can be modified.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Active Collector	PHD Shadow Server	PCN	54000/TCP	1st RDI, each RDI has a separate set of ports

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Active Collector	PHD Standby Server	PCN	54000/TCP	1st RDI, each RDI has a separate set of ports
PHD Standby Collector	PHD Shadow Server	PCN	54001/TCP	1st RDI, each RDI has a separate set of ports
PHD Active Collector	PHD Shadow Serve	PCN	54002/TCP	2nd RDI
PHD Active Collector	PHD Standby Server	PCN	54002/TCP	2nd RDI
PHD Standby Collector	PHD Shadow Server	PCN	54003/TCP	2nd RDI

PHD security account requirements

There are two client security models for PHD: standard and integrated NT security:

- With standard security, separate logins are required for the PHD Configuration Tool, PHD Data Access, and Oracle.
- With integrated NT security, the Windows login is assigned to a Windows local group that is granted permissions to Oracle. A secondary login is not required.

The service log on account used by the PHD Server and RDI Server services on the PHD Shadow and PHD collectors must be an account that belongs to the Administrators and PHD_MANAGER local groups of the machine. For ease of administration it is recommended that this be a domain account.

11.6 Specifying communication ports for Network API clients

By modifying the services file for client nodes, it is possible to identify specific ports so network API clients only send out requests on those ports. This allows client nodes and server nodes to be separated by a firewall and still communicate without having to open all ports on the client node so that it can pass UDP packets.

You must open the appropriate UDP ports (server and client) on any firewall the client must go through to reach the server. This includes any firewalls installed as part of the operating system or third party product as well as hardware firewalls.

Specifying client outbound ports in the services file

To specify outbound ports on the client node, perform the following:

- Open the services file from the following location.

  C:\Windows\system32\drivers\etc\services
- Add the following to the services file.

  hscnetapi_low_port <*port number low*>/udp

  # Lowest UDP port for use with the Honeywell Experion Network API

  hscnetapi_high_port <*port number high*>/udp

  # Highest UDP port for use with the Honeywell Experion Network API

Ports for client nodes

Following are requirements for client node outbound ports.

- Port numbers can range from 1 to 65535, but ideally start higher than 3000.
- Verify you do not use any port numbers already listed in the services file.
- The <*port number low*> value must be lower than the <*port number high*> value.

Ports for server nodes

The ports used by the server to provide the Network API services are defined in the **hsc_nif** and **hsc_nif_write** entries in the services file on the server. By default **hsc_nif** is 50000/UDP (read requests) and **hsc_nif_write** is 50001/UDP (write requests). If you modify the **hsc_nif** entry, you must also perform the following:

- Edit the **Server Port** in the **hscnetapi.ini**
- Copy the **hscnetapi.ini** to the C:\Windows directory on all clients

The read port must be set the same value on all servers so that the clients can connect to it through the **hscnetapi.ini** change. However, the write port can be different on all servers, in addition, no client side **hscnetapi.ini** change is required to be made for changing the write port.

SQL Ports for the Experion Server

The default instance of SQL is used for the Experion database. The default instance of SQL uses port 1433 for sqlserver.exe and 1434 for sqlbrowser.exe.

Ports for System Management

System Management uses the following two reserved ports.

- 3456: SRP point to point TCP listener – created on demand for limited time while remote node needs to synchronize.
- 51967: SRP multicast UDP port

ESM Ports

ESM opens up the firewall for mostly specific applications and a few selected ports.

For nodes hosting ESM server/SQL Express

ESM uses SQL Express. On the ESM Server sqlbrowser.exe uses port 1434. The port that sqlserver.exe uses is dynamically assigned for named instances of SQL. ESM uses a named instance of sql. So the port number for sqlserver.exe cannot be specified.

The applications for which the Firewall is opened on nodes hosting the ESM Server/SQL Express are as follows:

- sqlExpressPath =*C:\Program Files(x86)\Microsoft SQL Server\MSSQL_10_50.SQLEXPRESS_ESM\MSSQL\Binn \sqlservr.exe*
- sqlBrowserPath = *C:\Program Files(x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe*
- SvrHostPath = *C:\Program Files(x86)\Honeywell\ANCIM\serverhost.exe*

For all other Experion nodes

On all Experion nodes, the following applications open up the firewall.

- AgentHostPath = *C:\Program Files(x86)\Honeywell\ANCIM\Agenthost.exe*
- Currently ServerHost.exe and AgentHost.exe communicate using WCF on ports 5016 and 5017.

11.7 Allowing EMDB access between network levels

Use one of the options described in the following table, to communicate between network levels separated by a firewall (for example, between level 2/3 and level 4, or between level 2 and level 3).

Option	Comments
Open the firewall to the extent that it allows downloads from the EMDB to all relevant clusters.	Your network security policies may not allow this option.
Place the EMDB in the DMZ or on the higher level, and ensure that the relevant servers can access the file share on the EMDB.	Security policies may allow file share access from lower levels to higher levels, but not vice versa. Similarly, security policies may allow various levels to have access to file shares in the DMZ, but not vice versa.
Create a multi-system topology, with at least one system for the lower levels and one system for the higher levels.	The disadvantage of this option is that you need to manually keep your enterprise models sufficiently synchronized to allow the sharing of assets, point data and alarms.

11.8 Connecting other nodes to the process control network

There may be a requirement to connect non-Honeywell nodes to the process control network (PCN). This includes permanently connected computers associated with equipment such as analyzers, turbines, compressors, or metering systems, as well as laptop computers that are temporarily connected to the process control network for configuration purposes.

Laptop computers

The portability of laptops poses a particular risk, as they can become infected elsewhere with malicious agents such as viruses or worms and spread these to the PCN.

As it is not possible to completely mitigate against this risk, Honeywell recommends you not to connect laptop computers to the PCN. Instead, you must adopt other approaches such as using the Terminal Server in the DMZ when you need to make configuration changes.

If this is not possible, you should check the state of a laptop before allowing it to be connected to the PCN. As a minimum you must perform the following:

- Check the patch level of the operating system. If it is running Microsoft Windows, ensure that all current security hot fixes have been installed.
- Check the antivirus software on the laptop. The latest antivirus engine and virus definition files must be installed and properly configured.
- Perform a full system virus scan and view the log file to check that no files or directories were skipped, and that the virus scan successfully completed.
- Audit the software on the laptop to ensure compatibility of the laptop software with the control system software.

These audits and checks must be performed by a qualified independent person. The audit must not be undertaken by the user of the laptop. Standards for security hot fixes, antivirus software and compatible software must be in place before the audit is performed.

Once the state of the laptop has been verified, it can be connected to the PCN. If the laptop is disconnected from the PCN at any time and connected elsewhere, it must be checked again prior to reconnecting. It is strongly recommended that laptops not be used for web browsing prior to connection to the PCN.

Permanently connected non-Honeywell computers

Non-Honeywell computers connected to the PCN must conform to the recommendations in this document. This includes at a minimum:

- Up-to-date antivirus software
- Up-to-date Microsoft security hot fixes
- Strong passwords for all accounts
- A "least privilege" access model for users of the computer: users should only have access to resources required to perform their task.

11.9 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 must 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.

Unused physical ports on the process control network's infrastructure equipment (for example, switches and routers) should be disabled and then only enabled when needed through your site's change management procedure.

11.10 Domain name servers

Whenever a TCP connection (that is, a DSA node, Station or other client tool) is made, the system has to convert the user-provided host name into an IP address. This is usually performed by the Domain Name Server (DNS), a service generally hosted by the domain controller. In turn, this DNS consults other DNS systems, both internal and external on the Internet to resolve unknown names. There is a well-known attack method, known as cache poisoning, which results in incorrect resolution, generally aimed at leading web browsers to rogue sites which causes malware to be downloaded. Since users should not be web browsing from within the control network, the intended attack is not successful, but a possible side affect is that clients are unable to find the host, resulting in Station or DSA nodes being unable to connect.

The mitigating actions include the following:

- Isolating the process control network (PCN) DNS from the business LAN using firewall protection
- Hardening the DNS, W200x has a registry setting which causes the DNS to reject some false updates.
- Using the local hosts file on each client machine in place of a DNS to perform the resolution.

Use of the hosts file provides protection from DNS poisoning attacks, but has some administrative disadvantages in that each client must be manually updated if IP addresses change. One approach is to have a central copy of hosts which is copied to each node when required. This also acts as a backup should an individual hosts file become corrupted.

Unfortunately some malware also targets the hosts file, usually adding its own entries. This threat is greatly reduced by the presence of anti-virus software, by setting tight file permissions on the file (by default only Administrators can modify it), and by marking the file as read-only. If corruption still occurs, then only one machine is affected; if DNS corruption occurs, then all nodes are affected.

11.11 Remote access

Remote access allows connection to the process control network (PCN) from outside the business network using a corporate WAN, the Internet, or a dial-up connection. The client connects to a Remote Access Service (RAS) server placed on the business LAN or in the DMZ, where authentication occurs, then uses various tools to reach the target system. Security aspects of RAS configurations are discussed in “Remote Access Server” on page 176.

The access may be used for the following:

- Perform remote control from home after normal hours or for emergency situations. In this case the client would run Station as if it were an in-house Level 4 user. This would either be through a DSA node in the DMZ (assuming there is one and that the server allows the required access) or directly to the Level 2/3 server that owns the points to be controlled.
- Perform engineering tasks on an Experion system in a remote plant. In this case, the client would connect to the Engineering Terminal Services Server (the RESS described in section “Remote access for Station and Configuration Studio” on page 101) and then proceed as a normal Level 4 user.
- Perform remote support by Honeywell engineers or other support staff. In this instance, more direct access to the target machine is needed and tools such as Altiris Carbon Copy or Remote Administrator (Radmin) are used.

  If an RAS server outside the PCN is used then additional ports need to be opened in the firewall to allow the Carbon Copy (or other tool) client and server to communicate. These ports would be shut off as soon as the support project was complete. An alternative, and simpler, method is to connect a modem directly to the target machine. This limits the remote access to the target, but places a modem within the protected PCN area, which must then be carefully managed and disconnected when not in use. It may also be beneficial to have a special account that is used only by the remote support user and is disabled when connection is not expected. You can achieve this automatically by specifying a short password age time.

Where modems are used regularly for dial-in purposes, they should be set for auto re-dial if possible. This only allows calls to pre-configured phone numbers, thereby preventing attacks from unknown sources.

11.12 Dual-homed computers

Honeywell recommends you to not 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 must be through the firewall.

11.13 Dual home configurations for SCADA server

- Ensure that the lower MAC address is selected for FTE network installation. As the Dell servers like Dell 320 have four built-in NIC interfaces, ensure to use the first two NICs for FTE connection and other two NICs for IEC 61850 network connections. If you have installed additional dual NICs on two NIC built-in type server, ensure that lower MAC address NIC is selected for FTE. With this setup, Experion installation automatically selects the lower MAC interfaces (first two interface of built-in NICs) for FTE and system management and also sets proper binding order that FTEMUX is on top .
- Disable the IP routing between the FTE interfaces and the IEC 61850 interfaces.
- Disable Microsoft Windows Client and File Sharing for the IEC 61850 ports on the SCADA server.
- Change the TCP/IPv4 interface metric on both the IEC 61850 interfaces to 5 and 10, and disable netBIOS on both IEC 61850 interfaces.
- Do not include a gateway address on either IEC 61850 interface with an assumption that gateway address is already defined on the FTEMUX.

To verify IP routing is disabled

1 Choose **Start > All Programs > Honeywell Experion PKS > Server > Diagnostic Tools > Experion Command Prompt**.
The **Experion Command Prompt** window appears.

2 Type `ipconfig /all` and press ENTER.
The IP configuration details are listed.

3 In the **Windows IP Configuartion** section, ensure that the value of **IP Routing Enabled** is set as **No**.

To disable Microsoft Windows Client and File Sharing for the IEC 61850 ports on the SCADA server

1 Choose **Start > Control Panel**.
The **Control Panel** window is displayed.

2 Perform one of the following depending upon your operating system.

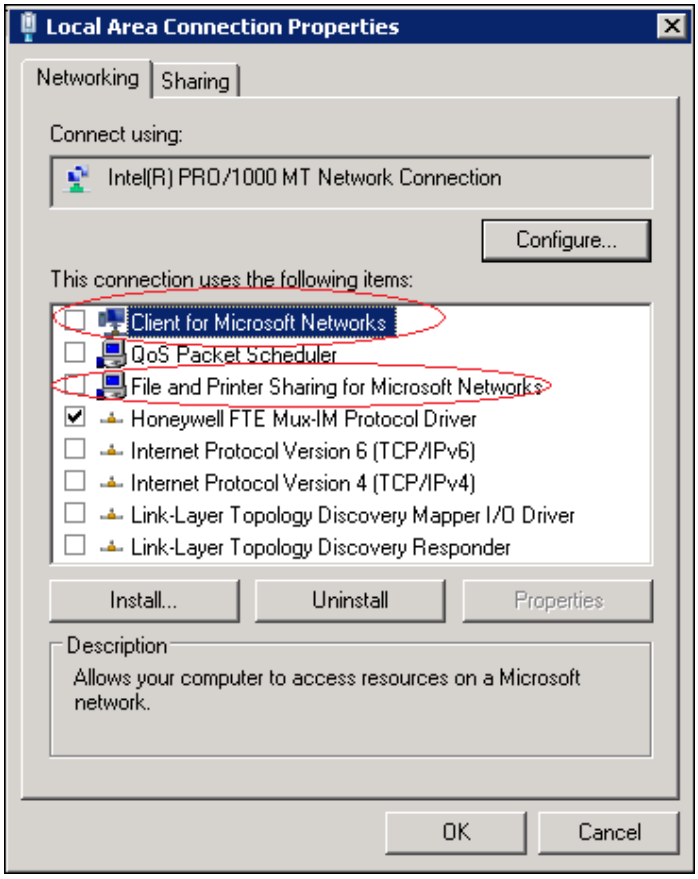
Option	Description
Windows 7	Click **Network and Internet > Network and sharing Center > Change Adapter Settings**.
Windows Server 2008	Click **Network and sharing Center > Manage Network Connections**.

The **Network Connections** window is displayed.

3 Right-click the network connections and choose **Properties**.
The **User Account Control** dialog box is displayed.

4 Click **Continue**.

5 In the **Networking** tab, disable the following options.
- Client for Microsoft Networks
- File and printer sharing for Microsoft Networks



6 Click **OK**.

To change the TCP/IPv4 interface metric and disable netBIOS

1 Choose **Start > Computer**.

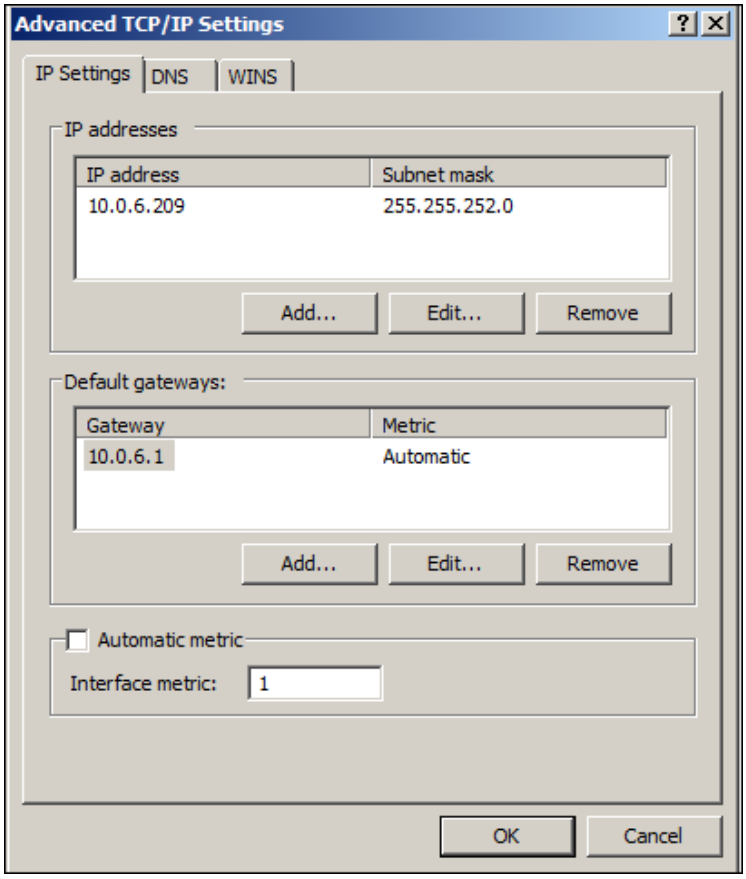
2 Right-click **Network** and choose **Properties**.

3 Right-click on the **DHEB Network connection** and choose **Properties**.

4 Select **Internet Protocol (TCP/IP)** and choose **Properties**.

5 Click the **Advanced** button on the **Internet Protocol (TCP/IP) Properties** window.

6 In the **Interface Metric** box, specify **5** for one IEC 61850 interface.



7 Click the **WINS** tab.

8 Click **Disable NetBIOS over TCP/IP** and then click **OK**.

9 Click **OK** on the **Internet Protocol (TCP/IP) Properties** dialog box.

10 Click **OK** on the **DHEB Network Properties** dialog box.

11 Repeat the above steps to change the **TCP/IPv4 interface metric** on the other IEC 61850 interface to **10**.

11.14 Port scanning

Only allow port scanning at the perimeter of your process control network (PCN), that is, from outside the firewall, pointing into the DMZ. Do not allow port scanning of online systems within the PCN, as this could lead not only to performance degradation, but to system failure.

11.15 Configuring secure communication settings

Before migration if you have unassigned the secure nodes for operating system change, then after migration use the **Secure option** in the Secure Communications user interface to secure the unassigned nodes. For more information about securing a node, refer to the *Secure Communications User's Guide.*

12 Securing controller hardware

Related topics

12.1 Ensure that only Honeywell-approved applications and services are installed

Only Honeywell-approved applications and services should run on nodes residing on a Honeywell FTE network on which secure C300 Controllers, and/or EUCN nodes, and/or secure FIM4/8 modules reside. This restriction decreases the likelihood that an application or service may either inadvertently or maliciously produce network traffic which compromises the network (for example, a network ‘storm’ or Denial-of-Service attack) or impairs the operation of the C300 Controllers, and/or EUCN nodes, and/or FIM4/8 modules reachable on that network.

12.2 Ensure that proper Access Management Policies and Permissions are configured and enforced

Unauthorized tampering with control strategies or operational parameters, unauthorized C300 Controller or EUCN node or FIM4/8 module state changes and unauthorized initiation of firmware update are all significant security threats which are managed in the Experion system via the proper definition and enforcement of access management permissions and policies.

12.3 Anti-Virus and Patch Management

It is strongly recommended that a Honeywell-approved anti-virus application be used on all appropriate nodes on an Experion system and that these applications be maintained up-to-date with respect to virus and malware definitions and latest version of the application itself. It is strongly recommended that the latest approved operating system patches be applied to all nodes running the Windows operating system. Honeywell maintains a Honeywell Qualification Matrix (HQM) on HoneywellProcess.com/support. The HQM matrix lists all Honeywell supported products, and all patches supported for each release, including Microsoft and other 3rd party software patches. It is strongly recommended that other Honeywell-approved applications running on Experion Systems nodes be maintained up-to-date, especially when new versions of these applications are released that specifically address security issues.

12.4 Adhere to Guidelines and Rules in Experion Best Practice documents

In configuring and operating an Experion C300 system, adhere to the principles and best practices recorded in the following documents:

- Network Best Practices White Paper

12.5 Ensure limited Physical Access to CF9 Firewalls and associated C300 Controllers, EUCN Nodes and FIM4/8 Modules

Removing or damaging modules or disconnecting cables between a CF9 Firewall and the C300 Controllers, and/or EUCN nodes, and/or FIM4/8 modules, to which it is connected will result in disruption of essential functions (control, alarming and notification, ability to view and control the state of these devices). With this in mind it is essential that:

- Physical access to these devices be controlled
- CF9s only be connected to C300 Controllers, EUCN nodes, FIM4/8s, and Safety Managers
- The latest version of firmware for the CF9 be installed

12.6 Use recommended CF9 configuration

Revision JJ for CF9s to which EUCN nodes are connected.

12.7 Configure higher level switches as per Experion Best Practice documents

Only Honeywell-approved switches should be used in ‘higher levels’ of the network architecture (L2 and above.) These should be configured according to Honeywell Best Practices documents using Honeywell-approved tools and configuration files provided by Honeywell.

12.8 Must use PM I/O or Series C I/O only

Essential control functions in a secure C300 Controller system must use the IO Link network which is connected directly to the C300 Controller on which these functions execute and the IO devices residing on these networks. The reasons for this are as follows:

- These IO networks have no direct connection to the Ethernet/FTE networks connecting to higher levels of the system and hence are protected to a significant extent from attacks via the Ethernet/FTE network by their isolation.
- Points of connection to these IO networks are (or should be) protected from easy access and tampering by physical measures required in secure systems (for example, they are located within locked cabinets).

12.9 Place peer C300 Controllers and FIM4/8 ‘under’ one CF9 for more secure connections

The CF9 Firewall provides very important protections against malicious attacks to the C300 Controller and FIM4/8 modules connected to it. It blocks traffic identified as suspect and blocks ports and protocols not used by these modules. Peer-to-Peer connections which span across multiple CF9’s expose the data transferred to network segments which do not provide maximum security protections. Hence peer connections between C300 Controllers and/or FIM4/8 modules are most secure when the entire path remains ‘under’ a single CF9. Since all peer-to-peer connections may not be possible under a single CF9, the user should place the most critical modules under the same CF9 Firewall.

12.10 Place EHPM and applicable EPNI2 nodes ‘under’ a seperate CF9 to avoid excessive multicast activity

Do not connect EUCN nodes and Series C controllers to the same CF9. The CF9 with the revision FF or above detects the extra multicast port needed by the EUCN nodes automatically and opens the port for EUCN nodes connected to that CF9. Maintaining separation of EUCN and Series C controllers will prevent these packets from getting into a C300 or FIM4/8 which might result in excessive multicast activity.

12.11 Do not configure or load support for functionality not to be used in a secure system

The C300 Controller, EUCN nodes and FIM4/8 only enables the protocols and TCP/UDP Ports required to support the configured system. As an example, the protocols and ports required to support PROFIBUS™ via the PGM or MODBUS-TCP™ using PCDI are only enabled if the configuration loaded to a C300 Controller includes function blocks and interfaces associated with these devices and networks. Considering these, a secure system will:

- Not use any functions which are not permitted in a secure system (for example, since only Series C and PM I/O are permitted, PROFIBUS™ via the PGM and MODBUS-TCP™ via PCDI cannot be used in a secure system).
- Not include configuration for any functions not permitted in a secure system even if the physical devices (for example, PGM) are not installed in the system.

12.12 Denial-of-Service

Denial-of-Service attacks may work via a number of different mechanisms. For example they may be intended to consume so much execution time on the target under attack that critical functions on the target do not get sufficient time to execute in a timely fashion. They may also attempt to consume so much memory (for example, communications buffers) that essential functions cannot get the memory they need to perform properly. In the case of the C300 and the EHPM Controllers, the most essential function is execution of control algorithms and CPU is a key resource. The C300 and the EHPM Controller have the following protections against Denial-of-Service attacks:

Control overrun protection

The C300 and the EHPM Controller implement mechanisms supporting ‘graceful degradation’ of control when there is not sufficient CPU to execute control at the rates configured. Note that when such a condition exists, appropriate alarms are generated.

Overload protection

The C300 and the EHPM Controller implement mechanisms to ensure that if it is grossly overloaded, CPU time is reserved to maintain communications. This in turn allows an operator or engineer to take measures to unload the C300 and the EHPM Controller by deleting control strategies or to set the C300 and the EHPM Controller state as required by the circumstances.

When CPU time available (that is, CPUFREE) falls below 10%, an alarm is generated. This alarm cannot be disabled.

Throttling

The C300, EUCN nodes and FIM8/FIM8 perform message throttling using 802.x flow control and by disconnecting from the network under extreme packet rates. This helps these nodes to maintain control strategies and local control.

CF9 Blocking

The CF9 Control Firewall blocks unused TCP and UDP ports, as well as throttling broadcast, multicast and other normally low-frequency traffic.

12.13 Use C300 Controller, EUCN Nodes and FIM4/8 redundancy

Device redundancy is optional, but it is recommended for higher availability, that is, protection against hardware faults. In some cases, redundancy may also provide an additional layer of recovery in the face of denial-of-service attacks.

12.14 In FOUNDATION FIELDBUS™ configurations use only ‘Fieldbus-Local’ control

The FIM4/8 is a FOUNDATION FIELDBUS™ **gateway**. As such it does **not** perform control, rather it administers the Fieldbus links on which it resides (providing and managing the link schedule, and so on) and the FIM4/8 communicates with any associated C300 Controller via a peer connection. This peer connection may be disrupted during a ‘network storm’ or denial-of-service attack but will be re-established upon cessation of the storm or attack. With these facts in mind, essential control functions on a secure FOUNDATION FIELDBUS™ system must execute on the Fieldbus link. Control involving loops from a Fieldbus input device (via the FIM4/8) to a C300 Controller and back (via the FIM4/8) to a Fieldbus output device are not permitted in a secure C300-FIM4/8 FOUNDATION FIELDBUS™ system.

12.15 Report a Security Vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software. Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services. To report a potential security vulnerability against any Honeywell product, follow the instructions at: https://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

- Send an email to security@honeywell.com
- Contact your local Honeywell TAC or support center listed in the “Support and other contacts” section of this document.

13 Securing Wireless Devices

When planning to connect wireless devices to your Experion system, you need to consider the topics described in this section.

This section provides high-level guidance for users with knowledge of, and experience with, installing wireless systems. It is therefore assumed that readers are familiar with terminology such as MAC address, PEAP, RADIUS, and SSID.

Related topics

"About Experion wireless devices" on page 140
"Radio frequency survey" on page 141
"Configuring and securing WAPs" on page 142
"Connecting wireless devices" on page 144
"Securing the OneWireless Network" on page 149

13.1 About Experion wireless devices

The Experion system includes the following wireless mobile productivity devices.

- IntelaTrac PKS for collecting field data
- Mobile Station for allowing remote access to the control system.
- Experion Mobile Access for accessing key process data and alarms on a web browser, optimized for smaller hand-held devices.

These mobile productivity devices connect through commercially available wireless access points (WAP). WAPs are typically connected to a wired network, which connects the wireless devices and servers on the wired network.

As this connection can represent a significant security risk for the servers and other parts of the wired network, it is essential that the recommendations for connecting the WAPs in this guide are followed.

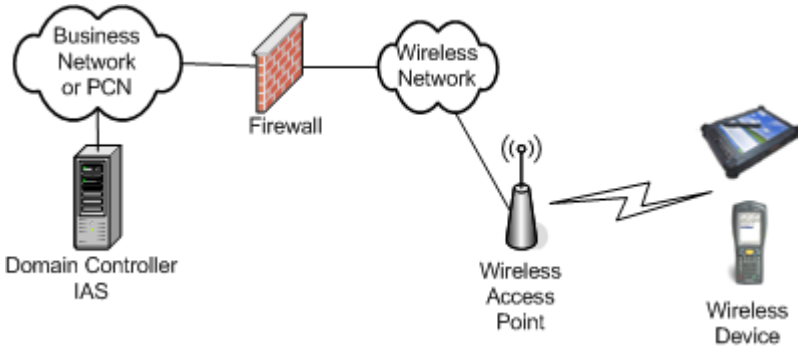
13.2 Radio frequency survey

Prior to deploying wireless devices, a radio frequency (RF) survey should be carried out to determine the following:

- Areas of the facility where wireless access is needed
- Areas of the facility where wireless access must not be allowed or made available
- The number and placement of Wireless Access Points (WAPs)
- Antennae strengths for each WAP

13.3 Configuring and securing WAPs

The basic implementation of a wireless device connection is illustrated in the following image. This displays the components of the network used to secure the wireless access point (WAP). Components that communicate with the wireless devices for data are described in subsequent sections.



Connecting wireless devices

The wireless device should not connect directly to the process control network (PCN). It is recommended that the WAP be connected to a separate network segment, separated from the network by a firewall. The WAP must have access to a Microsoft Windows domain controller which is running Microsoft's Internet Authentication Service (IAS). IAS supports the 802.1x RADIUS protocol, which is used to securely authenticate the wireless device. This can be a domain controller in the PCN or the business networks.

The domain controller and IAS

The domain controller provides an additional layer of protection for the network. Traffic from the wireless device is blocked until the user has authenticated with the domain controller using RADIUS. Microsoft supports RADIUS in both Windows Server 2003 and Windows Server 2008 as part of the Internet Authentication Services (IAS) package. For detailed guidance on configuring wireless access with RADIUS see the Windows Server 2003 and Windows Server 2008 documentation.

Information on RADIUS is available in RFCs 2138, 2139, 2865 and 2866 of the IETF (http://www.ietf.org).

Firewalls

When wireless devices are used on an Experion network, the firewall must be configured to only allow traffic between the following:

- The domain controller running RADIUS (refer to “The domain controller and IAS”
- The nodes being accessed by the wireless devices
- The WAP(s)

The firewall access required between the WAP in the wireless network and domain controller running IAS is displayed in the following table.

Secure Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Wireless Access Point	Domain Controller IAS	Wireless Network	1812/UDP	RADIUS 802.1x
Wireless Access Point	Domain Controller IAS	Wireless Network	1813/UDP	RADIUS 802.1x

Configuring WAPs

When configuring a wireless access point (WAP) it is recommended that you perform the following:

- Configure a unique SSID. Do not use the default SSID.
- Disable SSID broadcast.
- Configure authentication for EAP authentication to the Network. PEAP is preferred.
- Configure the RADIUS server address.
- Configure for dynamic WEP.
- Configure 802.1x authentication.
- Enable MAC filtering and enter MAC addresses for wireless Stations.

For detailed configuration information refer to the setup instructions from the WAP supplier.

Wireless network interface cards

The wireless device, IntelaTrac PKS or Mobile Station, contain a wireless network interface card. The following configuration recommendations must be followed:

- Configure the proper SSID
- Configure 802.1x authentication
- Configure WEP with key supplied from WAP
- Configure Protected EAP authentication Note: both PEAP-TLS and PEAP-MS-CHAP are supported.

For more information on wireless security recommendations refer to the following links.

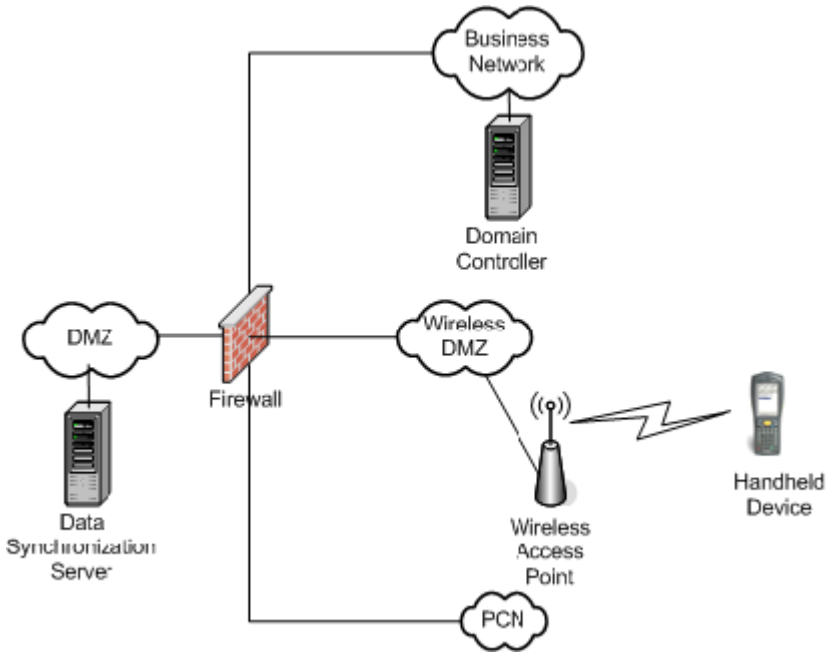
- http://cnscenter.future.co.kr/resource/hot-topic/wlan/1350.pdf
- http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html (Download the Cisco Aironet Wireless LAN Security Overview document.)
- http://www.microsoft.com/technet/community/columns/cableguy/cg1202.mspx
- http://technet.microsoft.com/en-us/library/cc759077(WS.10).aspx

13.4 Connecting wireless devices

This section describes the connections for wireless access in an Experion system.

IntelaTrac PKS

The IntelaTrac PKS hand-held wireless device connects to the data synchronization server. The IntelaTrac PKS interface does not require access to the process control network (PCN). It is recommended to place the data synchronization server in the wireless DMZ (Level 3.5). If no DMZ is present, then the data synchronization server should be placed on the Business Network. The following diagram shows the best practice for IntelaTrac.



Note in this diagram that the WAP resides in the Wireless DMZ and IntelaTrac PKS Data Synchronization Server resides in the DMZ. IntelaTrac PKS users are authenticated with the domain controller IAS in the business network. Additional nodes are included in an IntelaTrac system, the Database Server and Decision Support Systems. It is recommended that these nodes be located in the DMZ or on the business network. For more information, refer to the *IntelaTrac PKS System Installation Guide, IntelaTrac PKS Version 2.4*.

Authentication, firewall access and wireless device configuration are described in the section “Configuring and securing WAPs” on page 142.

The firewall configuration for Data Synchronization Server and other IntelaTrac PKS system components, such as the IntelaTrack PKS database and PHD depends upon what options are being used. Details are contained in the two following documents:

- *IntelaTrac PKS System Installation Guide, IntelaTrac PKS Version 2.4*
- *Administration User's Guide, IntelaTrac PKS Version 2.4*

Refer to these documents for detailed information on the port configuration required.

Further reference information is available in the following:

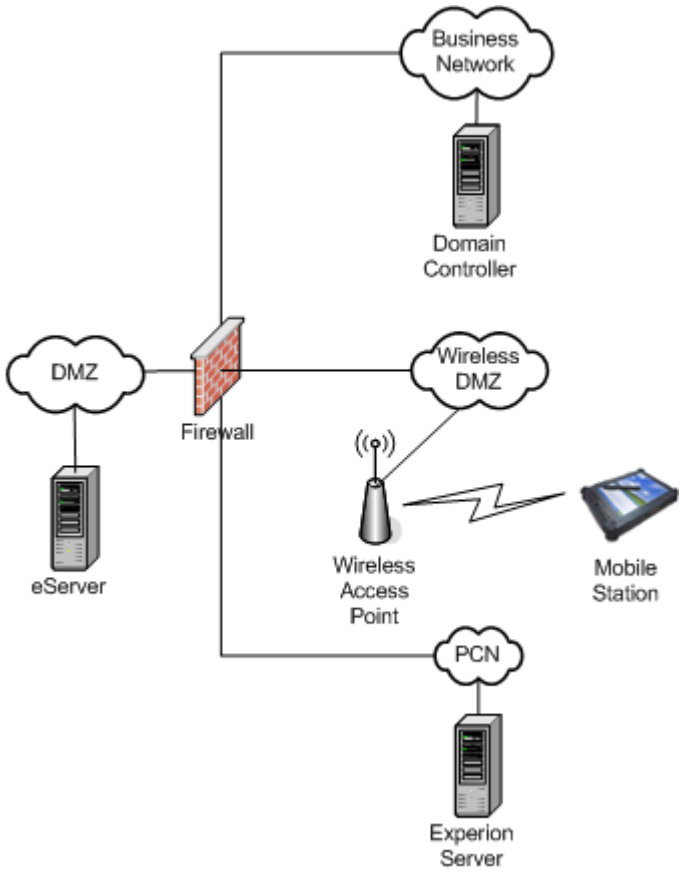
Mobile Manager for Pocket PC User's Guide, IntelaTrac PKS Version 2.4

Mobile access for eServer

Mobile Station devices have three ways of connecting to Experion. Two of these provide access through an eServer. For this type of access, the eServer resides in the Level 3.5 DMZ.

eServer Standard Access

The following image illustrates the Mobile Station Access for eServer Standard.

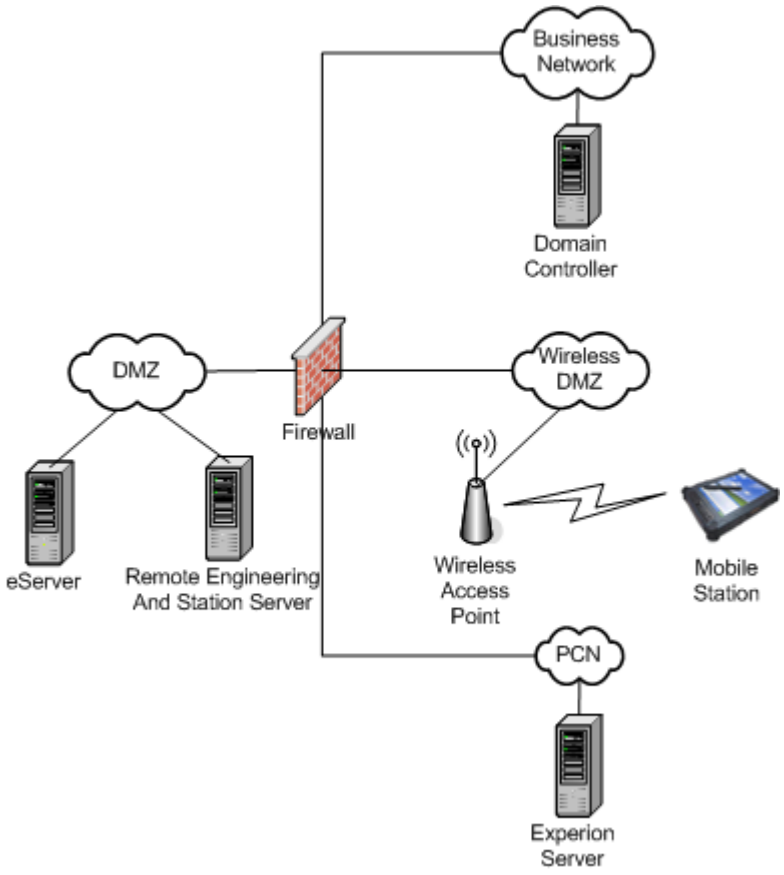


Note in this image, the WAP resides in the wireless DMZ. The domain controller with IAS is in the business network. In general, it is a better practice to use the domain controller in the business network.

Authentication, firewall access and wireless device configuration are described in the section “Configuring and securing WAPs” on page 142. Firewall access between the eServer and Experion server is illustrates in the eServer topics of “Configuring the DMZ firewall” on page 93.

eServer Premium Access using Terminal Services

The following image illustrates the Mobile Station Access for eServer Premium.

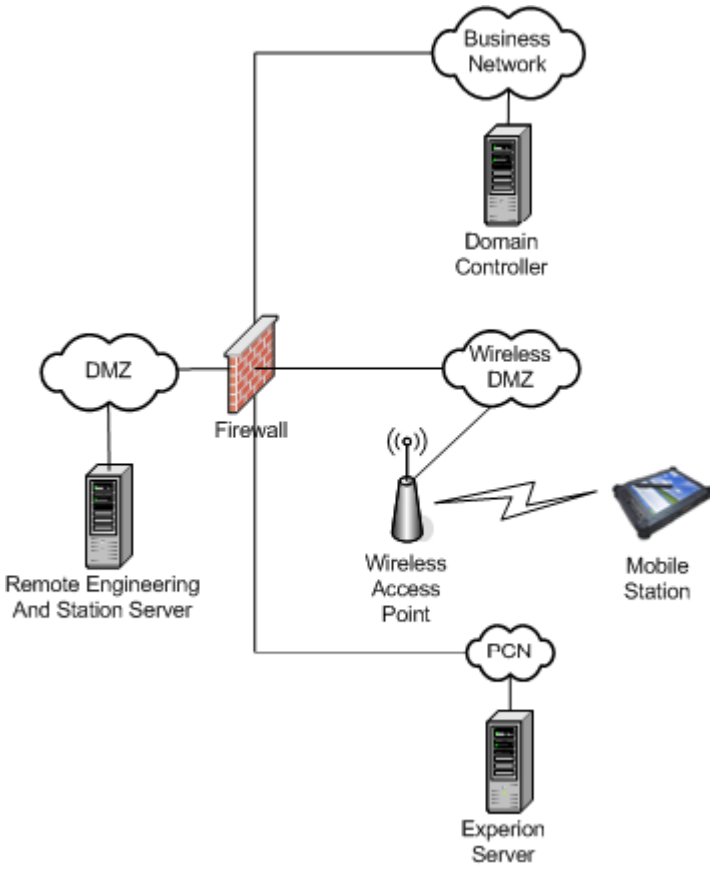


Note in this image, the WAP resides in a wireless DMZ. The domain controller with IAS is in the PCN.

The eServer obtains information from the Experion server in the PCN via DSA. The firewall access and account requirements for DSA are described in section “Distributed system architecture” on page 93. Authentication, firewall access and wireless device configuration are described in the section “Configuring and securing WAPs” on page 142. Firewall access between the eServer and Experion server is displayed in the eServer topics of “Configuring the DMZ firewall” on page 93.

Mobile Station

The following image illustrates the Mobile Station.

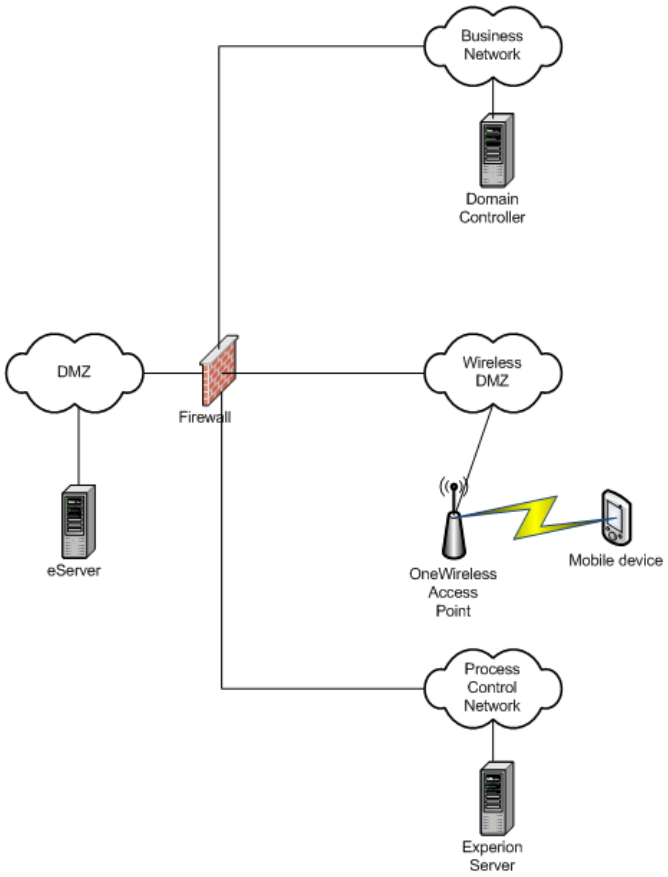


Note in this image, the WAP resides in a wireless DMZ. The domain controller with IAS is in the business network.

Authentication, firewall access and wireless device configuration are described in the section “Configuring and securing WAPs” on page 142. Firewall access between the eServer and Experion server is displayed in “Remote access for Station and Configuration Studio” on page 101.

Experion Mobile Access

The following image illustrates the Experion Mobile Access.

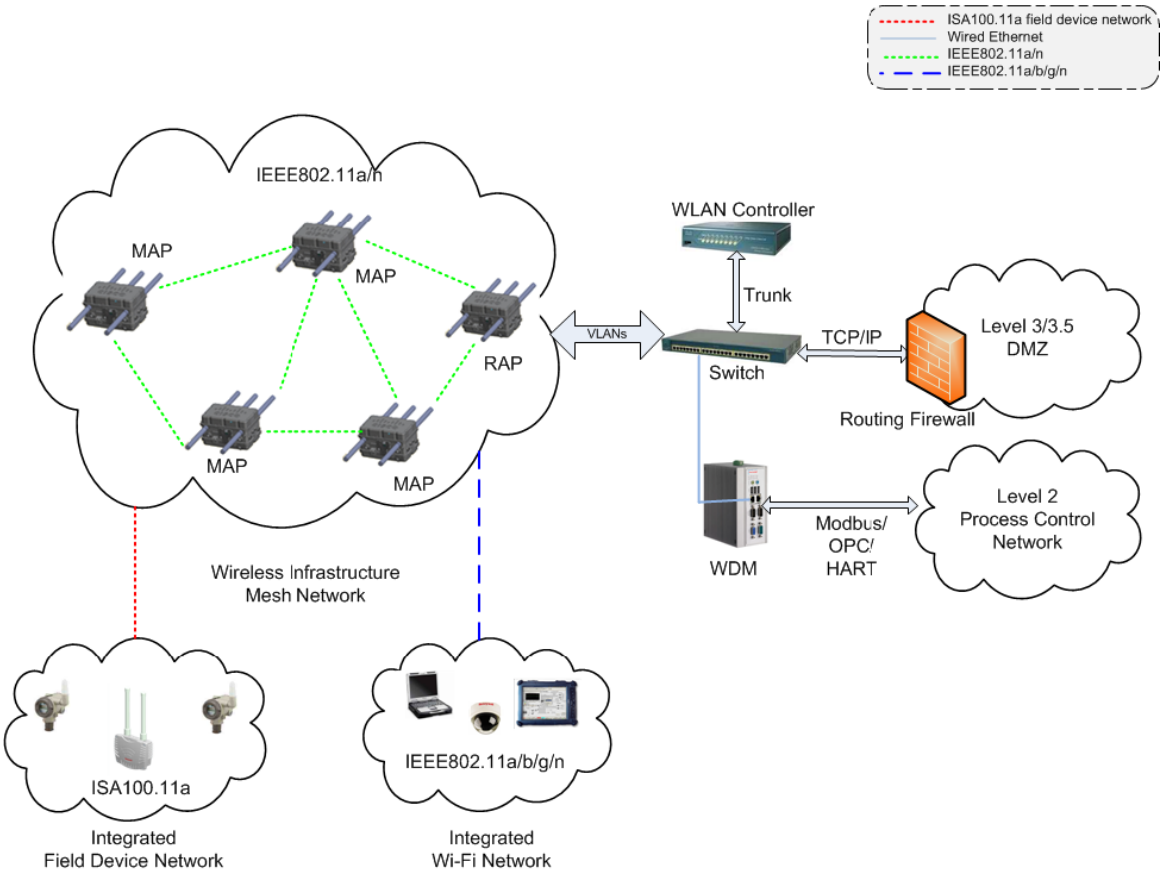


Note in this image, the WAP resides in a wireless DMZ. The domain controller with IAS is in the business network.

13.5 Securing the OneWireless Network

OneWireless and Experion systems

The following topology diagram illustrates the OneWireless network integrated with the Experion system.



IEEE 802.11a/b/g WLAN network security

The IEEE 802.11a/b/g/n WLAN utilizes a combination of access control, VLAN, and encryption over Control and Provisioning of Wireless Access Points (CAPWAP) to protect the WLAN network. The configuration and security scheme of the Cisco 1552S Access Point used in the OneWireless Network is controlled by the WLAN controller. All data from Wi-Fi clients and ISA100.11a devices using the WLAN mesh are encapsulated with the CAPWAP protocol and transmitted to the WLAN Controller. The WLAN Controller removes the encapsulation and forwards the data to the appropriate consumer over the wired network. Perform the following methods of security to secure the WLAN network.

- Enable MAC address white list on the WLAN Controller to ensure that only authorized Cisco 1552S APs join the IEEE 802.11 mesh network.
- Use VLAN tagging to separate traffic between different Wi-Fi services utilizing the WLAN mesh network. Such traffic from the management VLAN must be separated. Note that the ISA100.11a backbone router in the Cisco 1552S AP resides on the management VLAN of the Cisco WLAN Controller.
- VLANs that are used to separate the traffic cannot be used as security barriers. Therefore the guests or other untrusted user traffic should not be permitted on this network. Separate APs should be set up in areas where this traffic is required and routed through the appropriate security level network.
- Enable IEEE 802.1x security for Authentication, Authorization, and Accounting (AAA) in combination with IEEE 802.11i (WPA2) to secure the Wi-Fi client network. The Microsoft version of a RADIUS server is the Internet Authentication Service or IAS, which is available free with Windows Server 2003 and is easily

added to an active directory domain controller. FreeRADIUS and open source AAA server is also supported by the Cisco WLAN Controller.

- Protect the mobility group name and RAP/MAP MAC addresses as they are used in network security.
- Configure firewall access lists to provide wireless access to only legitimate subnets on the PCN.

Placement of OneWireless multinodes

Multinodes have three antennas, which are used for the following purposes.

- Wi-Fi access point
- Mesh network
- Sensor network

Multinodes must be strategically located to achieve the following within the Experion system.

- Form a mesh network with multiple redundant paths
- Provide dual sensor network communication paths to each field device
- Increase the Wi-Fi coverage for Wireless Worker client applications within the customer’s installation

14 System Monitoring

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 succeeds 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.

Related topics

“Using Microsoft Baseline Security Analyzer” on page 152
“Setting up and analyzing audit logs” on page 153
“Detecting network intrusion” on page 155
“Setting up an event response team” on page 156

14.1 Using Microsoft Baseline Security Analyzer

It is recommended that you download and run Microsoft Baseline Security Analyzer (MBSA) on your system.

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 hot fixes, 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.

14.2 Setting up and analyzing audit logs

It is recommended that you enable the auditing of your file system and registry access. 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.

Considerations

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 (for example, "Overwrite events as needed"), and check the log frequently enough to prevent loss of events.

To view the log settings, start the Event Viewer tool, select **Log** > **Security** and then select **Log** > **Log Settings**. Then change either the Maximum Log Size, or the Event Log Wrapping options.

Ensure that the audit log is regularly inspected and cleared, or else disable the security option "Audit: shut down system immediately if unable to log security audits".

Configuring the log settings to overwrite will ensure that the system never stops when the log is full but this can also be used to hide events of interest by falsely filling the log with other events. This highlights the need for regular monitoring.

You can also configure the System Event Server to send system events to the Experion alarm and event subsystem when certain thresholds are reached in the audit logs. For more information, refer to the chapter "Configuring system performance and event monitoring" in the *Server and Client Configuration Guide*.

To enable auditing

1. Set the appropriate Group policy, or 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), you must specify the group "Everyone".

To configure the auditing of file access

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".

To configure the auditing of 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 mentioned in the previous procedure.

To enable the auditing of Experion database access

1. Before starting the database service, give the "Everyone" account "Generate security audits" rights.
2. Enable audit object access.
   This will ensure that any attempt by an executable to open the Experion database will also generate a security log entry.

14.3 Detecting network intrusion

Network Intrusion Detection Systems (NIDS) can take many forms. NIDS can be a dedicated server on the same network branch, freeware software available under GNU or similar licenses (most of these are aimed at the UNIX world), or commercial products aimed specifically at Windows systems.

The purpose of NIDS 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.

Most firewalls, switches and routers have reporting facilities whereby they can report various levels of events, varying from debugging to emergency failure. These reports can be either viewed via telnet, collected by a central logging server, or be sent via e-mail to an administrator. For example, the Cisco PIX firewall and Catalyst 4500 switches can be configured to send selected levels of events to a central syslog server where further analysis can occur and significant events be detected.

Syslog servers commonly exist on Unix systems, but third party syslog services are available for Windows. They vary in functionality and cost from freeware, which simply writes to a log file, to sophisticated IDS systems which analyze the logs in detail. As well as being able to control the level of severity of events, the PIX firewall allows the suppression of individual messages. This can significantly reduce the clutter and also provides some ability to recognize common attack signatures and to raise appropriate alarms.

When configuring the logging of these network events, a balance must be kept between collecting too many acceptable events (and missing something important) and between filling storage disks and deleting information (which is subsequently needed for an intrusion investigation).

The following is a typical log from a firewall.

```
Jun 03 14:17:44 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp
src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX (type 0, code
0) by access-group "outside_access_in"
Jun 03 14:17:49 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny tcp
src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX by access-group
"outside_access_in"
Jun 03 14:17:51 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp
src outside:XXX.XXX.XXX.XXXX dst inside:XXX.XXX.XXX.XXX (type 0, code
0) by access-group "outside_access_in"
Jun 03 14:17:51 XXX.XXX.XXX.XXX local4.err %PIX-3-305005: No translation
group found for tcp src inside:XXX.XXX.XXX.XXX dst outside:XXX.XXX.XXX.XXX
Jun 03 14:17:57 XXX.XXX.XXX.XXX local4.err %PIX-3-305005: No translation
group found for tcp src inside:XXX.XXX.XXX.XXX dst outside:XXX.XXX.XXX.XXX
Jun 03 14:18:01 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp
src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX (type 0, code
0) by access-group "outside_access_in"
Jun 03 14:18:11 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp
src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX (type 0, code
0) by access-group "outside_access_in"
Jun 03 14:18:23 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp
src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX (type 0, code
0) by access-group "outside_access_in"
```

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.

14.4 Setting up an 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://technet.microsoft.com/hi-in/library/cc184906(en-us).aspx
- http://www.sans.org/resources/
- http://csrc.nist.gov/
- http://www.us-cert.gov/control_systems/

15 Windows Domains and Workgroups

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.

Related topics

“About domains and workgroups” on page 158
“Comparing domains and workgroups” on page 159
“Implementing domains and workgroups” on page 160
“Inter-domain trusts” on page 161

15.1 About domains and workgroups

Domains

A Windows 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 account 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.

Workgroups

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.

15.2 Comparing domains and workgroups

This section discusses the advantages and disadvantages of using domain and Windows workgroups.

Feature	Windows Domain	Windows Workgroup
Security level	Greater level of security.	Reduced level of security.
Ease of maintenance	Central database of user and global security policies. Changes in the central database are applied to all computers within the domain.	Users and limited security settings need to be configured separately on each computer in the workgroup.
Required effort for security maintenance	If your Experion system contains more than 5 nodes, the use of a Windows domain controller can reduce the effort and cost for maintaining the user and security configuration in the system.	If your Experion system contains only a small number of nodes (less than 5), it is feasible to manage system security without a Window domain controller.
Windows domain controller server	Requires one or more separate servers to act as Windows domain controllers. An Experion server cannot be a Windows domain controller.	A Windows domain controller is not required.
Security model in Experion	You can use Integrated Security, where Experion users are defined within the Active Directory. Provides a consistent security model between Experion and the Windows operating system.	To use Integrated Security, users must be created on each computer, and then added to the Windows groups.

15.3 Implementing domains and workgroups

For more information, refer to the Windows Domain and Workgroup Implementation Guide. For planning information, refer to Windows Domain and Workgroup Planning Guide. For operation system migration information, refer the appropriate operating system-specific implementation guide Windows Domain Implementation Guide for Windows Server 2008 R2/Windows Domain Implementation Guide for Windows Server 2012..

15.4 Inter-domain trusts

Inter-domain trusts are used to allow users in one domain to access resources on a different domain. Native Windows 2003 Server and Windows Server 2008 domains have implicit two-way trust relationships called transitive trusts between domains within a forest, and may have explicit trusts between domains in different forests.

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. It is recommended that you do not permit trusts between the process control network and business network domains. If no trusts exist, administrators can be assured that no access to Windows resources can be configured for users from other domains.

If trusts are necessary, then the "least access" principle should be followed: that is, only have the trusts that are required. Use a one-way trust if possible. Explicit trusts can be configured between Windows 2000, Windows 2003 and Windows 2008 domains.

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 server in the process control network domain.

If Stations do reside on the same domain as the Experion server then single sign-on for operators is possible; that is, Station will be able to automatically connect to Experion using the same credentials as those used when the operator logged onto the Station computer. For more information, refer to "Single Signon" topic under “Configuring System Security” section in the *Server and Client Configuration Guide*.

16 Securing access to the Windows operating system

An essential component of any security strategy for a process control network is to secure access to the operating system to ensure the following:

- Only authorized users have access to the system
- User access to files, systems, and services is limited to those necessary for the performance of their duties

Related topics

"Windows user accounts and passwords" on page 164
"Honeywell High Security Policy" on page 167
"File system and registry protection" on page 170
"System services" on page 172
"Other Microsoft services" on page 175
"Use the firewall on Windows 7 and Windows Server 2008 machines" on page 177
"Windows 7 and Windows Server 2008 registry and other settings" on page 178

16.1 Windows user accounts and passwords

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. User account and password policies are therefore important security measures.

16.1.1 User account policies and settings

As a general rule you must perform the following:

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

Experion operator accounts

Experion operator accounts must be set up to ensure the following:

- Enable them to log in only to operator Stations.
- Do not use a shared operator account if individual accountability is required.

Use Signon Manager to modify user credentials without loss of view.

Non-operator user accounts

Accounts for engineers and others who need interactive access to server nodes for maintenance activities must be enabled to log in to all process control nodes.

New accounts

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

Where Experion operator-based security is configured, similar care must be taken in choosing passwords. For more information about operator-based security refer to the topic "Administering users" in the chapter "System administration" of the *Server and Client System Administration Guide*.

Administrator accounts

Microsoft best practices for security encourage disabling the built-in Administrator account, and creating a site-specific account. This is because the SID (internal id) of the Administrator account is fixed and well-known, so it provides a security vulnerability that can be exploited.

Experion installation now disables the Administrator account, and prompts the user for a new account name and password, setting up the new account to be the initial system administrator. As site conventions dictate, additional administrative accounts may be created later.

For more information about Administrator accounts, refer to “Administrators” on page 184.

Service and server accounts

Windows services 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 the preferred order.

- “Local Service" account
- "Network Service" account
- Local accounts with minimum rights. Most Experion services run under the local “mngr” or “LocalComServer” accounts.

- Domain accounts with minimum rights
- Local or domain user belonging to the Local Administrators group
- Built-in "System"

Running services under the Built-in "System" account must be avoided, 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.

16.1.2 Password policies and settings

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.

Password settings

The Honeywell High Security Policy applies the following default password policies. These may be adjusted to site requirements using domain Group Policies, modifying local machine policies, or individually controlling each account.

The settings described in the following table are suggested.

Parameter	Setting	Comment
Maximum password age	45 to 90 days	Forces the choice of a new password after this time. The setting for the Administrator account should be shorter. A maximum of 30 is recommended. **NOTE**: it is disruptive to system operation to force some accounts (e.g. MNGR) to change passwords frequently. For such accounts, the “Password does not expire” option should be selected. This attribute should be used as little as possible.
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	10 attempts	Prevents continual password guessing by disabling account after the specified number of attempts. Consider disabling account lockout for operator (or other user) accounts where denial of service or loss of view would be detrimental to safety or the continued operation of the plant.

Parameter	Setting	Comment
Lockout duration	30 minutes	Specifies the period of time during which a user will not be able to log on following an account lockout. (Note that the administrator can re-enable the account before the expiration of the specified lockout period.)
Lockout counter	29 minutes	The time before the account lockout is reset to zero. For example, with the account lockout set at 10, and the lockout counter set at 29 minutes, lockout will occur if there are 10 invalid logon attempts within 29 minutes. Note that the lockout counter must be less than the lockout duration.

Strong passwords

It is recommended that you enforce strong passwords, that is, passwords consisting of at least 8 characters including one numeric. Weak passwords that are easy to guess provide an opportunity for unauthorized access. Minimum password complexity can be enforced by group policy or local password policy.

An alternative way of increasing password complexity is to recommend 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.

Account lockout

The lockout values displayed in Table 1 in “Password settings” are those suggested by Honeywell. Additional information is available in the Microsoft "Account Lockout Best Practices - White Paper" (Account Lockout Best Practices.doc) available at the following link.

http://www.microsoft.com/downloads/details.aspx?familyid=8c8e0d90-a13b-4977-a4fc-3e2b67e3748e =en

Account lockout policy must be used with caution. Although it will slow down an attempted password guessing attack; it will not prevent a determined attacker, who will capture logon packets and use cryptographic tools to break the password offline. It may also lead to a Denial of Service, where authorized users find themselves unable to log on. It is generally better to rely on strong passwords and system audit log monitoring to prevent and detect password cracking attempts.

16.2 Honeywell High Security Policy

The Honeywell High Security Policy leverages Microsoft Windows Groups and Group Policy to implement the Experion security model which enables you to control how programs, network resources, and the operating system behave for users and computers in your organization.

The Experion security model is based on roles, effectively classes of users on an Experion system. Honeywell has defined seven roles and makes use of the Microsoft-defined roles of System Administrator and User. The following table describes the roles defined by the security model.

Role	Description
Product Administrator	Administers Honeywell Experion software: SQL administration, HCI and other component configuration
Engineer	Engineering functions: display creation and deployment, CAB block development, point definition
Supervisor	Privileged operational activities
Operator	Normal operational activities
Ack View-Only	View privilege plus acknowledge alarms
View-Only	View privilege
Server/Service	Non-interactive accounts that may be used for the identity of services that do not fit with Microsoft's built-in accounts and servers/COM servers that need an identity to RunAs
Windows Administrator	Configure and maintain the Operating System and network: software installation, network settings, account creation/maintenance
User	No Experion privilege
Security Administrator	Configure and maintain Secure Communications

Windows groups are used to assign user accounts to roles, as described in the following roles group assignment table.

Role	Domain account group	Local account group
Product Administrator	DCS Administrators	Product Administrators
Engineer	Engineers	Local Engineers
Supervisor	Supervisors	Local Supervisors
Operator	Operators	Local Operators
Ack View-Only	Ack View Only Users	Local Ack View Only Users
View-Only	View Only Users	Local View Only UsersQ
Server/Service	DCS Domain Servers	Local Servers
Windows Administrator	Domain Admins	Administrators
User	Domain Users	Users
Security Administrator	SecureComms Administrators	Local SecureComms Administrators

By assigning a user account to a single role group, you assign the responsibilities of that role to the user. By assigning an account to multiple role groups, you authorize that user to perform activities appropriate to all assigned roles.

Permissions and privileges to local resources on each computer should always be set using local groups. These permissions will automatically apply to the equivalent global groups. Local user accounts should always be added to local groups to assign roles. Domain user accounts should always be added to global groups to assign roles. The domain accounts will inherit the permissions and privileges of the equivalent local group on each machine.

The High Security Policy provides an appropriate security configuration for each user role. The High Security Policy is based on the Windows security model, but has been tailored for use with Experion and related products with the addition of specialized security templates, accounts, and groups.

Attention
High Security Policy blocks a number of groups like the Windows-created group "Users" from using Experion. Only members of the domain or local groups Described in the table are assigned privileges within Experion.

16.2.1 High security policy, domains, and workgroups

The High Security Policy applies to both domain and workgroup environments, but as Windows only supports Group Policy in a domain, workgroups do not receive the full benefit of Honeywell's High Security Policy.

If you implement:

- A domain, Windows Group Policy is used to tailor the user environment based on roles. Group Policy settings apply to every domain user regardless of the computer they are logged on to.
- A workgroup, Group Policy does not apply, however a procedure is provided in the Windows Domain and Workgroup Implementation Guide to restrict the environment of selected users and groups.

16.2.2 Honeywell high security policy installation packages

The default Experion security policy is applied on Windows 7 and Windows 2008 Server (non-Domain Controllers) through installation of high security software packages. Honeywell supplies high security model as two separately installable packages on the Experion System Software CD/Experion Application DVD, they are as follows:

- **Experion – High Security Domain Controller Package** – This package creates the security components on the Domain Controller, including the secure Group Policy Objects (GPOs) and global groups.
- **Experion – High Security Workstation Package** – This package is installed automatically on every Experion node whether in a domain for workgroup, and optionally on other non-Experion nodes. It creates the security components on workstation or member server nodes.

Attention
For more information on Using High Security Policy, refer to the sections Implementing High Security Policy in a Domain environment and Implementing High Security Policy in a Workgroup environment in *Windows Domain and Workgroup Implementation Guide*.

Domain Controller - Experion – High Security Domain Controller Package

The domain security package installation performs the following tasks.

- Creates Group Policy Objects (GPOs) for each user type
- Creates global groups used to assign user roles (refer to the "Domain account group" column in the table described in section "Honeywell High Security Policy" on page 167)
- Assigns the GPOs to roles using the Honeywell global groups
- Creates one global account and assigns it to the appropriate global groups

The domain security package does not modify file or registry permissions on the domain controller other than those applied to the global policy object files as required by Microsoft.

Results

The following modifications are made when you install the High Security Policy Domain Controller Package.

- Several Windows global groups are created.
- One service user account is created and added to the correct global groups.
- Group Policy objects are installed.

- Group Policy objects are linked to the created global groups.

The following Windows global groups are created.

- DCS Administrators
- Engineers
- Supervisors
- Operators
- Ack View Only Users
- View Only Users
- DCS Domain Servers

The DCSComServer domain user is created.

Attention

TPSApp: This account is no longer automatically created. If needed, create site-specific account, which may be named TPSApp, if desired. Assign appropriate group memberships. This account has no default group.

TPSComServer: This account is no longer created in R431. Use DCSComServer instead.

Experion – High Security Workstation Package

The High Security Policy workstation package is automatically installed with Experion software. The following modifications are an overview of the changes made when the package is installed.

- Local Windows groups used to define security roles are created (refer to the “Local account group” column in the table described in section“Honeywell High Security Policy” on page 167)
- Honeywell-required local user accounts are created and assigned to the correct local groups.
- Creates proxy files for managing Honeywell application access
- Ensures the workstation DCOM settings support interoperation within the system
- Establishes local computer policy settings
- Registry and file permissions are updated to secure access
- Provides the Link Domain Groups commandthat you must run to make specific global groups members of local groups – this integrates the workstation into the domain security model

Results

Attention

To view the detailed settings made by the workstation security package, refer to the Workstation Security Settings section under Appendix chapter of the *Windows Domain and Workgroup Implementation Guide*.

16.3 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, in which each entry specifies 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.

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. New directories, files, or registry keys will inherit ACLs from their parent node.

When installed, Windows applies default ACLs to its system directories and registry trees to prevent malicious or accidental damage. Similarly, the Experion installation will apply ACLs to its directories and registry tree. In general, the site should not adjust those ACLs. However, for new files, folders, shares and registry keys, the site is responsible for adjusting or assigning permissions as appropriate to maintain an acceptable level of security. In most cases, Experion assigns modify permissions based on the local groups created by Experion installation, or the built-in administrators group. This is a best practice for site-created objects as well.

ACL protection can only be applied to files and directories if the containing file system is in NTFS format. Experion can only be installed on a disk partition with NTFS and so ACLs should be applied as described.

NTFS also supports the ability to encrypt files. Runtime data and executables are not suitable for encryption for performance reasons, but static configuration files such as those used by qckbld, and archived data such as history may be encrypted if the additional level of protection is required. Note, however, that file encryption requires additional administrative work in the form of key management.

Most Experion data files are contained within the *C:\Program Files(x86)\Honeywell* and *C:\ProgramData\Honeywell* directories except where site choices save files to other locations. Experion registry keys are saved under *HKEY_LOCAL_MACHINE\Software\Honeywell* and *HKEY_CURRENT_USER\Software\Honeywell*. Files, folders, and keys created within these areas will inherit a default set of permissions that in most cases will be adequate without user adjustments. Changing ACLs in these areas is not advised.

CAUTION
Changing ACLs for file and registry data used by Experion may either compromise the security of the control system, if security is made more open, or effect the operation of Experion if security is tightened.

16.3.1 File system ACLs

ExperionExperion configures default file system security during installation, and in general, those permissions should not be changed by the site. Unless directed by the user, Experion uses the following two major file system folders to contain the files necessary for operation.

- *C:\Program Files(x86)\Honeywell* contains the executable files that make up the Experion application, as well as some data files that are created by install, and generally do no require user modification. This directory tree is secured such that most users have read and execute access, but only Administrators and some other highly privileged Microsoft-defined groups have modify permissions.
- *C:\ProgramData\Honeywell* contains installed files and folders that are to be modifiable at runtime as well as those created during the running of the system. This tree also has general read access, but write access is restricted as follows:
  - *C:\ProgramData\Honeywell\ProductConfig* is intended for Experion administration files. By default, all files and folders created within this tree are writable by Honeywell's Product Administrators and Microsoft's Administrators groups.
  - *C:\ProgramData\Honeywell\EngineeringData* is intended for data created and maintained by the engineering role that should not be modified by other users. This folder assigns write access to Honeywell's Local Engineers and Microsoft's Administrators groups.

– All other files/folders under C:\ProgramData\Honeywellare general runtime data for Experion, and are assigned by default write access by all of Honeywell's groups plus the Administrators group.

Specific procedures for managing file system ACLs are described in the *Windows Domain and Workgroup Implementation Guide*.

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 from operating correctly.

16.3.2 Registry ACLs

Experion configures default registry security during installation, and in general, those permissions should not be changed by the site. Initial registry security is set as follows:

- *HKLM\SOFTWARE\Honeywell* is intended for Experion administration data. By default, all keys created within this tree are writable by Honeywell's Product Administrators and Microsoft's Administrators groups, with the exception of the two keys described below.
- *HKLM\SOFTWARE\Wow6432Node\Honeywell\EngineeringData* is intended for data created and maintained by the engineering role that should not be modified by other users. This key assigns write access to Honeywell's Local Engineers and Microsoft's Administrators groups.
- *HKLM\SOFTWARE\Wow6432Node\Honeywell\ProgramData* contains general runtime data for Experion, and by default is assigned write access by all of Honeywell's groups plus the Administrators group.

Specific procedures for managing registry ACLs are described in the *Windows Domain and Workgroup Implementation Guide*.

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 must back up any valued data on your computer. For detailed information about backing up and restoring system data like registries, refer to the *Backup and Restore Guide*.

16.3.3 File share Security

File shares must also be protected. By default, any directory which is made available for network access will give "read access" to the everyone group. Anyone on the network can read any file under the shared directory tree. This is generally too permissive. Any file shares created by the site should be careful to adjust share security to prevent unauthorized access/modification.

ExperionExperion configures share permissions on those shares required by Experion as follows:

- Read access should be allowed to only the Honeywell-created local groups and the Administrators group.
- Modify permission is granted only to those Honeywell-created local groups that require it, and the Administrators group.
- Broad groups such as “Users”, “Authenticated Users” and “ANONYMOUS LOGON” should be avoided for both read and write access.

16.4 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 itself runs as a set of these services, many of the system default services are not needed by Experion. However, they provide avenues for malicious network attack and must be disabled.

16.4.1 Services required by Windows operating system

For the list of Windows operating system services required by Experion, refer to the following links.

- http://technet.microsoft.com/en-us/library/dd349799(WS.10).aspx
- http://technet.microsoft.com/en-us/library/hh125927(WS.10).aspx

Ensure to identify the services that need to be disabled and perform the required testing if you make these changes.

16.4.2 Services required by Experion

The following table lists the Experion services installed during an Experion installation. Ensure to identify the services that need to be disabled and perform the required testing if you make these changes.

Service name	Description
Web Server (IIS)	Refer to “Other Microsoft services” on page 175 for more information.
Windows Terminal Services	Refer to “Other Microsoft services” on page 175 for more information.
SNMP	Simple Network Management Protocol

16.4.3 Services required by third-party applications

The following table lists the third-party application services required by Experion applications that are installed as part of an Experion installation.

Attention

Unless otherwise noted, the services listed in the following table are:

- Set to ‘Automatic’ startup.
- Running (status is ‘Started’).
- Service running as a ‘Local System’.

Service name	Description	Experion Server	Console Station	Flex Station	Console Extension Station	ACE / SIM / APP	Notes
AppSight Black Box Service		X					
EloSystemService	Elo TouchSystems services.		X	X			

Service name	Description	Experion Server	Console Station	Flex Station	Console Extension Station	ACE / SIM / APP	Notes
Iap	Provides routing services for components of Dell OpenManage Client Instrumentation (OMCI).		X	X	X	X	
Matrox.Pdesk.ServicesHost	Desktop Management Service Control.			X			
NVIDIA Display Driver Service	Provides system and desktop level support to the NVIDIA display driver.		X				
NVIDIA Stereoscopic 3D Driver Service	Provides system support for NVIDIA Stereoscopic 3D driver.		X				
Sentinel Keys Server	Manages Sentinel hardware keys attached to this computer.	X					
Sentinel Protection Server	Manages Sentinel SuperPro and UltraPro keys attached to this computer.	X					
SigmaTel Audio Service	Manages SigmaTel Audio Universal Jack configurations.				X		
SQL Active Directory Helper Service	Enables integration with Active Directories.						

Service name	Description	Experion Server	Console Station	Flex Station	Console Extension Station	ACE / SIM / APP	Notes
SQL Server (MSSQLSERVER)	Provides storage, processing, and controlled access of data, and rapid transaction processing.	X					Service runs under '. \ExpSQLSvc' account.
SQL Server Agent (MSSQLSERVER)	Executes jobs, monitors SQL Server, fires alerts, and allows automation of some administrative tasks.	X					Service runs under '. \ExpSQLSvc' account.
SQL Server Browser	Provides SQL Server connection information to client computers.	X					Service disabled.
SQL Server VSS Writer	Provides the interface to backup/ restore Microsoft SQL server through the Windows VSS.	X					
Visual Studio 2008 Remote Debugger	Allows members of the Administrators group to remotely debug server applications using Visual Studio 2008. Use the Visual Studio 2008 Remote Debugging Configuration Wizard to enable this service.	X	X	X		X	ACE node. Service disabled.

16.5 Other Microsoft services

Experion relies on the presence of several complex Microsoft services that need to be configured securely.

16.5.1 Internet Information Services

Internet Information Services (IIS) is needed for the following Experion functionality.

- Alarm Pager option (e-mail notification)
- eServer

IIS 6.0, as installed on Windows 2003, has most options disabled by default, unlike IIS 5.0 which had to have unwanted options disabled by use of the IIS Lockdown tool. The installation instructions for IIS 6.0 and details of the components required for Experion are documented in the *Experion Software Installation and Upgrade Guide*.

It is strongly recommended that you run the Microsoft Baseline Security Analyzer (refer to the section “Using Microsoft Baseline Security Analyzer” on page 152).

In setting up and maintaining IIS you must also ensure the following:

- 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 caller's 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.

16.5.2 SQL Server

The following information relates to Experion requirements in relation to SQL Server. If other databases are hosted by the Experion SQL Server, then their own security model must also be applied.

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

The following security recommendations apply to SQL Server.

- Where possible, do not give users access to multiple databases.
- Run Microsoft Baseline Security Analyzer (refer to “Using Microsoft Baseline Security Analyzer” on page 152) on your SQL Server.

Note that Experion installation process sets authentication to "Windows only" and ensures that the password is not blank.

16.5.3 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.

16.5.4 Remote Access Server

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.

Ensure to follow the following 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.

16.5.5 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 2008 servers and Windows 7 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.

16.6 Use the firewall on Windows 7 and Windows Server 2008 machines

About firewall settings

Honeywell applications set the correct firewall settings when they are installed. Honeywell recommends that you leave these settings at their default values in order that the applications function at their optimum levels.

16.7 Windows 7 and Windows Server 2008 registry and other settings

Windows 7 and Windows Server 2008 have many registry settings that can be used to increase the overall security of a system.

Note, however, that extreme caution needs to be exercised when making any changes to the registry. For more information, refer to the section “File system and registry protection” on page 170.

There are additional security considerations you may want to consider to increase your system security. For more details refer to *Windows Server 2008 Security Compliance Management Toolkit*.

Disable the 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. If the control room is disconnected from the domain server; the user cannot logon until the control room re-connects to the domain server.

Harden the TCP/IP 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.

The following Microsoft link provides the details

http://technet.microsoft.com/en-us/network/bb545475.aspx.

17 Experion Security Features

This section describes security features specific to Experion.

Experion 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".

Note that in the context of this chapter, the term "assets" refers specifically to the Experion assets that comprise your asset model. For information on the Experion asset model, refer to the "Assets and asset models" section in the *Server and Client Planning Guide*.

Related topics

"Windows accounts and groups created by Experion" on page 180

Experion users fall into several roles, which can be specified by 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.

"User accounts and Experion user roles" on page 183

"Station security" on page 185

"ODBC client authentication" on page 186

"Configuring a secure Station" on page 187

"Electronic signatures" on page 189

17.1 Windows accounts and groups created by Experion

Experion users fall into several roles, which can be specified by 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 adds a number of local groups and accounts to existing Windows groups and accounts. The groups are listed in the roles group assignment table described in section "Honeywell High Security Policy" on page 167. The user accounts are listed in the following table.

Name	Account/Group	Description	Refer to:
mngr	Local account	Experion processes run under this account.	"Requirements for the Windows mngr account" on page 180
LocalComServer	Local account	Used for DCOM servers and Windows services.	"Requirements for the LocalComServer account" on page 181
DCSComServer	Domain account	Typically used for HCI COM/OPC Servers provided as part of the Experion/TPS system. This account is configured to log on only as a batch job.	Refer to the "User account types" section in the *Windows Domain and Workgroup Implementation Guide*.

17.1.1 Requirements for the Windows mngr account

The Windows mngr account has a number of specific requirements which are set up by the High Security workstation installation. The following settings must not be modified.

- Password should never expire
- The account is a member of the 'Local Servers' and 'Local Engineers' groups.
- The following settings must be applied (via membership in above groups)
  - Deny logon locally
  - Deny logon through terminal services
  - Logon as a batch job
  - Logon as a service
  - Lock pages in memory
  - Create global object
- 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 below.
- The mngr password on Console Stations must also be the same as the parent Experion server.

About changing the Windows mngr password

The mngr account is used by:

- All Experion core processes
- Certain Experion Windows services
- Certain Experion COM servers
- DSA node authentication
- Console Stations

Notes

- Because the mngr password is used when configuring these services and COM servers, you need to exercise caution in changing this password. Incorrectly changing the password can render the system inoperable.
- 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.
- The Experion server and all Console Stations synchronized with that server must have the same mngr password.
- As best practice requires frequent password changes, it is important to use the password utility pwdutil.exe to ensure that the change is made consistently. The system administrator should run this periodically but with care as an invalid password could prevent Experion from operating correctly.
- For information about using pwdutil.exe, refer to the topic "Changing the Windows mngr account password" in the *System Administration Guide*.
- To change the service account passwords across an entire system, refer to the following online support website. In the following website, refer to a technical note covering information about how to do this.

  https://www.honeywellprocess.com/en-US/

17.1.2 Requirements for the LocalComServer account

The Honeywell Administrators group is given the following privileges by the High Security Policy workstation install.

- Create global object
- Shut down the system

Note that the Product Administrators group also needs permission to execute *%windir%\system32\cmd.exe*, otherwise the Experion server cannot run

17.1.3 Experion group key

Experion 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\Wow6432Node\Honeywell\Experion PKS Server\Group

You can specify multiple account groups by separating them with semicolons (;). This allows several user groups to access Experion 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 server, not a domain server.

Note, however, that extreme caution needs to be exercised when making any changes to the registry. For more information, refer to the section “File system ACLs” on page 170.

By default the Product Administrators group is the only group given access, and normally there would be no need to change this.

Attention

A user whose account is a member of the Product Administrators group has extensive access to Experion files, executables, and registry keys. Only provide this access to those who require it. For more information, refer to “Group Policies in an Experion System.”

17.2 User accounts and Experion user roles

User Roles are used to define the set of operations a user is allowed to perform. For the list of roles that are defined by Experion, refer to the table roles defined by the security model in section “Honeywell High Security Policy” on page 167.

The users in an Experion system generally fall into one of the four following user classes.

- Operational users
- Engineers
- Product Administrators
- Administrators

The user account and access requirements of each class are described below. The above classes of user have distinct responsibilities with little overlap between them. However, a site may choose to assign multiple roles to select users, giving them broader responsibilities.

17.2.1 Operational users

Operational users include the roles of Supervisor. Operator, Ack view-only user, and View-only user. These users are focused on the operation of the process with varying degrees of privilege. They generally have little need to access general Windows capability. The environment for these users is restricted to the applications started for them by a logon script.

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. Depending on the Experion security model you choose, operators may be:

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

Best practice is to place all operators in a single Windows account group, depending on security level, then that group can be used to provide read-only access to the file shares exposing display files and reports.

Note that operator accounts would not normally belong to the Honeywell Administrators group since they do not need the level of access this would provide.

For more information, refer to the section “Station security” on page 185.

17.2.2 Engineers

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

Engineers should not develop on the production 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/ strategies.

Development should occur on an off process system, and new executables should only be allowed on the production system after they have been thoroughly tested.

In addition, if they need to stop and start the Experion services, or run utilities with direct access to the database such as trace or dct, then their Windows user account must also belong to the Product Administrators group.

Honeywell recommends using a separate account for each engineer. As long as they belong to a domain account that is a member of the domain “Engineers” group or local account that is a member of the “Local Engineers” group, they will all have equivalent access to Experion nodes. This then also allows the ability to trace an individual's activities in audit trails.

17.2.3 Product Administrators

Product administrators require even greater flexibility than engineers. They are responsible for system-wide settings, starting and stopping services, and other operations that affect the Windows applications that make up Experion. In general, these users are not either engineering or operational personnel, and must have very little process access.

17.2.4 Administrators

The administrative role is defined by Microsoft. There are several roles that Microsoft defines that fall under the general heading of system administration. Much like Honeywell's role groups, users that are granted system administrative privileges must be added to one or more of the Microsoft-defined groups that represent the administrative roles. Some of those groups, and their related responsibilities are described in the following table.

Role Group	Role Responsibilities
Administrators	• Manage user accounts • Manage local policies and privileges • Installing software and operating system updates
Backup Operators	• Backup and restore all files on a computer, regardless of the permissions that protect those files • Log on to the computer and shut it down
Network Configuration Operators	• Make changes to TCP/IP settings • Renew and release TCP/IP addresses
Performance Monitor Users	• Monitor performance counters on the server locally and from remote clients without being a member of the Administrators or Performance Log Users groups
Performance Log Users	• Manage performance counters, logs and alerts on the server locally and from remote clients without being a member of the Administrators group
Print Operators	Manage printers and document queues

Best practice requires that users granted administrative privilege have two accounts, and that they only use the account belonging to the administrative group(s) when absolutely necessary. This reduces the risk of accidental damage, and of leaving a highly privileged account logged on and liable to hijacking.

Where possible, the general administrator account created during installation should not be used directly if the site has several administrators, since actions will not be attributable to any individual. The built-in Administrators account should not be used because of security concerns, and is disabled during Experion installation.

17.3 Station security

For more information about planning and implementing Station security, integrated and group accounts, and security levels on a station, refer to the Configuring System Security section of the *Server and Client Configuration Guide*.

17.4 ODBC client authentication

ODBC clients using the Experion 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 sign-on will take effect if permitted.

17.5 Configuring a secure Station

A secure Station is one that can only be used to run the Honeywell Station functionality. This level of security goes beyond what is applied by the High Security Policy to servers and non-dedicated clients. It is appropriate for dedicated static Stations used in a control room environment.

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 High Security Policy.

To restrict access to the operating system and non-Station applications, you must perform the following:

- Set up a secure Station.
- Remove access to the operating system and applications other than Station.

17.5.1 Setting up a secure Station

Perform the following tasks for locking down (that is, securing) the Station.

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. Create a batch file which starts the Station automatically.
   With Experion R431, OEP or IKB function properly only if MsgTransfer.exe application is running in the background.
   - If you restrict access to explorer.exe on all **Experion nodes** (except for T-node), then the MsgTransfer.exe also gets restricted. To prevent MsgTransfer.exe from getting restricted, add `C:\Program Files(x86)\Honeywell\TPS\base\MsgTransfer.exe` to the following:
     – *start_station.bat*, which is the default start up script file
     – Any other customized start up script file
   - If you restrict access to explorer.exe on **T-nodes**, then the MsgTransfer.exe also gets restricted. To prevent MsgTransfer.exe from getting restricted, add `C:\Program Files(x86)\Honeywell\TPS\base\MsgTransfer.exe` to the following:
     – *start_station.bat*, which is the default start up script file
     – Any other customized start up script file
       – *operator.bat*, which is the default start up script file
       – Any other customized start up script file
2. Specify the batch file as a logon script to the user account.
3. Prevent the operators from shutting down their computer.
4. Remove access to applications through the Task Manager and Windows Explorer.
5. Set up automatic logon (optional).
   If you set up automatic logon, to log on as Administrator you must press the **Shift** key to prevent automatic logon.
6. Prevent users from locking the computer.
   For detailed instructions on completing each of these tasks, refer to the section "Securing the operating system" in the *Windows Domain and Workgroup Planning Guide*.

17.5.2 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, refer to the procedure in the section “Configuring a secure Station” on page 187 and use the High Security Policy.

Changing the Station command line allows you to perform the following:

- 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, refer to the section "Changing the Station command line" in the chapter "System Administration" in the *Server and Client System Administration 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*.

17.6 Electronic signatures

Electronic signatures are the legally binding equivalent of an operator's handwritten signature. With Experion's Electronic Signatures option, 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 configure a set of reasons that require operators to choose from a pre-configured set of reasons before they perform the action.

Each time an action requiring an electronic signature is performed, the events database is updated with the following:

- The name of the operator(s) who initiated the action
- The specified reason
- The date and time

An event is also generated, in the following scenarios.

- The user name or password provided by the operator is invalid
- The operator cancels the Electronic Signature dialog box.
- A time-out 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.

Tip

- The Electronic Signatures option requires the use of integrated accounts. Refer to the section "Using integrated security" in the chapter "Configuring security and access" in the *Server and Client Configuration Guide*.
- The IKB and the OEP keyboard are not compatible with Electronic Signatures. You cannot use either of these keyboards with Electronic Signatures.

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

17.6.1 Complying with 21 CFR Part 11

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

Title 21 CFR Part 11 of the Code of Federal Regulations deals with the Federal Drug Administration guidelines on electronic records and electronic signatures in the United States. Part 11 defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records.

In summary, Part 11 requires drug makers, medical device manufacturers, biotech companies, biologics developers, and other FDA-regulated industries, with some specific exceptions, to implement controls, including audits, validation systems, audit trails, electronic signatures, and documentation for software and systems involved in processing many forms of data as part of business operations and product development.

Compliance with 21 CFR Part 11 also requires that computer systems audit all logon attempts and all (manual) changes to system time.

Applying the Honeywell High Security Policy will restrict the ability to make system time changes to users belonging to the Administrators group. For information on Honeywell High Security Policy, refer to the section “Honeywell High Security Policy” on page 167.

Controlling access to the system clock is important because the Federal Drug Administration (FDA) requires all electronic records to be time-stamped. This means any change to the system clock will affect the audit trail.

To enable audit logging of user log on and system time changes:

- In a domain, you use Group Policy

- In a workgroup, you set the local audit policy

System time changes will be logged if "Audit system events" is enabled for "Success". As a minimum, therefore, audit settings should log successful attempts, but if attempted intrusion is suspected then failed attempts must also be logged.

Note, however, that the default setting for audit logs is to halt the system if the security log becomes full. This is to prevent activity occurring without any traceability but it can also provide an opportunity for a denial of service attack. For information on setting up audit logs to mitigate this kind of attack, refer to the section “Setting up and analyzing audit logs” on page 153.

18 Glossary

Access Control List (ACL)

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.

Authentication

When a user logs on to a system the authentication process verifies that a user is known to the system. Also refers to authorization.

Authorization

When a user logs on to a system, the authorization process controls what a known user can do within the system. Also refers to authentication.

Business Network

A collective term for the network and attached systems at Level 4. Also refer to “Levels 1 through 4”.

Configuration Studio

Configuration Studio is an Experion tool that provides a central location from which you can configure your Experion 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 license 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 Station that provides similar functionality to a “Flex Station”, but is hosted by a Console Station rather than an Experion 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 (DMZ)

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 (DSA)

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

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 (ERD)

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.

FIM

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 65,536 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 (DMZ)”.

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; which is connected to the server using either a static or rotary connection.

Compare with a “Console Station”.

FTE

Fault Tolerant Ethernet, the control network for Experion.

GUS

Global User Station, a TPS node.

IP

Internet Protocol.

LAN

Local Area Network.

Levels 1 through 4

The location of a node within an Experion 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 (PCN)”. Between Levels 3 and 4 you might have a “Demilitarized Zone (DMZ)” 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

In Wireless 802.11, MAC stands for Medium Access Control. The lower level of the Data Link Layer (under the IEEE 802.11-1997 standard).

Can also be an abbreviation for Message Authentication Codes, a cryptographic hash added to a message to enable the detection of tampering.

MES

Manufacturing Execution Systems.

MRP

Manufacturing Resource Planning.

Network Address Translation (NAT)

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.

Process Control Network (PCN)

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

PHD

Process History Database. PHD is Honeywell's advanced historian, providing distributed data collection, and data consolidation.

Port

A port is a logical endpoint on a network node used for communications. There are approximately 65,536 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.

Process Controller

Experion's controller 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.

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 an 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 operator interface.

TCP/IP

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

TotalPlant® Solutions.

Uninterruptible Power Supply (UPS)

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.

WAN

Wide Area Network.

WSUS

Microsoft Windows Software Update Services.

19 Notices

Trademarks

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at http://www.honeywell.com/ps/thirdpartylicenses.

19.1 Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

http://www.honeywellprocess.com/support

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

19.2 How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

https://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

- Send an email to security@honeywell.com.

  or

- Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

19.3 Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx.

19.4 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.

Experion Network Best Practices

Author/Editor: Jay Gustin

Document ID: WP-07-02-ENG (formerly ENBP-WP)
Original Issue Date: April 2004
Revised: October 2015
Version: 4.4

1. Introduction

Scope

This document is intended to provide “best practices” advice for planning the installation of Experion FTE networks, and connecting them into the plant IT network.

Users

Intended users of this document include:

- Honeywell System Consultants, Technical Assistance Center, Project Services
- Honeywell clients

Changes for R400

- New controller type Profibus Gateway Module (PGM)
- New HMRF Modbus Firewall
- One Wireless Firewall
- Clarification of PCDI operation and topologies
- Domain Controller best practices
- L2 to L3 fault recovery times
- Low cost FIM switches for cost sensitive projects
- IP address effects and warnings
- OLS navigation for configuration files

Changes for R410

- Virtual architectures
- One Wireless R200
- Revisions and clarifications on access between levels
- Improved matrix of equipment connections
- Safety Manager on FTE
- PMD on FTE

Changes for R430

- EUCN architectures
- Ethernet IP
- Secure communication
- FMC722
- New switches

Changes for R431

- EUCN architectures
- New switches
- ETNi

Definitions

Definitions	
ACE	Advanced Control Environment- An Experion node used for high-level control
ACL	Access Control List- A command for filtering traffic
CDA	Control Data Access- The Experion data access layer

DC	Domain Controller
DHEB	Data Hiway Ethernet Bridge
DSA	Distributed Server Architecture- The Experion method of sharing data.
EIP	Ethernet IP
ESVT	Experion Server TPS
ES-T	Experion Station TPS
ETNI	Enhanced T-Nade Interface
EUCN	Experion Uninversal Control Network
ACE	Experion application node
CAB	Custom Array Blocks
FIM	Fieldbus Interface Module
FTE	Fault Tolerant Ethernet- the control network of Experion PKS
FTEB	FTE Bridge- FTE interface for C200 controllers and FIMs
GBIC	Gigabit Interface Converter module for Cisco switches
HSRP	Hot Standby Router Protocol
IP	Internet Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol- a client-server protocol for accessing a directory service
MAC	Media Access Control
NAT	Network Address Translation
NTP	Network Time Protocol
PCDI	Peer Control Data Interface
PGM	Profibus Gateway Module
PHD	Process History Database- Honeywell’s data historian solution
SFP	Small form factor plug-in interface module
TCP	Transport Control Protocol
Uplink	Any interface that connects switches to switches or switches to routers

2. FTE Network Infrastructure

Overview

An FTE network is comprised of a variety of node types and networking components. This section describes the considerations and requirements for connecting and configuring these elements to provide a system that has significant security and reliability improvements over a simple Ethernet network.

Best Practices vs Requirements

Best practices presented in this document should be treated as requirements for the safe and secure operation of an Experion network. The variations on the best practices can be implemented for those conditions that cannot for economic or geographic reasons adhere to the primary best practice. Recommendations are also included as enhanced security, reliability or availability practices. Deviating from best practices or recommendations can result in reduced support by the Honeywell TAC.

Plant Network Levels

A plant network has four layers or levels. The following table briefly describes these levels. Level numbers are used to simplify the description of the node location within the network hierarchy. The FTE network of an Experion PKS system includes levels 1 and 2. Sections 3 through 6 of this document provide further details on these levels, including specific network requirements.

Level	Node Descriptions
Level 4	Plant Level Applications
Level 3	Advanced Control and Advance Applications (Non-Critical Control Applications)
Level 2	Supervisory Control, Operator HMI (HMI, and Supervisory Controllers)
Level 1	Real Time Control (controllers and IO)

FTE Communities

An FTE community is a group of nodes that have fault tolerant communication coverage using FTE test messages. These nodes are all members of the same broadcast domain. Nodes that are either single attached, or are dual attached but do not run FTE, may also be members of the FTE community. FTE is not qualified and will not run correctly with multiple FTE communities in the same broadcast domain.

The FTE node number limits seem to inhibit large systems using FTE. This is not the case, however, as FTE communities can be interconnected using a router. The individual FTE communities should be designed to include those nodes that have critical intercommunication requirements. Data can be shared between routed FTE communities via Distributed Server Architecture (DSA). Using this technique, a very large system can be constructed of FTE nodes with a wide geographical distribution.

Best Practice Architecture

The drawings shown in this paper represent the Honeywell best practice for a large installation. While variations of the architecture are possible, this topology represents the highest level of security and reliability. The emphasis is on isolating critical areas of function with layers of switches so that local peer-peer control is most important, peer to external peer is second most important, controller to server/station is third most important and server to station, ACE and other L2 nodes

is fourth most important. Communication from L2 to L3 is generally less critical and more restriction can be placed on this path.

3. Level 1

Description

Level 1 nodes are the heart of the control system. This network segment contains controllers, FTEB-based I/O, and Series A or Series C FIM and PGM nodes.

Level 1 Best Practices

The best practice is to put Level 1 nodes on a separate switch or Control Firewall pair. This allows critical peer-to-peer traffic that cannot tolerate a communication delay of longer than 250 ms following an FTE cable fault. It also gives controllers a level of isolation from other nodes during catastrophic failure or network disturbance. The user should arrange for the most critical elements of control to be connected to this switch. Because Level 1 nodes include controller nodes, the critical control traffic must have adequate bandwidth. The following sections describe how to accomplish this.

Control Firewall Best Practice

Experion R300 introduced the Control Firewall. This appliance offers a level of protection of the embedded controller nodes against unwanted traffic from Level 2 and above. It supports 802.3x Ethernet flow control which is used by the Series C controllers to cut off overwhelming levels of traffic. All Series C nodes including C300, FIM4, FIM8, and PGM must be connected to the internal interfaces of a Control Firewall, or in cost sensitive projects a SFE2000. FTEB-based 1756 I/O Safety Managers using PCDI or CDA communication and HC900 using PCDI may also be attached. The uplink of the Control Firewall is attached to a Level 2 FTE Qualified switch using an interface configured for 100Mbps full duplex and port fast. An interface configured as an uplink can be used with the “spanning-tree portfast” attribute added to the configuration of the interface, or one configured as a normal Level 2 node connection can be used. Control Firewalls cannot be cascaded.

The Control Firewall has the following features:

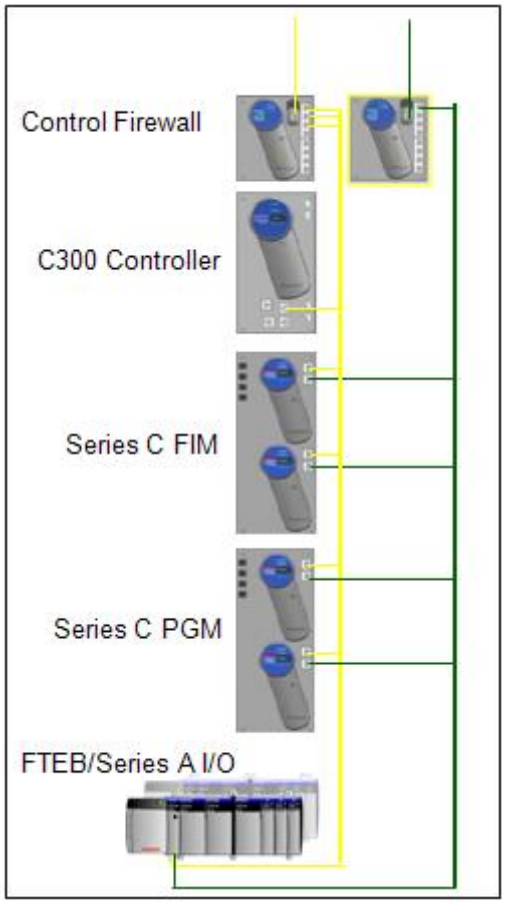
- Allows only CDA connected traffic and Modbus TCP traffic through by using TCP port filtering
- Limits broadcasts to ARP and Bootp packets and limits the data rate
- Limits the rate of connection to mitigate SYN flood attacks
- Limits multicast to FTE messages
- Allows NTP and IEEE 1588 time sync packets, but limits the data rate
- Prioritizes internal packets over external packets
- No user configuration required

NOTE: Computer nodes running a Windows operating system with file sharing enabled must not be attached to the inside of the Control Firewall. NetBIOS messages will be blocked from entering the CF9, and the internal node will become the master browser as it can’t see any other nodes in the system. This will have the effect of preventing file sharing for Level 2 nodes.

The introduction of the features in the CF9 for EUCN (in revisions FF and JJ) and for secure communication (in revision JJ) added new requirements for updating these devices. These new features enable certain packets to pass through which have not in previous versions. Adding a previous version to a working system, whether EUCN or R430 with secure communications can cause a loss of view and control for the nodes connected under this CF9. A failed CF9 can only be replaced by one with the proper minimum revision.

Steps have been taken in revision JJ to prevent issues, especially if a firmware update fails and the CF9 reverts to the previous revision which is less than JJ. These steps include checking if the micro firmware irevision is JJ or greater revision. If it is less, the FPGA firmware will not be allowed to update. The JJ or greater micro image has the ability to detect if the FPGA image is less than JJ and will shut off the 8 ports where the L1 nodes are connected. This prevent a loss of view until the FPGA can be updated to the proper minimum revision. The L2 uplink port will be unaffected allowing the update packets to be received.

CF9s that are in stock are recommended to be updated to the minimum revision so there will be no chance of replacing a failed device with one that is less than the minimum revision. CF9s not at this minimum revision can be upgraded to the proper revision by removing the L1 connections from the CF9 IOTA, then upgrading the micro then FPGA to revision JJ or later. When the upgrade is complete and the revisions are confirmed, the L1 nodes can be reconnected to the IOTA.



Series C Level 1 LAN Cluster

- Citizenship
  - Controller (C300)
  - Series C Fieldbus Interface Module (4 or 8)
  - Series C Profibus Gateway Module
  - FTEB/Series A I/O
  - Control Firewall
  - Safety Manager using PCDI
- Purpose
  - Peer-peer Control
- Level 1 Control Firewalls
  - Provide point to point connectivity
  - Storm control
  - Prioritization of inside over outside packets
  - Throttling of network management packets
  - Port filtering

C200 With FTEB Best Practice

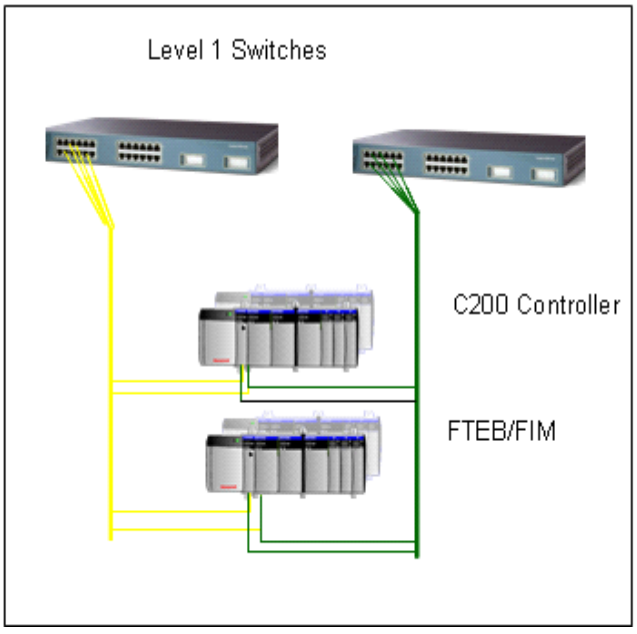
Installations with C200 controllers connected to FTE with the FTEB must be connected to a FTE Qualified switch with a Level 1 configuration installed. Several configuration settings in the Honeywell scripts enable protection for the Level 1 traffic.

First, the TCP ports that are used for critical control and display traffic will be fixed and well known. Reception of a packet with those TCP port values informs the FTE Qualified switches that this packet must be given priority. The output queue in the switches is configured to ensure traffic priority as follows:

- Control traffic is sent to the highest priority output queue.
- Display traffic is sent to the second level priority output queue.
- Any remaining traffic is sent to the lowest priority output queue.

Second, the uplink interface on the FTE Qualified Level 1 switch is configured to limit the amount of broadcast and multicast traffic. Broadcast or multicast traffic levels that exceed the limit will be cut off, but other traffic will not be affected. Cisco 2950 switches have a minimum limit on the gigabit interfaces of 8 mbps of broadcast traffic. Improvements have been made in the Cisco 2960 and newer switches and they have the capability to limit gigabit ports to 1 mbps of broadcast independent of the actual speed used for connection.

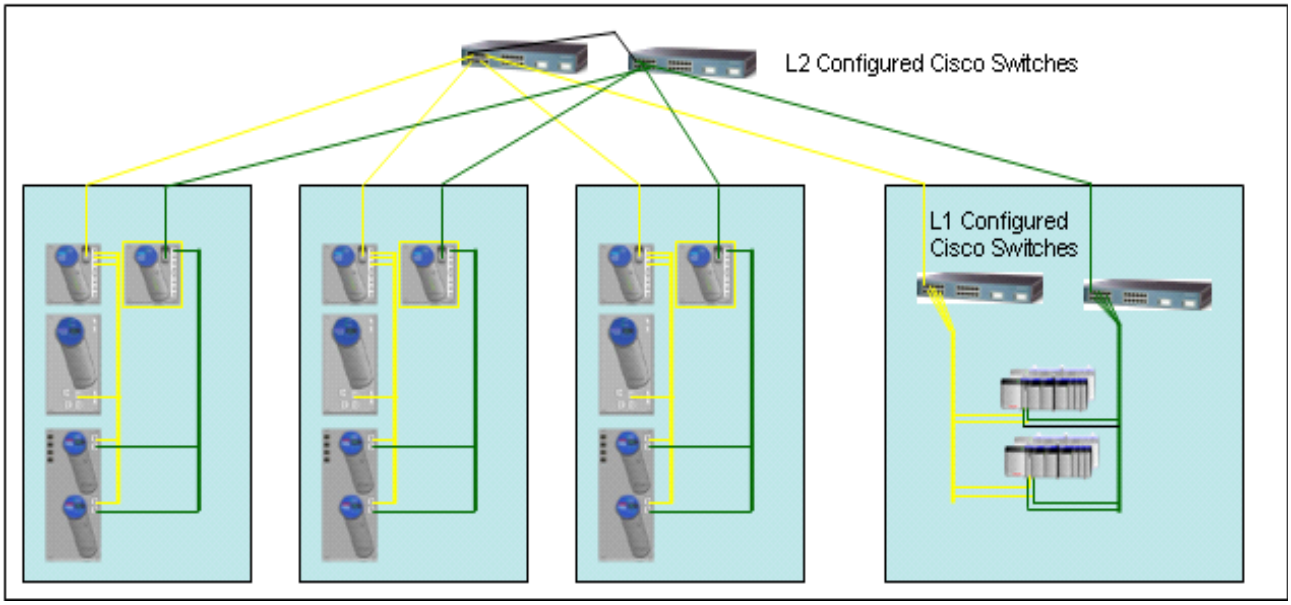
The use of a separate IP address range for Level 1 nodes is no longer being recommended as an overall best practice due to the difficulty of configuration. This scheme is still recommended for those installations where Level 1 address reuse is required. There is a discussion of this in the section on IP addressing:



Series A Level 1 LAN Cluster

- Citizenship
  - Controller (C200)
  - Fieldbus Interface Module
  - FTE Qualified Switches
- Purpose
  - Peer-to-peer Control
- Level 1 Switches
  - Provide point to point connectivity for FTE devices in cabinet
  - High Reliability Configuration
    - Always redundant
    - Pre-configure CDA traffic in high priority switch queue
    - Pre-configure view traffic in second highest priority queue
    - Pre-configure other traffic in low priority switch queue

Connectivity Between Level 1 LAN Clusters



- FTE Qualified Switches
  - Connect Level 1 clusters
  - High Reliability Configuration
    - Pre-configured bandwidth limits for broadcast, multicast storm suppression:
      - High traffic conditions will trigger FTE Qualified switch to disable offending ports
      - Automatic port enabling when traffic profile returns to normal
    - Dual FTE Qualified switch faults impact inter-cabinet traffic only

(alternatively, one pair of switches with the L1|L2 split configuration might be used)

Connection of Level 1 Nodes that Intercommunicate

The best practice is to connect Level 1 nodes that intercommunicate to the same switch pair, so that they will have the shortest communication path and the lower cable fault detection time. If intercommunicating Level 1 nodes cannot be contained on a single switch due to size of the installation or geographic dispersion, then their communications may go through the Level 2 switches. Level 2 switches are configured to have the same quality of service approach as the Level 1 FTE Qualified switches. The same TCP ports are given the prioritization scheme described for Level 1. The control traffic entering from a Level 1 switch will be tagged with the highest priority at the ingress. The output queue to the destination Level 1 node will send the control traffic before any other traffic. Communications redundancy is provided for this peer to peer traffic by always having two “pipes” for peer to peer and using FTE to provide four possible paths. In addition, the Level 2 switches are configured to have storm protection on the interfaces where Windows operating system nodes will reside. This storm protection will prevent broadcast or multicast storms caused by a node that is infected and using a denial-of-service attack. If a node reaches a broadcast or multicast limit of 20% of the connection bandwidth, then the interface cuts off broadcast or multicast until the traffic level falls below 18%. Normal FTE broadcast or multicast traffic is below 2%. (2 mbps).

Level 1 Uplink Configuration Differences

The best practice configurations for Level 1 switches (contained in FTE switch configuration files) include storm limits on all interfaces of Level 1 switches. Cisco 2950 model switches have a limitation on the level that can be limited to 8 mbps maximum on gigabit uplinks. Storm limits on Level 2 nodes will protect the Level 1 switches against a high level storm.. For best protection of Level 1 nodes, it is recommended that the 100 Mbps interfaces are used for uplinks on these switches. The newer models starting with the Cisco 2960 do not have these limitations and are set to the same limit of 1 Mbps for broadcast and 2 Mbps for multicast on the gigabit interfaces as the 100 Mbps interfaces. The L1 switches now have 2 styles of multicast protection depending on the number of FTE nodes in a system. See the section on Safety Manager switch connections for further details.

Refer to the Matrix of Equipment Options table later in this document for all controller connection options.

EUCN to Experion Peer-Peer connections

Release 430 introduces the real time peer to peer connection of the C300 and ACE(T) controllers to the EHPM controller. The EHPM and ENIM are in the class of nodes that belong to the EUCN network. EUCN encapsulates the IEEE802.4 based UCN protocol in an Ethernet packet and uses the FTE network switches and redundancy to provide point-point communication. EUCN nodes are part of the FTE network and are included in the 330 node count limit. There are several best practices associated with the EUCN network and nodes. There are several best practices associated with the EUCN network and nodes. In addition, history collection from the Experion server has the ability to go directly to the EHPM for the data. ENIM resident parameters will still take the TPN Server path.

Release 431 introduces a direct connection from consoles to EHPMs for collection of parameters that populate an HMIWeb display. This has the potential to greatly offload traffic from both the ENIM and the LCN.

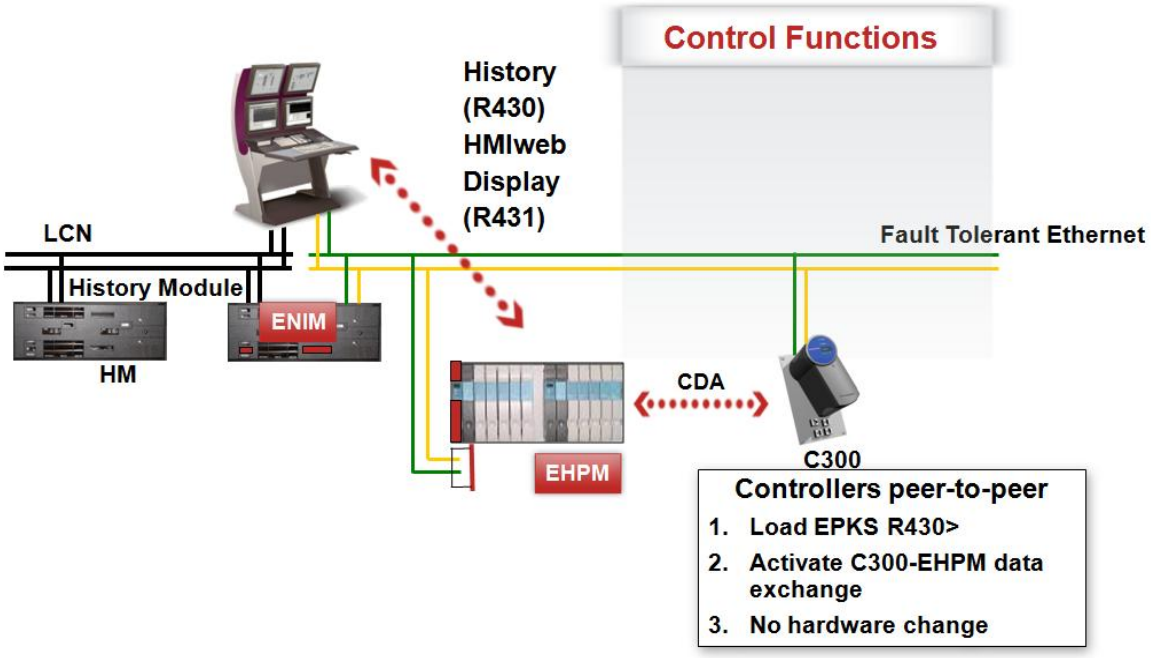
EHPM

The EHPM takes the COM/CONTROL system of the HPM controller and replaces the Token Bus Controller (TBC) with a PowerQuicc processor equivalent to the processor in the C300 and FIM. This processor performs TBC emulation over Ethernet and communicates through FTE to the Experion network. The EHPM node must be connected to a CF9 pair. These CF9s are dedicated to EUCN nodes. Series C nodes must not be connected to the same CF9s as a EUCN node. The CF9 must be revision JJ or higher starting in R430. There are special provisions to sense if the EUCN node is connected inside and allow the multicast packets needed for EUCN operation to pass through. C300s and FIMs are prevented from receiving this additional multicast traffic which causes unnecessary increases in CPU utilization. The CF9s can be uplinked to any other L2 switch in the network.

ENIM

The ENIM replaces the EPNI 802.4 based interface in a TPS NIM node with an EPNI2 EUCN/FTE based interface. The ENIM is a Level 1 node and must be connected to a L1 switch. The ENIM does have flexibility to connect either to an EUCN CF9 (not a Series C CF9) or a Level 1 switch. This switch can also be the L1 side of a split switch. Switches for ENIM connection must follow the environmental requirements for the TPS nodes. Thus, the Cisco IE3000 industrial switch is used for this purpose. This switch can be configured as a L1/L2 split or as a L1 only switch. The split enables connection of the ENIMs on the L1 side, the EUCN CF9s on the L2 side and the uplink to other L2..This uplink can either be a copper or fiber connection.. If fiber SFP modules are used they must be the RGD version to match the environmental specifications of the IE3000. Installations that have qualified L1 switches near the ENIMs may use as them long as they

have the EUCN special configuration. Non-ENIM nodes can also be connected to these switches. The SFE2000 will not have the EUCN configuration defined and are not recommended for this application.



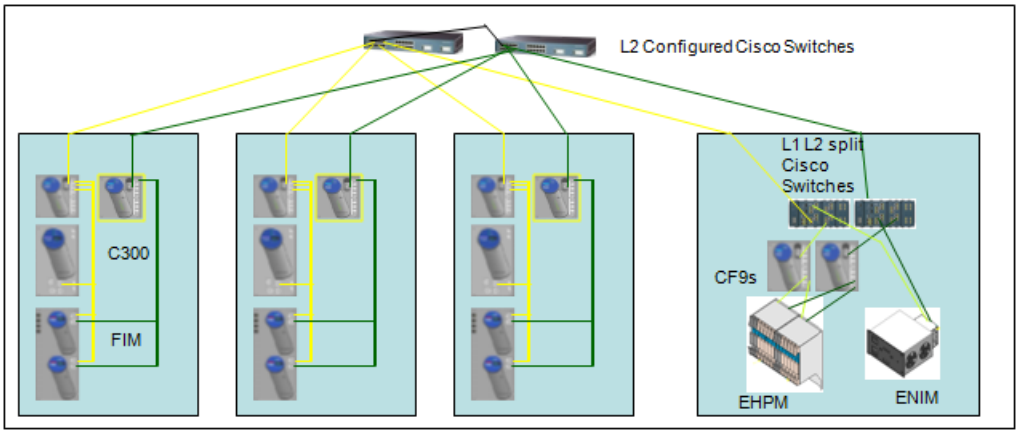
EUCN Direct Access Network

IEEE1588 server

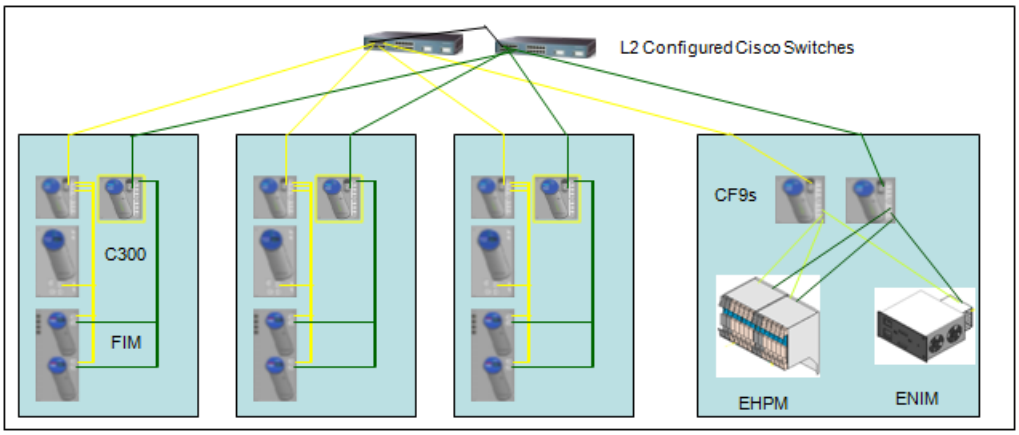
An IEEE1588 Precision Time Protocol (PTP) server is necessary in the EUCN network to provide the time precision to support Sequence of Events (SOE). This time source is not used in EUCN to provide precision network time. That is accomplished with LCN and UCN time as in the past. The function of the PTP system in EUCN is to remove the network transport delay in the time sync messages to more closely mimic the operation of the token bus network of IEEE802.4. The time server used for this function can also be used as the PTP source for Series C nodes to provide SOE.

An alternate connection method not shown in the drawings would be to connect the EHPM CF9s directly to the top L2 switch and the ENIMs directly to IE3000s configured as L1 switches and uplinked to the top L2 switch. In any case, the maximum of 3 levels of switches must be maintained per FTE community rules. CF9s and the L1 side of a split switch do not count as a level.

EUCN to L2 connection with L1/L2 split switch



EUCN to L2 connection with only EUCN CF9



Safety Manager switch connections

The Honeywell Safety Manager must be connected to either a Level 1 switch or a CF9 for use in peer-peer control strategies. Configurations for FTE Qualified L1 and the CF9 devices have provisions for SCADA, Modbus TCP and Safety Builder traffic to pass. In pure SCADA applications, the SM can be connected to a Level 2 switch at any end node configured interface. The use of L1 switches or CF9s for connection offers higher security for pure SCADA applications and may be preferred for the protection of the SM. The CF9 controller ports are protected against multiple MAC addresses in order to prevent loops. The connection of multiple Safety Managers to an isolation switch before connection to a CF9 will cause the port to shutdown.

Safety Manager starting with R410 supports FTE and CDA protocol. The connection options for this new feature are too numerous and complex to describe here. Refer to the document Safety Manager Planning and Design Guide EP-SM.MAN.6276 for the options.

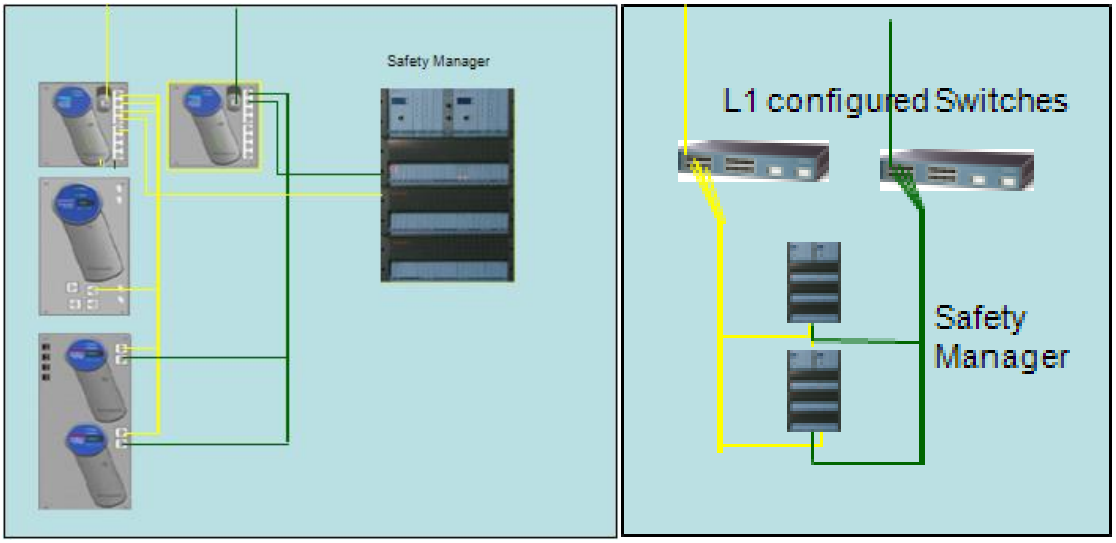
L1 switch configurations now have 2 style of configuration files. One set is for systems with 200 FTE nodes or less and one set for systems with greater than 200 FTE nodes. The multicast storm protection is higher on the > 200 node configuration as these switches are intended to be used with Safety Managers that can handle the higher level of multicast traffic. Any Series A nodes limit a system to 200 max FTE nodes where the multicast traffic is within the lower storm limit of the 200 or less configurations.

PMD controller switch connections

The Honeywell PMD controller also supports FTE and the CDA protocol beginning in R410. This controller may be connected to either a L1 switch or a CF9.

Peer Control Data Interface Connections

The Peer Control Data Interface allows peer-peer communication between the C300 and Safety Manager as well as third party devices such as Modbus TCP gateways. The best practice for connecting these devices should protect critical equipment from third party equipment, whose characteristics are unknown. Honeywell manufactured equipment can be connected to the Control Firewall. This equipment includes the Honeywell Safety Manager and the HC900 Controller. Other third party equipment must not be connected to Level 1 switches or Control Firewalls. A firewall especially for Modbus TCP is available. Refer to the section on third party equipment and risk for an explanation of why this rule is necessary.



PCDI and Honeywell Safety Manager Connections

4. Level 2

Description

Level 2 nodes are the primary server, view and advanced control nodes for the process control system. Examples of Level 2 nodes include servers, stations, ACE nodes, and PHD collector nodes. These nodes are essential for operation of the process, but not as critical to control as the Level 1 nodes.

Level 2 Best Practices

The FTE Qualified switches in Level 2 are configured to provide the security and reliability described in the Level 1 to Level 2 discussion. The nodes that reside on this level are more susceptible to attacks by viruses or software glitches because of the open nature of the operating system and the customized software that is running on these nodes. Thus, protection for broadcast and multicast storms on the interfaces to these open nodes is configured in the FTE Qualified switches. Also the display traffic as with the control traffic is given a higher priority so the traffic for view to the process will

take precedence over other traffic on the switch. This is especially important if there is a “bad actor” on the LAN that is generating high traffic. The higher priority control and view traffic will get to the destination first.

An important best practice is to avoid connecting a computer node to multiple networks. Connection of a server, for example, to two networks (“dual-homed”) turns that node into a router, which is a poor practice. Instead, the Experion network structure provides for the use of routers to join Level 2 nodes to Level 3 networks or to other Level 2 networks. A built-for-purpose router must be used in order to provide security and reliability through the use of Access List filtering.

There are exceptions where a third NIC card can be used for private connection to a single device that uses Ethernet. One example is the Honeywell DHEB for bridging to the Data Hiway.

There are nodes other than the Experion server, console and application nodes that can connect to Level 2 switches. Some of these devices have dual Ethernet connections. FTE is compatible with dual Ethernet nodes; they will not have the FTE protection, but no interference will occur and both types of nodes can intercommunicate.

Non FTE Level 2 node examples:

- Safety Manager using only SCADA
- Terminal servers
- Matrikon servers
- PLCs using SCADA

Single attached SCADA nodes such as terminal servers or subsystem devices also can attach to Level 2. If there are a large number of single attached nodes, then a separate switch can be used to aggregate these nodes. This switch will be counted as a level for spanning tree purposes, so it must not be connected to a FTE switch that is at the third level. This switch must not be connected to Level 1 switches. It can be connected to either the Yellow or Green side. The Yellow side is preferred. The green side can be used if load balancing or reduction in scope of loss is desired.

Embedded operating systems may not have enough processing power to handle the volume of multicast and broadcast traffic generated by FTE test messages and Address Resolution Protocol (ARP) packets. This type of node must either be connected at Level 3 or protected with Access List filtering on a separate switch on Level 2. The recommended switch is one of the qualified Experion switches. Honeywell Network Services can be consulted for proper configuration of this switch. Modbus TCP devices, even if used for SCADA, will benefit from the filtering of FTE messages when a HMTF (see the section on PCDI Third-Party Devices and Risk) is used.

FTE networks require a single crossover cable at the top of the hierarchy. In large systems it is recommended that a gigabit connection be used for this crossover connection. In the case of multiple faults, the backbone traffic will pass through this connection so the highest bandwidth will be available for this traffic. A determination of the necessity for greater than 100 Mbps for this crossover can be made by adding the total of the average bandwidth of all of the cluster servers. If this is higher than 20 Mbps, then a 1Gbps connection is recommended.

The best practice for the crossover cable is to use only one per FTE community. The placement of this crossover can be between any of the Level 2 Yellow and Green switches, as long as the rule of 3 levels of switches is preserved. The switches where the crossover cable connects must be configured for spanning tree root on the Yellow switch and secondary root on the Green switch. The switch configuration files supplied by Honeywell for the FTE Qualified switches contain these configuration steps, but they are commented out. The user must remove the comment delineator to enable the features. The crossover must not be connected to Level 1 switches.

All non-network related equipment must be connected to interfaces that are configured for portfast. Some network related equipment must also be connected to portfast interfaces. These are CF9, HMTF, HMRF and the OneWireless Firewall. Any networking device that transmits BPDU packets must be connected to an interface that is not configured for BPDU guard.

Implementing Level 2 Best Practices

To increase reliability and security, Level 2 nodes must be divided into two IP address ranges. Using two ranges simplifies the use of access lists for filtering as described below.

- Servers need access to nodes on other subnets as well as access to certain nodes on Level 3 and possibly Level 3.5 (see the DMZ description in section 5). Communication to other nodes may include Distributed Server Access (DSA), as well as Engineering access to load control schemes and high-level control.

- Other nodes on Level 2 do not need to be accessed by nodes on Level 3 and should be protected from such access. The exception is from WSUS and virus update serves and possibly remote access nodes. Protections must be made in router ACLs for limiting access to these nodes only.

To accomplish node access control, filtering is done in either the router, or the switch interface that connects to the router. Filtering, which is implemented by creating specific access lists for the FTE Qualified equipment, must accomplish the following:

- Allow servers to have complete two-way communication with other necessary nodes on all levels of the network. Router ACLs are recommended to limit access to just those nodes necessary for L2-L3 access.
- Allow non-server nodes to communicate with Domain Controllers for authentication and name service.
- Allow Level 2 nodes to initiate communication with Domain Controllers on Level 3.

Communication between Level 2 nodes and Domain Controllers on Level 3 can be accomplished by adding access lists that enable established communications to return TCP packets from the Level 3 nodes to the initiating Level 2 nodes. In addition, communications can occur using Active Directory (AD) services. The filter must allow specific port numbers used for these packets. See the section on “Example Cisco Router Configuration Statements” for examples of access lists to be used for filtering. Additional filters may be needed for all AD services and are up to the user.

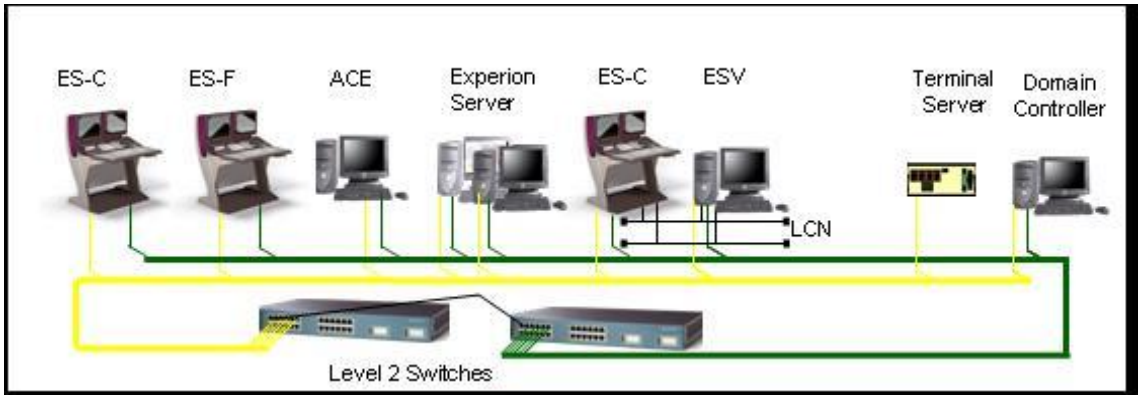
Domain controllers using Windows Server 2003 and beyond can have FTE installed when attached to Level 2. When using this configuration, the user needs to ensure that the green NIC IP address is removed from the DNS and that the DNS Service is only bound to the yellow NIC. Problems can occur when DNS is installed on a non-FTE node and then FTE is added to the configuration later if the above is not followed. FTE has benefits over using commercially available NIC teaming software in that more failure paths are detected without the need for IP address specific configuration.

Discoveries in R400 of the operation of Cisco routers have led to a change to the default FTE multicast address. The IANA assigned address of 224.0.0.104 will no longer be used. This is discussed in detail in the IP addressing section of this document.

Stacking Level2 switches

Certain Level 2 switch models are available for stacking. These include the Cisco 3750 and 3750x. There is a special stacking cable necessary to do the stacking. This stack is not qualified to be used as a Yellow-Green top level switch. The top switches must remain separate and connected with a single crossover cable or fiber. This stack counts as one level of FTE switch. NOTE: 3750 and 3750x switches cannot be combined in the same stack. If a replacement for a failed 3750 is not available, the entire stack must be replaced. Cisco will support replacement with 3750 switches for 5 years after End of Sale. SFP adapters are compatible between the 3750 and 3750x.

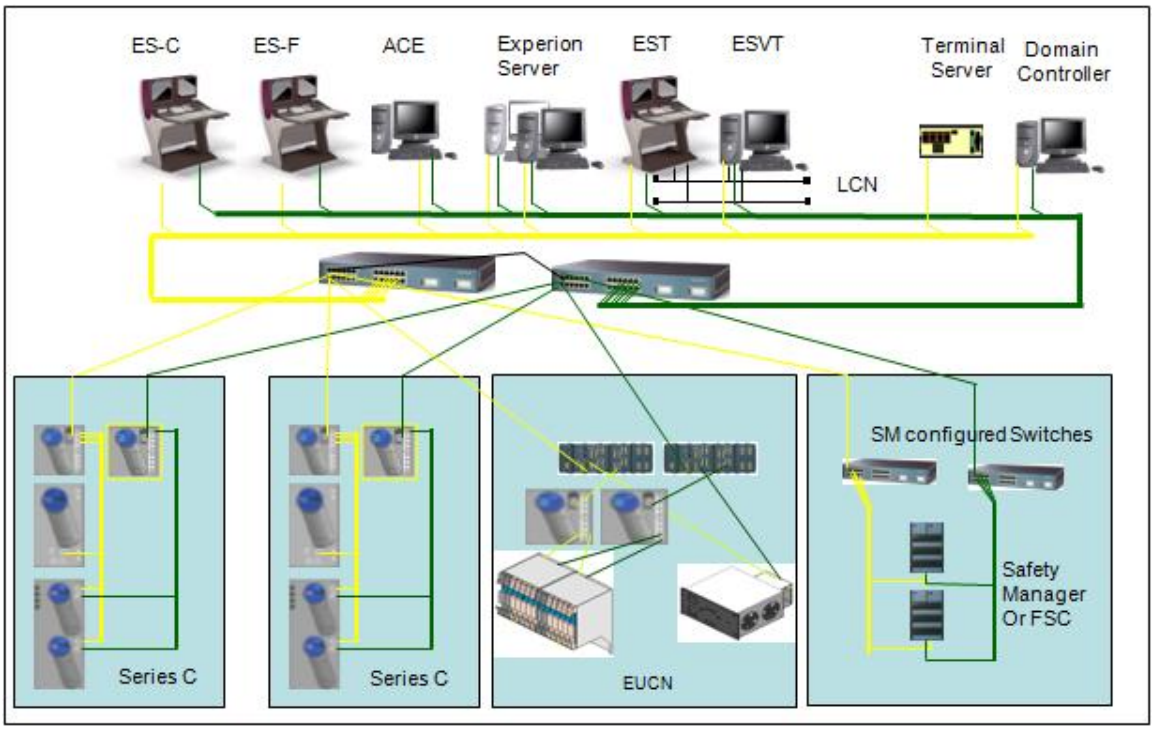
LAN Level 2



- Citizenship
  - PKS Server
  - Flex Stations
  - Console Stations
  - ACE
  - EST
  - ESVT
  - Subsystem Interfaces
  - Safety Manager using SCADA
  - Cisco Switches
  - Peer Domain Controllers

- L2 FTE Quaified Switches
  - Point-to-point connectivity for L2 Devices
  - Pre-configured bandwidth limits for broadcast, multicast, storm suppression:
    - disables ports with high traffic conditions
    - enables ports when traffic profile returns to normal
  - Preconfigure CDA traffic in high-priority switch queue (ACE-ACE, ACE-Controller)
  - Preconfigure non-CDA traffic in low-priority switch queue

L2 to L1 Connectivity – Complete FTE Community



- L1 Control Firewall
  - Blocks traffic not needed for control.
  - Higher level of protection for peer-peer nodes on same Control Firewall.
  - Prioritizes internal traffic over external.
- L1 FTE Qualified Switches
  - Prioritize ingress traffic; Non-CDA in low priority queue.
  - Ensures L2 – L1 supervisory traffic cannot disrupt L1 control
  - Blocks most traffic not needed for control
- L2 FTE Qualified Switches
  - Provide L1-L2 connectivity
  - Broadcast, multicast storm suppression
  - Preconfigure CDA traffic in high-priority switch queue (e.g., ACE-ACE, ACE-Cx, ACE-FIM, Server-Cx, Server-FIM)
  - Preconfigure non-CDA traffic in low-priority switch queue

PCDI Third-Party Devices and Risk

Third party Modbus TCP devices including PLCs and TCP/RTU gateways carry a certain amount of risk. Honeywell has tested a small number of gateways and consider them to be certified for use in a FTE network. This certification means that the devices have been tested with the PCDI blocks and SCADA, and the level of multicast and broadcast traffic in the FTE network will not interfere with their operation. Proper Modbus TCP operation is also validated. The parameters for best operation have been documented. This data is available in the PCDI *Frequently Asked Questions Whitepaper*.

All third-party Modbus TCP devices, certified or uncertified, are not in the control of Honeywell and defects may cause harmful operation that Honeywell cannot fix. The decision that this level of risk is high enough to warrant mitigation was arrived at after careful examination of the possible harm should the device generate large amounts of harmful traffic since they have direct contact with C300 controllers.

Third party device configuration presents another large threat for improper network operation. If a PC type node is connected to the Control Firewall to configure a third party device, the browser function will be disrupted. The node will broadcast a query for master browser. Any return packets from the real master browser will be blocked by the Control Firewall causing the node to assume master browser function. All browser requests will now be dropped and the file sharing will break. The result will be loss of Experion functionality. This is also the case for a Level 1 configured switch.

For this reason, it is imperative that a PC not be connected to a Control Firewall or a Level 1 configured FTE Qualified switch. Adding a device that may need configuration from a PC is another reason that third party devices are not recommended to be connected to a Control Firewall or L1 switch. For the two reasons above, it is recommended that for the lowest risk to controllers, a Honeywell Modbus TCP Firewall (HMTF) is used with third party Modbus TCP devices. This appliance is described later in this paper.

Some projects have been configured connecting certified gateways to the Control Firewalls. This configuration carries the risk that the third party device could cause harmful traffic if it gets into an unpredictable state. Although this behavior has not been observed during any of Honeywell's testing, the device is out of Honeywell's control and its operation cannot be guaranteed. Customers using this configuration must be warned about potential communication disruption that can be caused by connecting a PC to a Control Firewall. Every precaution must be taken to prevent this from happening, including special labeling or physical port blockage. The project and customer must decide that the risk is acceptable, or move the devices to a separate switch and install the recommended HMTF.

Honeywell Modbus TCP Firewall (HMTF) and Honeywell Modbus TCP Read-Only Firewall (HMRF)

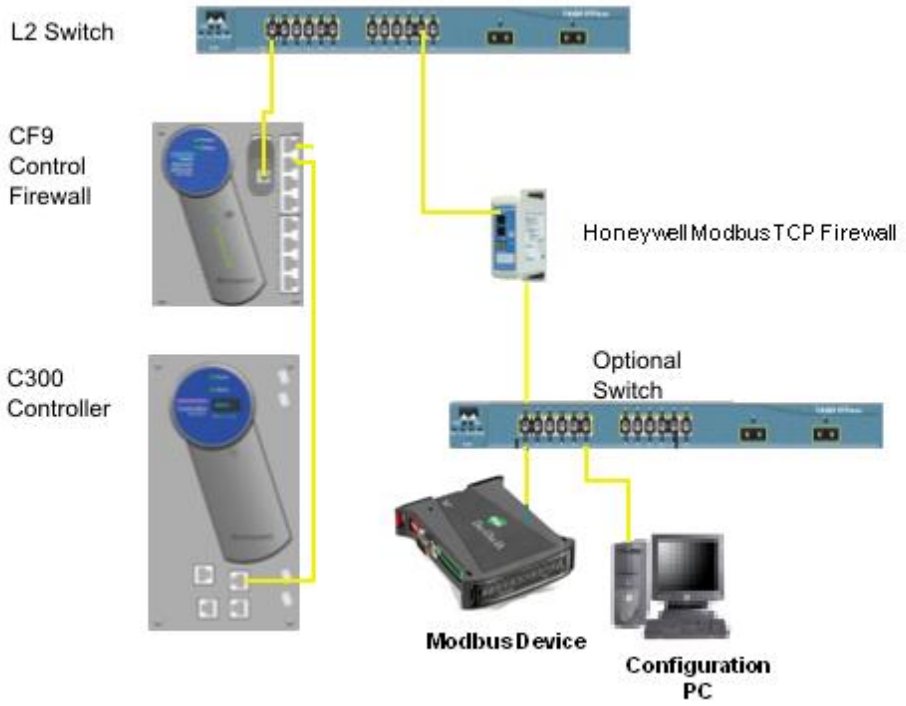
Protecting the Experion network is necessary to prevent third party equipment from introducing harmful traffic or possibly viruses or worms. This is especially needed when equipment must be configured or updated using vendor-supplied laptops or workstations. Therefore, the best practice is the use of a HMTF or HMRF . Connection examples are shown in the drawing below. Only the yellow leg of FTE is shown for simplicity. In addition, these firewalls will protect third party nodes from the levels of multicast used in the FTE network.

This topology is compatible with the topology employed for Series C components in that a protection appliance isolates the process-connected devices from the L2 network. In the case of the HMTF, the protection is two way. Only Modbus TCP traffic at TCP port 502 is allowed through from the high security side to the low security side and vice versa. A limited amount of ARP traffic is also allowed for network establishment. The limit is 1 mbps with a burst of 25 packets max. HMRF includes allowing NTP packets through with a 1 mbps limitation. HMTF revision D does allow NTP packets through. It is available on the HoneywellProcess web site for download.

In the case of the HMRF, the protection includes prevention of Modbus write function codes. Deep packet inspection is done on incomming packets and if a write function code is detected, the packet is dropped. The user must be aware that any write function codes will cause timeouts and slow down of the reads. It is therefore necessary to only configure read functions in PCDI function blocks. The other protections are the same as the HMTF with the exception that NTP packets are allowed through. HMRF topologies are exactly the same as HMTF as shown in the drawing below.

The HMTF is by default is set for Autonegotiation. A version of configuration is available on OLS to convert to 100/full duplex. The HMRF is only available in a 100/full duplex configuration. The L2 switch where the HMTF/HMRF is connected must have the matching setting for speed/duplex set in the interface where the device is connected. The optional switch shown in the drawing below can be used to add more than one 3rd party device under the firewall. The number of devices that can be connected to a single firewall should be limited to 10 for optimal operation. More than this will need a thorough bandwidth and packet burst analysis.

PCDI Device Connection Best Practice



PCDI Devices at Level 2

Devices or switches used to aggregate third party devices may be connected to either the yellow or green side of the FTE network through the HMTF/HMRF. The only difference is that traffic from the devices on the green switches will likely flow through the crossover cable to get to the destination. Yellow is therefore recommended as the preferred connection.

Devices that have redundant Ethernet connections are recommended to have one connection on a yellow switch and one connection on a green switch. This will give protection against network faults for the third party devices inherent in the FTE communication. As stated above, FTE offers better protection against faults with simpler configuation than commercially available NIC teaming. Again, the recommendation is to use a HMTF/HMRF to protect against third party operation risks and to enable the use of a configuration PC.

The switch in the drawing above is labeled as optional. A single MBTCP device can be connected directly to the HMTF/HMRF if it is configured for matching the speed/duplex or autonegotiate.

A Level 2 switch configuration can be used for the Modbus TCP device switch shown above. This will also provide the multicast and broadcast storm protection of the L2 configuration. The HMTF/HMRF must be connected to a L2 host port configured for the matching speed/duplex and have portfast configured. The uplink to the HMTF/HMRF from the Modbus device switch must be set to the proper speed/duplex as well. Portfast should be configured on the uplink from the Modbus device switch to provide faster spanning tree resolution.

It is a best practice that only one level of switch is allowed for the Modbus TCP devices. It can be any Honeywell qualified switch. If more than one switch worth of devices is needed, additional HMTF/HMRF and Modbus device switch combinations can be added.

Certified or uncertified devices can be connected at Level 2 directly for SCADA access as long as they are not configured by third party laptops connected to the network. Configuration by a serial port on the device, or offline configuration is the only acceptable method of change. Thorough testing of uncertified devices is recommended to be sure they can operate properly in the presence of the level of broadcast an multicast traffic in a FTE network.

It is a best practice that uncertified devices must be separated from the FTE network by a HMTF/HMRF for use with PCDI.

Ethernet IP

R430 introduces the addition of the EtherNet/IP communications stack in the C300 to enable integration of the C300 with Rockwell PLC components (ControlLogix, I/O and Drives) using EtherNet/IP.

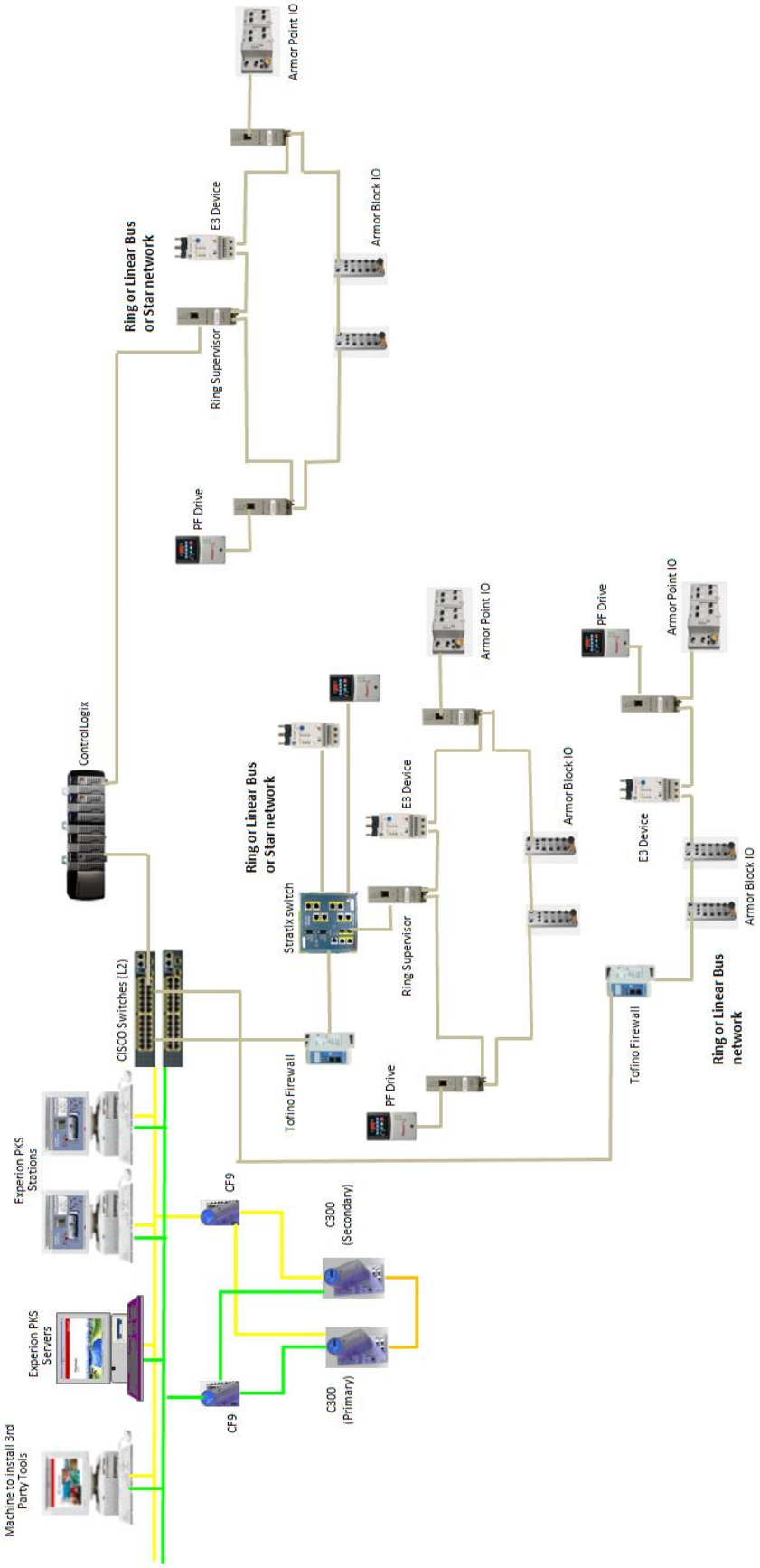
I/O (module and channel) and drive blocks types will be made available to make it easy to configure these devices. Support will also be added for interfacing with ControlLogix tags by allowing the user to create block types structures that match structures of the corresponding ControlLogix data types.

This solution will only be provided on the C300, and not on the C200 or C200E.

The following are the configuration rules for Experion systems using EIP:

- When using EIP, the maximum number of FTE Nodes per Community is reduced from 330 FTE Nodes to 200 FTE Nodes.
- EIP communication is only supported through the C300's FTE ports
- Controller redundancy is supported on a C300 that is EtherNet/IP-capable
- A Tofino Firewall configured to only allow EIP communications must be connected between any
- Ethernet/IP Devices or ControlLogix PLCs and FTE.
- EIP communication is supported between a C300 and EtherNet/IP devices that are connected in a switched star topology
- EIP communication is supported between a C300 and EtherNet/IP devices that are connected in a linear bus topology
- EIP communications is supported between a C300 and EtherNet/IP devices that are connected in a ring topology
- Each connected EIP Device or PLC counts as a Non-FTE Node towards the Non-FTE Node count limit per FTE Community
- Any Ethernet I/O connected and used by the ControlLogix PLC should be connected on an isolated separate downlink ENET card on the ControlLogix, and not be connected directly to the Stratix switch network.
- Rockwell tools should be located on a separate PC connected directly to the Stratix switch.
- The CF9 used by the C300 communicating with EIP Devices or PLCs must be upgraded to R430 compatibility level (Rev JJ or higher) to enable the proper TCP and UDP ports used for EIP Communications
- The 2950 cannot be configured to add EIP and must be replaced with a 2960 series or IE3000 switch.

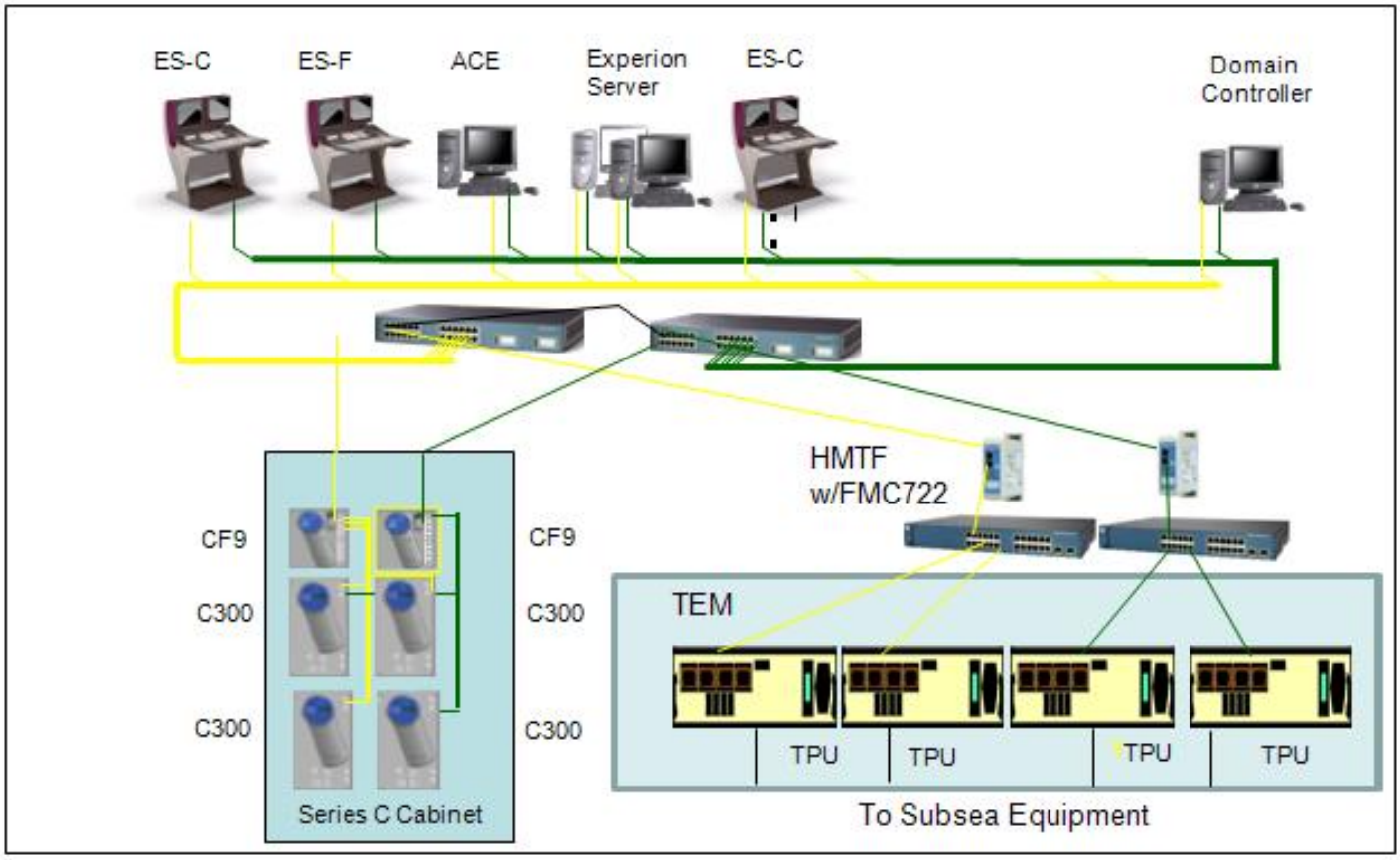
The figure below shows the network structure of a typical EIP installation.


Armor Point IO
E3 Device
Armor Block IO
Ring or Linear Bus or Star network
Ring Supervisor
PF Drive
ControlLogix
Armor Point IO
PF Drive
Armor Point IO
Ring or Linear Bus or Star network
E3 Device
Armor Block IO
Stratix switch
Ring Supervisor
E3 Device
Armor Block IO
CISCO Switches (L2)
Tofino Firewall
PF Drive
Tofino Firewall
Ring or Linear Bus network
Experion PKS Stations
CF9
C300 (Secondary)
Experion PKS Servers
C300 (Primary)
CF9
Machine to install 3rd Party Tools

FMC722

Experion C300 controllers now support the subsea protocol, FMC722. The protocol is supported with a new generic block in PCDI and a series of CAB custom blocks to extract the tags and parameters from the data payload. The equipment is connected to the Experion Level2 through a HMTF firewall with a special firmware version. This version is loaded into the factory HMTF using a USB flash drive. The image can be obtained from a Honeywell representative or via the honeywellprocess website.

FMC722 Best Practice topology



OneWireless

Refer to One Wireless best practices for connection of the OW system to FTE.

Matrix of equipment connections

The following table shows the matrix of connections of equipment compliant with best practices in the Experion network.

Controller	CF9	L1 Cisco	L1 *HP2620-24	L2 Any	HMTF/(F)/HMRF (+Cisco)	OWF	Generic Tofino w/EIP LSM
C300	Y	N	Y	N	N	N	N
ENIM	Y (EUCN)	Y	N	N	N	N	N
EHPM	Y (EUCN)	N	N	N	N	N	N
FIM(4&8)	Y	N	Y	N	N	N	N
FTEB	Y(for Series A I/O)	Y	Y	N	N	N	N
PGM	Y	N	Y	N	N	N	N
SM	Y(except for Safenet over FTE)	Y	Y	Y (S)	N	N	N
PMD	Y	Y	Y	N	N	N	N
HC900	Y (C)	Y (C)	Y (C)	Y (S)	Y (if (C) and a configuration PC is to be used)	N	N
Master Logic	N	Y (C)	Y (C)	Y (S)	Y (if (C) and a configuration PC is to be used)	N	N
RC500	N	N	N	Y (S)	Optional	N	N
HMTF/HMRF	N	N	N	Y	N	N	N
OWF	N	N	N	Y	N	N	N
OWG (or OW switch if used)	N	N	N	N	N	Y	N
WDM	N	N	N	Y	N	N	N
3rd party Modbus	N	N	N	Y (S)	Y (C)	N	N
3rd party EIP	N	N	N	Y(S)	N	N	Y
3rd party FMC							

(C) = used for control
(S) = SCADA only
(EUCN) = EUCN configured CF9 only
(F) = HMTF with FMC 722 firmware installed
*When qualification is complete

Glossary of terms in the table

Controller	Description
C300	Experion series C controller
FIM(4&8)	Experion series C Fieldbus Interface Module
FTEB	Experion series A controller
PGM	Experion series C Profibus Gateway Module
SM	Safety Manager
PMD	Pulp and Paper machine controller
HC900	Hybrid controller
Master Logic	Honeywell MasterLogic PLC
SC500	Honeywell RTU
HMTF/HMRF	Honeywell Modbus TCP Firewall (and read only firewall)
LSM	Loadable Security Module
OWF	One Wireless Firewall
OWG	One Wireless Gateway
Tofino	Belden/Hirschmann industrial firewall
WDM	Wireless Device Manager
3rd party Ethernet IP	I/O devices and PLCs that use the EIP protocol
3rd party Modbus	Any non-Honeywell device using Modbus TCP

Secure Communications

Starting in R430 selected Level 2 and Level 1 nodes will use secure communications for all data transfers to another secure node. There are new configurations for FTE Qualified switches to support this and there is a new configuration (Revision JJ) for the CF9. The new configurations allow the IKE authentication and key exchange ports to pass through L1 switches and CF9s. In addition, the ESP protocol is allowed through these switches. All FTE Qualified switches must be updated to the latest image that supports DSCP trust to enable the same QoS as current switches for the secured packets. The CDA protocol will apply the proper DSCP level in the packets on transmit. Note that 2950 and 3550 switches will not be able to be upgraded with the new configurations. They must be replaced with the latest qualified switches before enabling secure communications.

The crypto image of Cisco IOS with the SSH capability has been qualified for all of the current qualified switches. Honeywell has qualified the application TeraTerm for use as a SSH client for configuration and debug. This tool is qualified on Experion Station and Flex PCs.

The configuration and use of secure communications in Experion is documented in the Secure Communications User Guide - EPDOC_X270-en-430.

5. Level 3

Description

In Level 3, all of the subnets on the plant-wide network, including FTE communities, are tied together. Additionally, the Level 3 router may be connected to Level 4 through a firewall.

Level 3 Best Practices

In order to accomplish control strategies from one FTE subnet to another FTE subnet, complete access between servers on each subnet must be allowed.

Implementing Level 3 Best Practices

The following list summarizes the networking configuration requirements for Level 3 of the FTE network:

- Provide access between FTE community subnets by grouping servers into an IP address range that can be separated from the other Level 2 nodes through use of a subnet mask, as discussed in the IP addressing section.
- The use of unicast for DSA keep alive messages is the best practice. Multicast is less desirable, but if it is used, enable IP multicast routing for the DSA multicast address, which is 225.7.4.103, and create an access-list filter to allow only this multicast address to pass to the FTE subnets. Redirection Manager may also use multicast addresses as described in the paragraph Redirection Manager below.
- Configure each FTE subnet to be in a separate VLAN, different from VLAN1.
- Connect only Switch A (Yellow tree) to the router. If multiple connections are desired see the paragraph Multiple connections from L2 to L3 Best Practice below. The router interface connected to FTE must be a routed interface. The “no switchport” configuration statement must be attached to the interface.
- Configure access list filters for the FTE communities that:
  - Permit filtered access only to the server IP range, limited to the necessary IP addresses and ports.
  - Allow established access to the remainder of the FTE subnet for DC access.
  - Permit secure communication initiation and protocol through the router
  - Allow single IP address access only to selected distribution/collection nodes in L3 or DMZ with ports limited to those necessary.

    - WSUS
    - Virus update
    - Patch distribution
    - Service node

  - Deny all other access to the FTE subnet.
- If not using SFP/GBIC connections, configure the FTE switch's router interfaces for 100-Mbps Full Duplex.
- **Note**: IPservices IOS version for Cisco switch/routers is needed for routing to prevent performance problems that the IPBase software will cause due to lack of resources.
- It is CRITICAL that the router interface be configured for no ip proxy arp. If proxy arp is allowed, view to controllers can be lost under certain conditions. R400 introduces a proxy ARP detector. If a router is not configured for no ip proxy arp, then an alarm will be generated in the system status display.

NOTE: The router must be connected to a Level 2 switch interface that is configured as an uplink port, or to a SFP/GBIC-based interface.

Redirection Manager

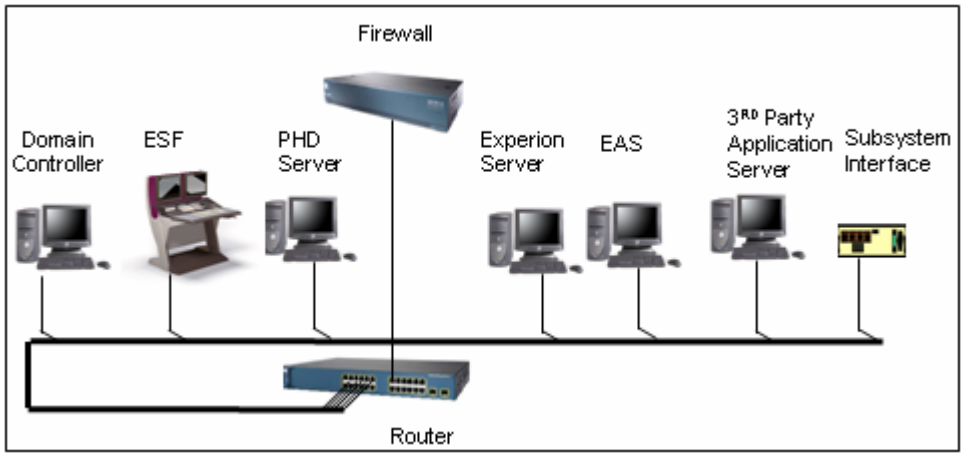
Honeywell's Redirection Manager (RDM) can use the FTE multicast test message multicast from the servers to keep track of when the primary OPC server goes off line. It is the best practice to use the multicast only when the OPC client is in the same FTE community as the servers. When the OPC client resides in Level 3, or when the client is in another FTE community, then a mechanism using ICMP must be selected. In this case, ICMP must be allowed between L3 nodes and subnets.

Multiple Connections from L2 to L2.5 or L3 Best Practice

Dual connections between the FTE backbone switches and Level 2.5 (see section 7) or Level 3 may be desired. The best practice in this case is to use two routers that are running the Hot Standby Router Protocol (HSRP). HSRP will provide a redundant level of protection in both connection and equipment for the Level 3 router. The Level 3 nodes can connect redundantly to both routers using dual Ethernet or can be single attached to the primary router. The HSRP algorithm will protect against Level 2 cable failures or routing failures that will cause loss of communication when the Level 3 node is single attached. The configuration of the router is not possible with a standardized configuration file. It is recommended that Honeywell Network Services group be contacted for router configuration consultation.

Recovery times of L2 to L2.5 or L3

Faults in a communication path of data going between L2 communities and L3 subnets are not within the control of the FTE algorithm. This can affect the recovery times of DSA, FDM and other communications going between FTE communities or FTE communities and Level 3. There are several mechanisms in combination that can lead to longer outage times. Cisco HSRP has a minimum limit on the test messages period of 2 seconds. In addition, it takes 2 missing messages for a maximum of about 6 seconds to detect the fault. On recovery of the fault, several mechanisms can interact causing increased recovery times. HSRP will discover the path is complete again and will revert immediately to the original primary. Routing will take some time to recover from the change of path when the primary changes back. In addition, because the connection to the FTE community is a routed interface, the spanning tree in the switches will cause the port to block. The blockage occurs because the port is configured with an expectation that network equipment is connected. When it does not see BPDU packets from the router, due to the routed port configuration, it will revert to standard spanning tree. The outage caused by this can be up to 45 seconds. It is important to note that fault tolerance methods other than FTE have no method of guaranteeing 2 second recovery times. Thus if a communication path is critical enough that it cannot tolerate this level of outage, then consider including the path in the FTE community where the critical communication originates.



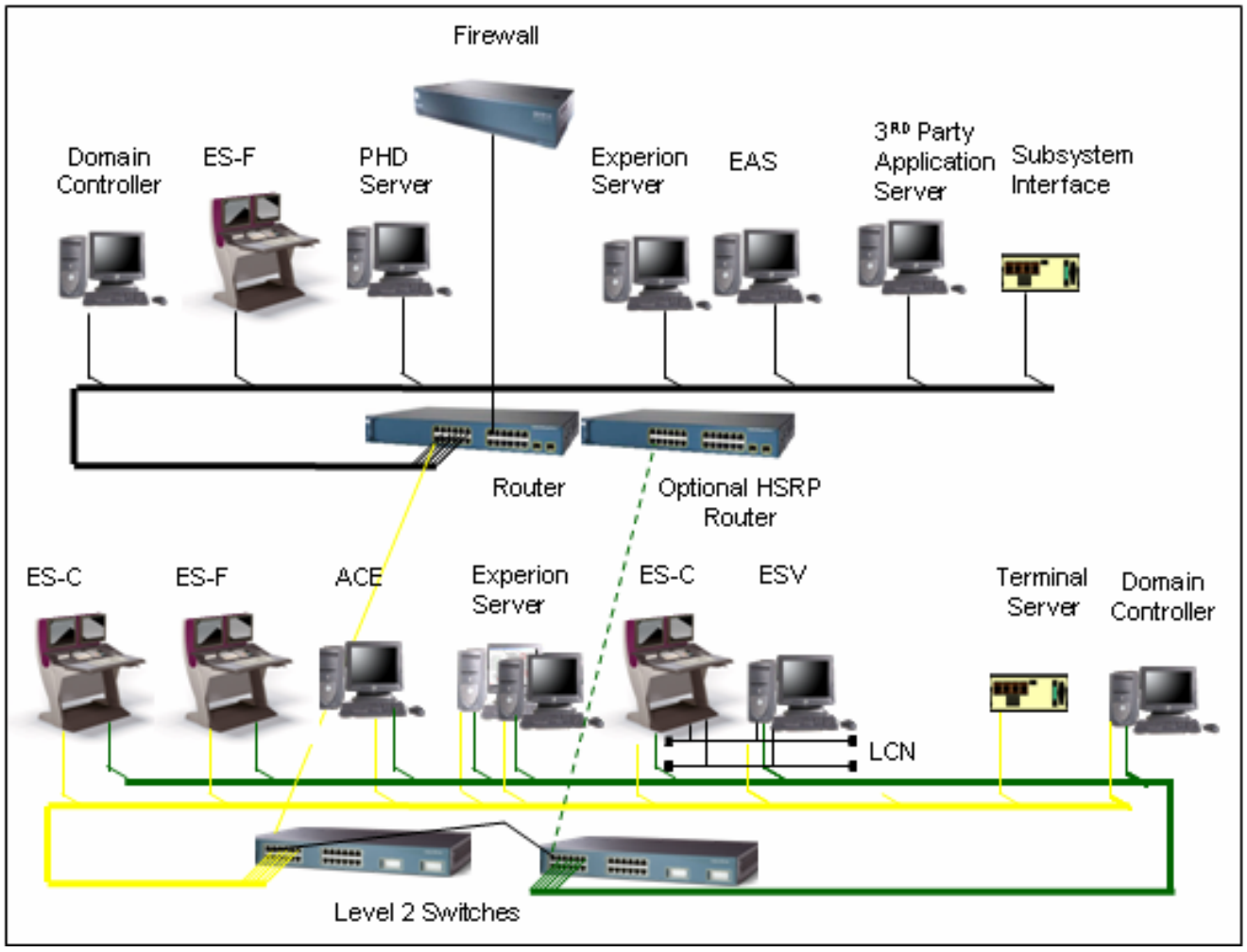
Level 3 LAN

Citizenship

- Plant Historians
- Applications
- Advanced Control
- Advanced Alarming
-

Router / Switch3 to L2 Connectivity – Routing

- Cisco 3560 or 3750-- recommended router between L3 and L2
  - Security Filter to permit communications to and from specific nodes (may be implemented in Cisco ASA Firewall)

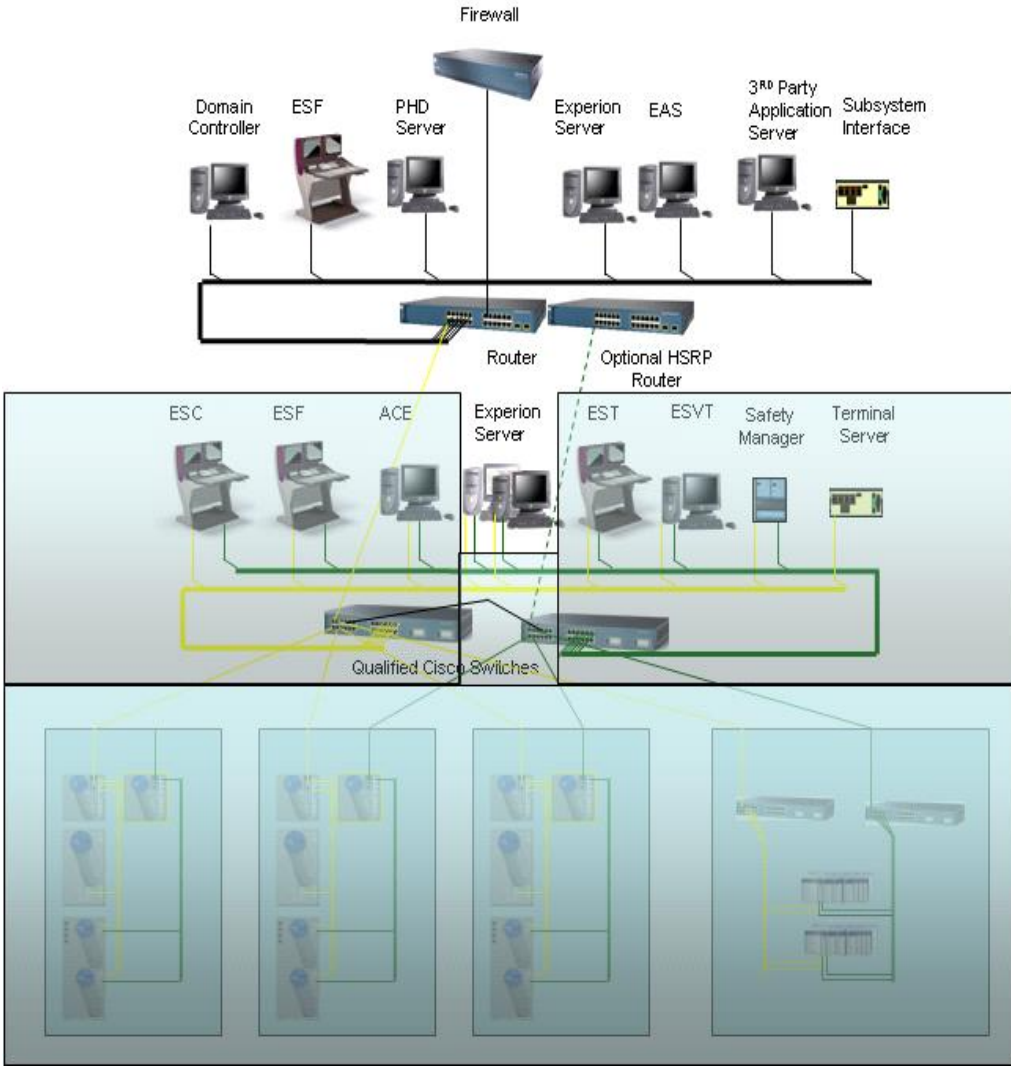

Firewall
Domain Controller
ES-F
PHD Server
Experion Server
EAS
3RD Party Application Server
Subsystem Interface
Router
Optional HSRP Router
ES-C
ES-F
ACE
Experion Server
ES-C
ESV
Terminal Server
Domain Controller
LCN
Level 2 Switches

Domain Controller Best Practices

Systems that use domains must carefully configure the domain controllers to ensure that proper authentication and name service perform correctly.. Misconfigurations or problematic upgrades from Windows 2000 to Windows 2003 or to Windows 2008 server based domain controllers can cause disruptions in communications with shares and OPC.

The primary domain controller must be at a level where all nodes can access it. Honeywell strongly recommends that a peer domain controller be present in the network for backup. The logical place for the primary domain controller is at Level 3. A peer domain controller can also be located in Level 3. However, for optimum coverage in case of a communications failure of a FTE community with Level 3, place a peer domain controller in each FTE community.. Starting with Windows 2003 server, FTE is qualified to run on domain controller servers.

View of L2 from L3 with Routing and Filter



- Level 3 Router/Switch (Cisco 3560, 3750 or equivalent)
    - Provides connectivity for L3 devices and L2 networks
    - Has customer-defined route between L3 and L2
        - Routes between Enterprise IPs on L3 to Private L2
    - Implements Access List Filtering
        - Domain Controller / Management (L3 DCs and L2 Nodes requiring authentication)
        - Limits access to only those L2 nodes that need to communicate with L3
        - Uses single IP limiting on nodes needing to contact all L2 nodes such as the WSUS
        - Prevents any communication with L1 controller nodes
        - Permits secure traffic

6. Level 4

Description

Level 4 is not part of the control network. Communication on this level may not be as secure as that on Level 1, Level 2 or Level 3.

Level 4 Best Practices

Because Level 4 is a different security and networking environment, Honeywell strongly recommends that Level 3 and Level 4 be separated by a firewall. Honeywell also stronly recommends the use of a L3.5 or DMZ (see section 5 on DMZ)

Implementing Level 4 Best Practices

Requirements for a firewall between Level 4 and Level 1, 2 and 3:

- The firewall should limit communication to only those nodes on Level 4 that require access to nodes on Level 3.5.
- Level 1 nodes must not be allowed to communicate with nodes on Level 3 or on Level 4.

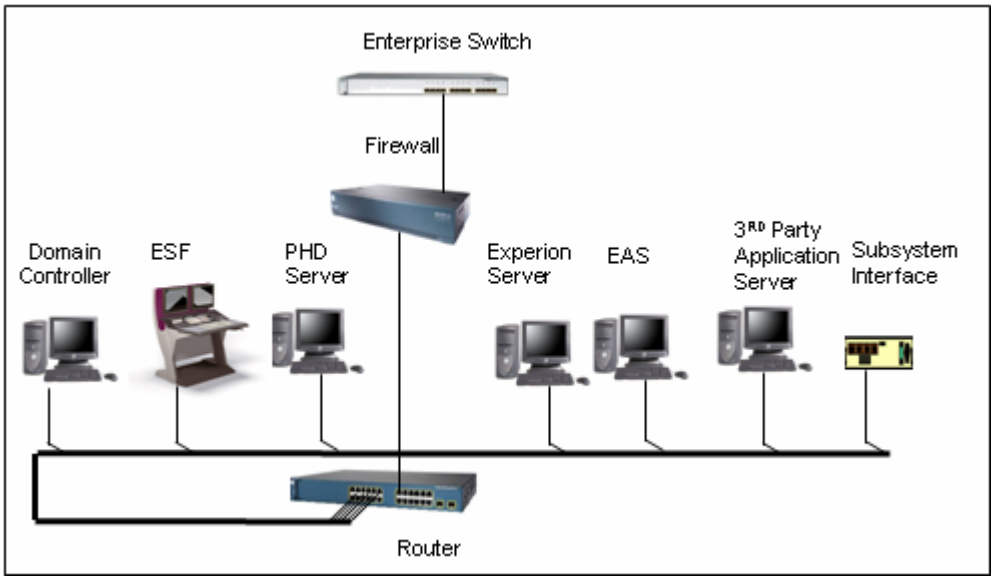
Router

The router-to-firewall connection should be a single point of connectivity. For redundant routers and firewalls, into each instance of firewall and router. This will enable higher security and improved management. A major advantage is the user just needs to pull a single cable per firewall to make an “air gap” between Level 3 and Level 4. The connection to the firewall isolates Enterprise LAN Broadcast and Multicast traffic while enabling connectivity between the PCN and Enterprise LAN.

Firewall

The firewall implements a restrictive security policy for traffic between Level 4 and Level 3. The firewall should deny all access to the PCN unless it is explicitly permitted. A best practice is to use IP address source and destination filtering. Only specific nodes on the enterprise network are permitted to communicate with specific nodes on the PCN. Permitted traffic must be limited to Server – Server traffic only (e.g., Experion Server or PHD). TCP Port Filtering is the best practice to stop denial-of-service attacks to well-known ports. While a firewall between L3 and L4 is the minimum recommendation for Experion networks, use of a DMZ is strongly recommended for critical control networks.

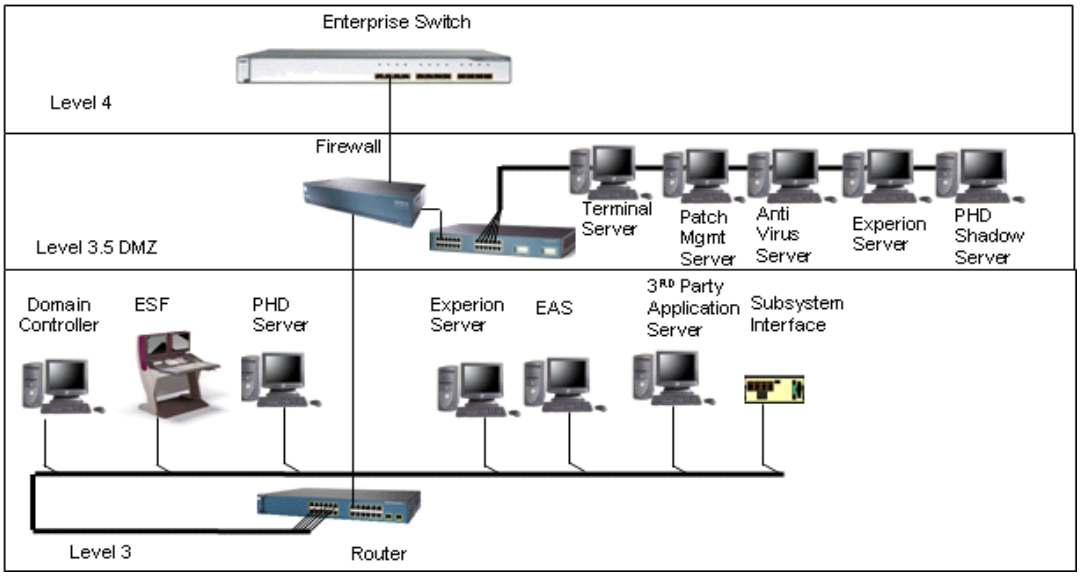
Process Control Network to Business Network



DMZ

Systems that require L4 nodes to access data on L3 or possibly L2 are recommended to use a “DMZ” or Level 3.5. Further, only nodes on L3.5 are allowed access from L4. These nodes are also accessible from L3 and L2 if necessary. Data for enterprise servers can be obtained by having an Experion server in L3.5 with DSA access up to L4 and down to L3. Terminal servers and virus update file servers can also be placed in the DMZ. The DMZ can either be a third leg on the firewall, or a separate network between L4 and L2 with a firewall between both L3.5 and L4 and L3.5 and L3. Further discussion of this best practice can be found in the Honeywell Security Planning Guide document.

L3 to L4 connection with DMZ



7. Variations on Best Practice

Low Cost L1 Switches for cost sensitive projects

To remain competitive in cost sensitive projects with large numbers of FIMs Honeywell has qualified a lower cost switch and provided a configuration for L1 use. These switches are the Cisco SFE2000 (now EOS) or the HP 2620-24 (SH-2620R4). The configuration includes QoS for CDA packets, multicast and broadcast protection and port filtering. Port filtering is used to only allow those TCP/UDP ports necessary for Level 1 operation and 802.3x Ethernet flow control. The projects that use this switch instead of CF9s must be aware that the CF9 has significant advantages over the low cost switch. It is the responsibility of Honeywell project services to make the customer aware of the differences. These differences include, temperature range, corrosion protection, mounting, and redundant power from the physical side.
From the security side, certain protections are missing from the SFE 2000. These include SYN attack protection, throttling of certain network management packets such as IGMP, NTP and SNMP. In addition, the broadcast and multicast limits of the SFE2000, when hit, will cut off all traffic including TCP and UDP unicast. Customers that are willing to accept the risk associated with this lower level of security may use the low cost switch in place of the CF9.
It is important to note that other qualified switch types must *not* be used for this application. The low cost substitution is limited to only the SFE2000 or HP2620-24, because theyare configured and qualified with the 802.3x capability needed to protect the controller from excessive traffic.

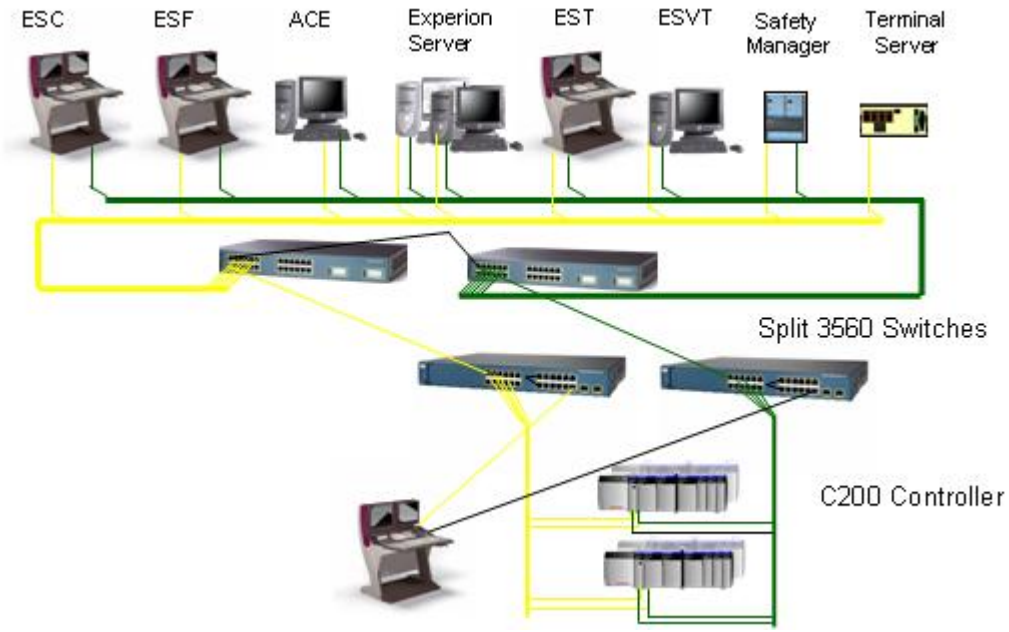
Feature	CF9	Cisco SFE2000	HP 2620 (SH-2620R4)
TCP/UDP port filtering (ACLs)	YES	YES	Yes
ICMP, NTP, IEEE-1588, TCP syn/rst rate limiting	YES	NO	NO- TCP sysn/rst rate limiting, ICMP is not allowed
Destination Lookup Failure (DLF) storm limiting	YES	NO	NO
Broadcast storm limiting	1Mb	3.5Mb for gigabit uplinks 2Mb if gigabit uplinks are not used *	1 Mb
Multicast storm limiting	2Mb	3.5Mb for gigabit uplinks 2Mb if gigabit uplinks are not used *	2 Mb or 3Mb for systems larger than 200 nodes
Spanning-tree	No	MSTP with BPDUguard on non-uplinks	MSTP with BPDU guard and loop protection on non-uplinks
QOS	Prioritize traffic local to the CF9	Prioritize CDA and FTE traffic	Prioritize CDA , FTE, and EUCN Controller Traffic
Flow control	YES	YES	Yes
Multiple MAC port blocking	YES	Port security optional	Yes
Secure communication	Yes	No	Yes

*WARNING: when the storm limits of the SFE2000 are exeeded, all traffic will be cut off. This includes TCP and UDP traffic used for controller-I/O communication.

Remote Locations

It may be necessary due to geographic limitations to make certain changes to the best practice architecture. The site may want to add one L2 console station node at a satellite control area for a roving operator to have a view to the process, or in case of a catastrophic break in the communications paths to the control room. In this case, it is acceptable to put the L2 station directly on mixed or split configured switches. Mixed configurations must only be used if 2950 switches are used. 2960 (or 2960plus) switches are available in a split configuration and it is best practice to use this configuration to protect the L1 nodes from the L2 traffic. Failure replacements of 2950 with 2960(plus)) may use the mixed configuration to be compatible with the replaced configuration.

.

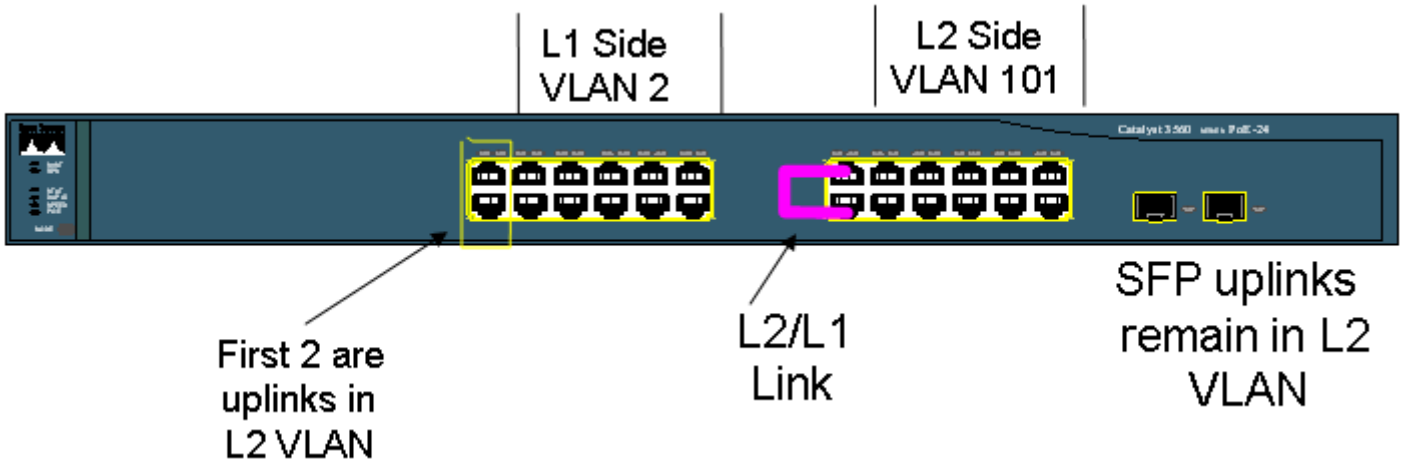


System with Console on Split L1|L2 Switches

If it is necessary to have multiple L2 nodes at the remote location, then it is the best practice that separate switches be used for the L1 controllers with uplinks to the switches where the servers and stations reside. The flow of data should be from L1 switches to local L2 switches then to the top-level switch pair at the central location. Or, a pair of switches with a split L1|L2 configuration could be used, where one section of a switch has L1 configuration and the other section has L2 configuration. Switches that can support L1|L2 split configuration are listed in FTE Specification EP03-500-300 (and later). Split switches should always be configured offline and added to the network when the configuration is verified. The L1 side of a split switch does not count in the 3 levels of switch limit.

Split Switch Configuration

- Switch is split in two pieces- one for L2, one for L1
- A New VLAN is created for the L1 side, L2 uses the FTE community VLAN
- A cross-level cable connects the two VLANs and L2 to L1. It must be a crossed cable, ie. the transmit and receive pairs must be crossed.
- Spanning tree is configured to prevent blocking between sides
- Filtering on the input to the L1 side passes all CDA TCP ports and all established traffic, all UDP and NTP.

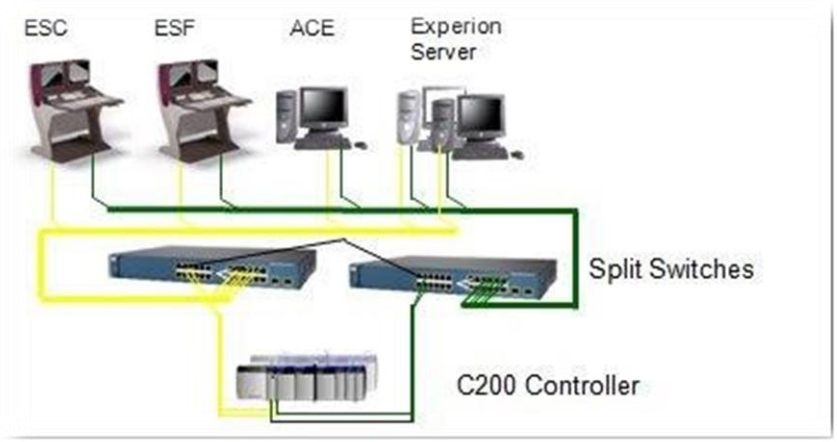


- Multicast policing @ 2 Mbps and broadcast storm limits at 1 Mbps are configured
- Only the Cisco Catalyst 2960, 2960Plus, 3560-24, and 3560V2-24 and the Cisco IE 3000 switches are supported in a Split Switch Configureation.

WARNING: it is essential to configure a split switch offline. Additionally, do not reset a split switch to a default configuration. The results can cause undesired effects in the network due to the L2/L1 link.

Small Experion Systems with FTE

The Experion system is expandable from very small systems with only a few nodes to very large multi-cluster and multi-FTE community installations. For small systems where all the FTE units are co-located, the best practice topology can be less restrictive to save cost. In this case, all units can be on the same switches. The split switch configuration file would again be used for this installation. When the installation requires multiple layers of switches or is geographically spread, then the Honeywell best practices should be followed.



Small system with single layer of switches.

8. Added Security Layer for Extra Protection

Expansion of the capabilities of the Experion system necessitates that high security communications expands beyond the FTE community. Introduction of a new secure network layer, Level 2.5, accommodates these new capabilities. This new network layer enables Peer-to-Peer communication between Level 1 nodes without exposing them to Level3 access. Contact for PCDI communications between controllers and devices outside of the FTE community is also possible. For Experion nodes deployed on Virtual Machines, Level 2.5 provides a secure method of distributing the management and storage area network between FTE communities without open access of these networks to Level 3 is part of this protection.

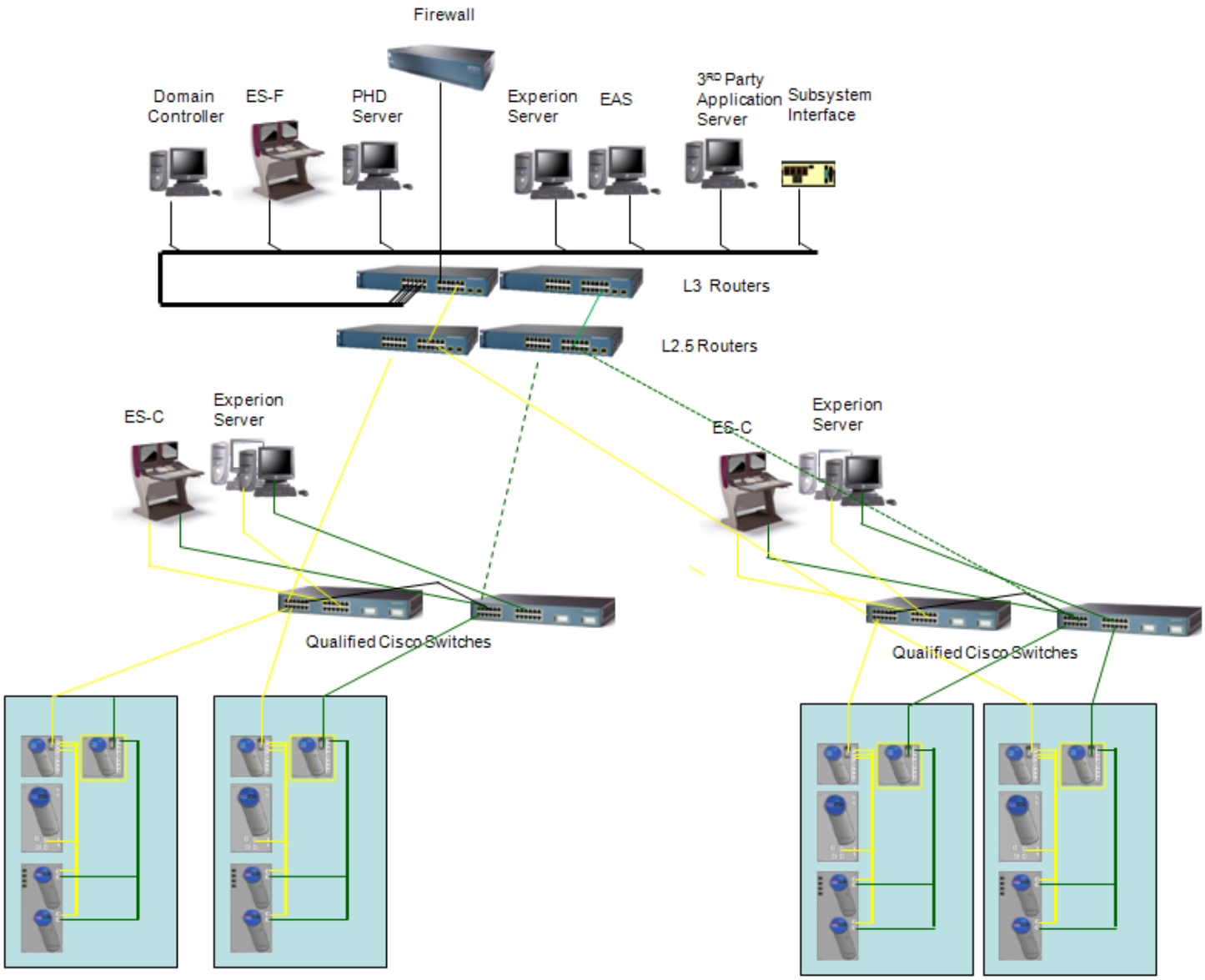
Cross Community Peer to Peer and PCDI communications

In order to protect the process, it is recommended that Level 3 PC nodes are not allowed to communicate with Level 1 embedded nodes. Exceptions are possible to enable cross community peer to peer but the project must understand and mitigate the risks involved, including additional security configurations. Exceptions include a Modbus node communicating with a dedicated C300 controller, or a pair of dedicated controllers in separate communities for batch control introduced in R410.

Access lists will help keep unauthorized nodes from having access to controllers. Additional protection is possible by ensuring that no I/O devices are connected to the Inter Cluster Peer-Peer nodes. In this scenario, the communication is purely PCDI, exchange block or CDA peer-peer with another dedicated controller or Modbus device in another community and local P-P with nodes in the same community.
This control strategy is only possible if a dedicated router is used between communities. That is, the router is connecting FTE communities and has a separate connection to Level 3 where optimization, history and other PC nodes connect. ACLs MUST be configured on the Level 2 interfaces that contain individual permissions to IP addresses, and ports of the dedicated Level 1 nodes. Example of an IP addressing scheme is shown in the section on IP addressing of this document. Examples of ACLs for a Cisco router are shown in the example router configuration section.

Other Level 1 nodes in the community MUST be denied access from outside of the community. ACLs MUST be configured on the Level 3 interface to deny any Level 3 access to Level 1 nodes.
Allowing this type of access requires advanced knowledge of router configuration. Users that are not familiar with this level of configuration should revert to the rule that no access to Level 1 controllers from outside of the community should be allowed. Assistance with configuration of IP addressing and ACLs is available from Honeywell Network Services. It is a best practice to use the same link bandwidth from L2.5 to L3.
An example configuration is included in the switch configuration files starting with R410.

Any communities that are reusing IP addresses for L1 nodes will not be able to use cross-community Peer-Peer as the addresses are in conflict. See the section titled IP address reuse below for further explanation.



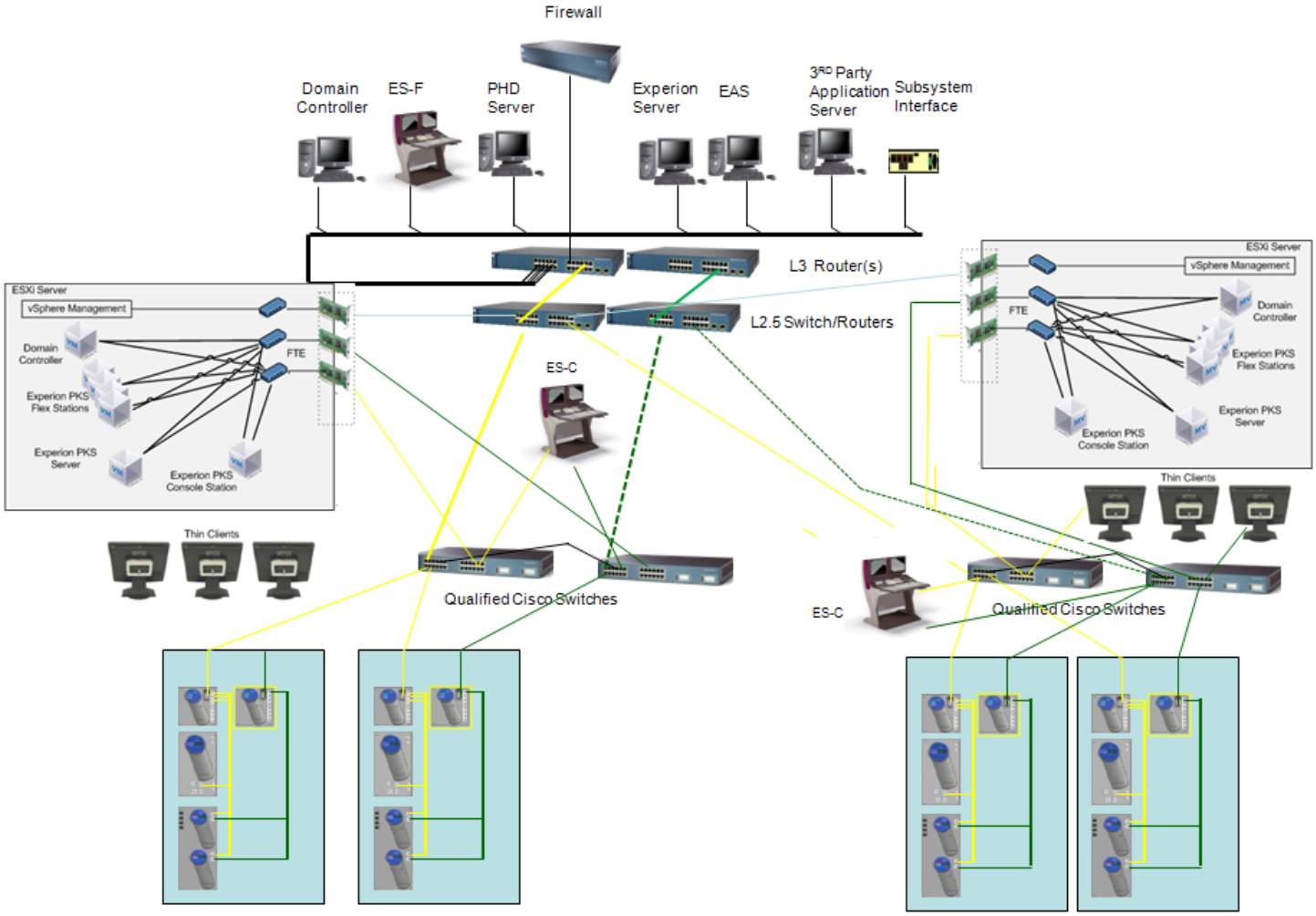
Cross community peer-peer with “L2.5” secure router protection

Additional networks used with Virtual Machine configurations

The use of virtual hosts has been growing recently for its many benefits including consolidation, footprint reduction and extended lifecycle opportunities. Experion is now available to run in a virtual environment. Deploying Experion on a virtual platform introduces the need for additional network(s) support the virtual infrastructure. This new network supports management of the virtual infrastructure (e.g. server hosts, virtual infrastructure client PCs, NAS, etc). The network also supports virtual machine backup and recovery In some cases, separate networks for the storage of the VM images’ virtual hard disks are introduced. The use of virtual storage networks is not currently supported at Level 2 when deploying on a virtual platform.

The management networks should be considered as critical as other Level 2 nodes. This is because a compromise to these management networks can interfere with the operation of the real time control system. For this reason, a L2.5 layer is recommended as best practice for management networks. Refer to the Experion Virtualization Planning and Implementation Guide for topology options that are aligned with the Experion Network Best Practices.

One cost effective option is to implement the management LAN in a VLAN in the L2.5 switch/router. The example shown below uses this configuration. Other examples may have a separate network just for management with its own switches. This network is then connected to the L2.5 router. Redundancy of the management network is optional. Honeywell has used the Cisco 3560 gigabit class of switch/router in lab tests with success. An example configuration is included in the switch configuration files starting with R410.
Access lists are added to limit the access to management network. The defined ACLs used are meant to limit access to the management network, allowing only those messages used for management.
The Experion Virtualization Planning and Implementation Guide also defines virtual machine consolidation guidelines. Please refer to the latest version of the guide for consolidation recommendations. In the example shown below, thin clients are used to connect to Experion Flex station virtual machines that reside in the server host. Virtualized Experion systems can be a combination of virtual machines on server hosts and external "bare metal" nodes. Deploying on a virtual platform with local storage limits the options for workload recovery in the event of a complete server host outage. In this case, users may opt to keep consoles on bare metal, especially if they are in a remote location.

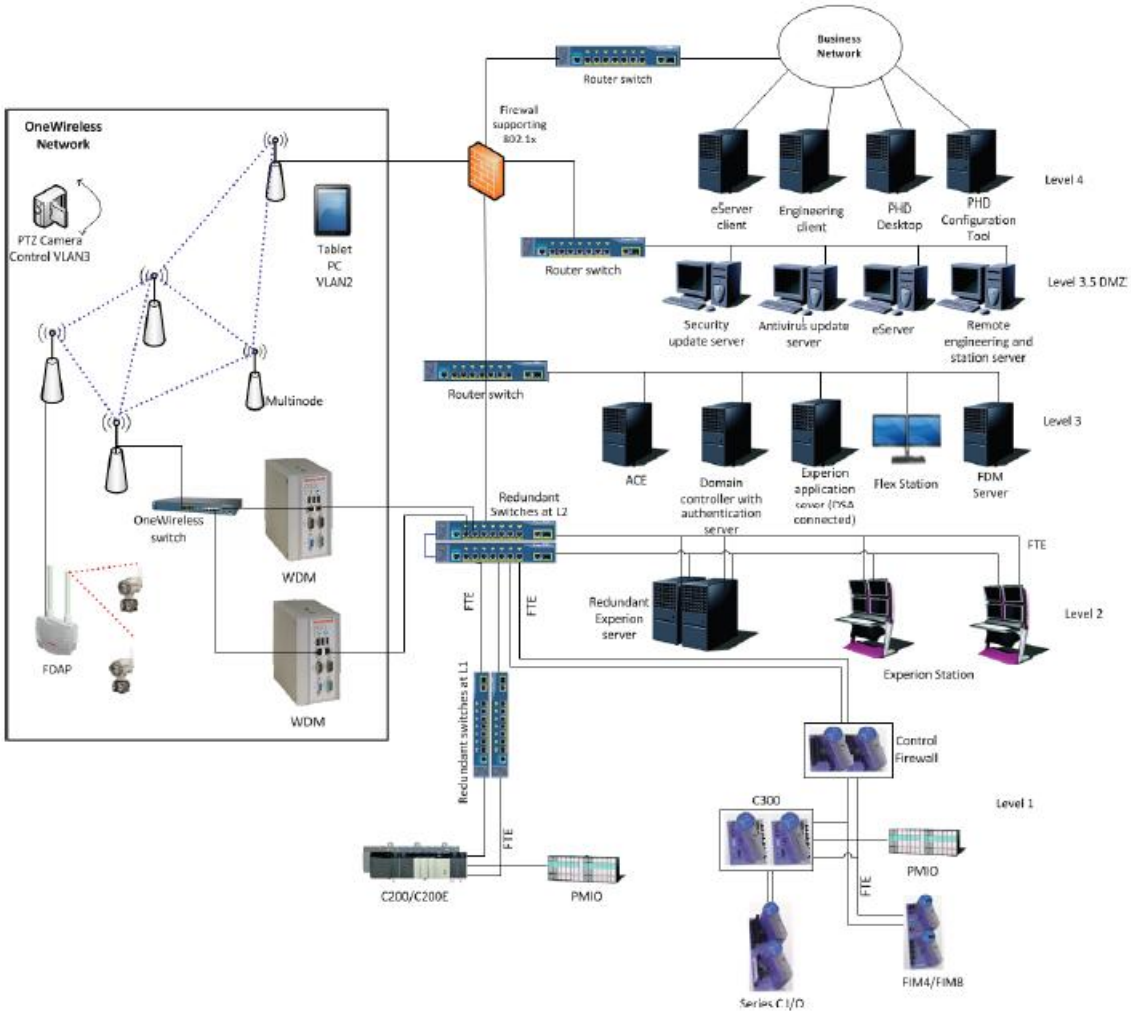


Virtual Network Support in Experion

9. One Wireless Network

OneWireless is an integrated wireless sensor and 802.11 network that can be connected into an Experion Network. Process data from the ISA100 wireless network is routed through the Wireless Device Manager, WDM to Level 2 using OPC, Modbus, HART or CDA protocols. All other wireless traffic, such as data from video monitoring devices or wireless worker terminals, is routed to the DMZ via a separate interface and security level in the firewall. The WDM performs a firewall function and gateway process. The data access is configured in Control Builder. Encryption and authentication protects data throughout the entire wireless network. Further information can be read in the OneWireless R210 Best Practices white paper available on HoneywellProcess.

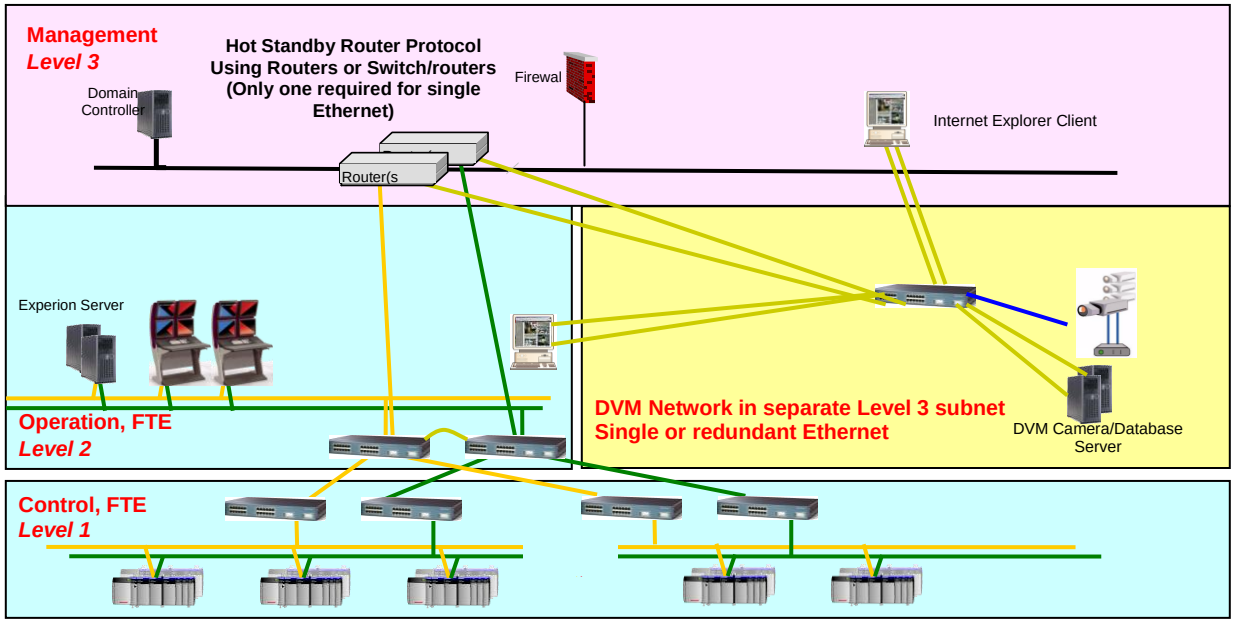
One Wireless Network topology



10. DVM Best Practices

The Digital Video Manager is capable of consuming a great deal of bandwidth depending on the configuration. For this reason, the best practice for DVM is as follows:

- Create a separate subnet for the cameras and DVM server on Level 3
- Utilize separate display nodes in this subnet for heavy traffic DVM displays
- Limit the traffic in Station and Server nodes to less than 20% of the bandwidth
- Baseline CPU utilization for required DVM displays
- Always use unicast for DVM. Multicast will trip storm limits in the FTE Qualified switches
- Use 1 GB port connections on FTE Qualified switches for DVM Console connections.



DVM Network

11. IP Addressing

With Experion controller nodes in the FTE community, communication reliability and security must be carefully planned.

Recent discoveries in the operation of Cisco router have led to a change to the default FTE multicast address. The IANA assigned address of 224.0.0.104 will no longer be used. The effect seen in the router is high CPU utilization for systems with many communities of near capacity FTE node counts. If the aggragite traffic from the FTE communities is greater than about 5000 packets per second, the CPU utilization just from servicing the FTE packets can go above 50%. Changing the FTE address out of the 224.0.0.x range will help cure this problem. This effect is only seen on very large systems. There is no need to change existing systems that do not have the levels of traffic described. The CPU usage in the routers can be checked by a qualified network technician. The R400 FTE IP address will be the same as previous releases of 234.5.6.7. This address is outside of the range that is forwarded to the CPU.

R400 has introduced a new FTE driver in PC based nodes called the “Mux”. Unlike previous FTE driver versions which had two TCP/IP stacks, this version only has one stack. What that means is only one IP address is needed. The Yellow adapter is given the address to use before FTE is loaded. The Green adapter does not need an address and can be set for DHCP if there is no DHCP server in the network. This will save addresses in the user IP address range. If there is a DHCP server, it can be set to an unused IP address in another range, or obtain an IP address from the DHCP server if there is a sufficient number of addresses to cover the Green adapters of all PC nodes.

Embedded Experion nodes use a special Experion BootP server to obtain IP addresses. It is critical that if more than one server is enabled in a FTE community, that the parameters configured in that server and in Control Builder are identical. Loss of communication, view and control may result if these parameters are not set correctly. Refer to Experion Knowledge Builder for the proper BootP configuration. The parameters are:

- IP Address Base - from Control Builder
- Subnet Mask - from Control Builder
- NTP server IP address - from Control Builder
- Default Gateway - from Control Builder
- Source Port - from Windows FTE driver in the server
- Destination Port - from Windows FTE driver in the server
- Pulse Period - from Windows FTE driver in the server
- Disjoin Multiplier -from Windows FTE driver in the server
- Time-to-Live - from Windows FTE driver in the server

NOTE: it is critical to the operation of the control system to be diligent in configuring IP addresses. Duplication of a server or controller IP address can cause loss of view or control. Best practice is to connect unpowered nodes into the Level 2 network and then power up. The ARP resolution test of the node can then discover duplicated IP addresses. Never plug a running node or switch with connected running nodes into the Level 2 network without a thorough audit of the IP addresses being used and compared with the addresses in the Experion nodes.

During Migration or in a mixed-release community, the bootp server should be running on the newer-release Experion Server.

Network topologies and security through IP addressing

The best form of security is “air gap”; that is, no connection between the control LAN and any other users in the plant. Unfortunately for security, most installations must have some form of communication between the control LAN and the plant LAN, so we must pay careful attention to IP Address management. Honeywell has developed several recommendations for IP address range selection to increase the security when connecting the Control LAN to outside communications networks. Another goal is to simplify selection of IP addresses for FTE networks. The examples in this paper all use a range of 10.n.n.n.

The types of networks are:

- Completely isolated FTE community
- Multiple FTE communities isolated from Level 4 networks
- FTE communities connected to Level 4 with private IP addresses
- FTE communities connected to Level 4 with corporate IP addresses

Completely Isolated FTE community

Even if there is complete isolation of the control LAN from the IT LAN, IP address ranges and rules should follow the best practices of the multiple isolated or DSA-connected communities described below. If the network expands so that a router is needed at a later day, the IP addresses will already conform to the Honeywell best practices for connected networks.

Multiple FTE Communities Isolated from Level 4 Networks

Plant-wide networks may contain several FTE communities connected by routers. If this network arrangement is isolated from the IT LAN, then Honeywell recommends that private IP addresses be used.

For ease of configuration, a simple address range of 10.CN.X.Y can be used for IP address distribution. CN stands for FTE community number. Multiple FTE communities can be connected together with a router. For example, the first FTE community subnet could be 10.1.x.y; the second could be 10.2.x.y, etc.

FTE Communities Connected to Level 4 with Private IP Addresses

For a plant-wide network that has a Level 3 network that connects multiple FTE communities and other plant Ethernet based nodes, Honeywell recommends using private IP addresses with Network Address Translation (NAT) for communication with Level 4. The NAT can be accomplished with a firewall: Honeywell recommends dedicated firewall equipment from Cisco. A Windows-based computer with firewall software is not best practice.

The private address distribution is similar to the previous scheme where the FTE communities are 10.1.X.Y, 10.2.X.Y, etc. X stands for the range of addresses where the two types of nodes exist. The servers must be in a separate range from other L2 nodes. An example would be 10.1.0.Y for server nodes, 10.1.1.Y for station nodes, and 10.1.2.Y for any other nodes such as ACE, PHD and third party IP-based nodes. Y stands for any address between 1 and 255. If the FTE community is connected to a router, the router interface IP address should be in the range where the servers are configured. In the above example, the router interface IP address would be 10.1.0.1.

Level 1 nodes should be in the address space above the other nodes on L2 and outside of the range of the subnet mask of the router interface, but within the subnet mask of the nodes that need to communicate. Thus, using the previous examples, the L1 addresses would appear in the range 10.0.4.Y. Nodes on L3 must not be able to communicate with the L1 nodes. The nodes will have the following subnet masks:

- L2 Servers and console stations with communication to L1 nodes: 255.255.248.0
- L2 nodes with no communication with L1 nodes: 255.255.252.0
- L1 controller nodes: 255.255.248.0
- L3 router interface to L2 255.255.252.0

IP Addressing Level 4 Connected Networks with Corporate IP Addresses

When it is necessary to use IP addresses from the corporate allocation, the L2/L3 addresses must be unique and compatible with L4 addresses, and NAT cannot be used. To minimize the number of corporate IP addresses used, the above addressing scheme cannot be used. Honeywell recommends a method that conserves addresses but is more difficult to configure, which is to obtain a subnet size that will cover all of the L2 nodes. The server range is contained in the lower addresses and the other L2 nodes would start on a power of 2 boundary. This is necessary so that the ACL filter used in the router to limit full access to the server nodes can be configured with a subnet mask defining the server range.

The following is an example of a FTE community subnet containing:

- 5 servers
- 10 stations
- 2 ACE
- 10 terminal servers
- 10 Controllers with FTEB

A range of addresses is obtained from the corporate range, which for this example is 164.1.0.0 with enough addresses for 126 nodes, the subnet default gateway and the subnet broadcast address. The address distribution would be:

164.1.0.1	The routed interface IP address with subnet mask of 255.255.255.192, enough for 62 usable nodes, the subnet mask and the subnet broadcast address.
164.1.0.2-15	Server nodes (5 servers 2 addresses each starting at address 2 rounded up to power of 2). The subnet mask is 255.255.255.128 to cover both L2 and L1 nodes
164.1.0.16-63	Stations, ACE terminal servers plus some spares. The subnet mask is 255.255.255.128, to cover the L2 and L1 nodes
164.1.0.64-127	FTEB (controller addresses must be outside of the subnet mask of the router interface). The subnet mask is 255.255.255.128, to cover the L1 and L2 range
164.1.0.64-127	The router interface to the FTE community blocks all access from L3 by the subnet mask of 255.255.255.192.

12. IP Address Reuse

L1 devices have the potential to consume many thousands of IP addresses in a corporate IP address space. To conserve Corporate IP addresses, an address reuse scheme is recommended by Honeywell. Only systems that have a need for address reuse should employ this IP addressing scheme. Systems that do not have this requirement must use one of the IP addressing schemes discussed above.

One range of addresses for L1-only should be requested from the corporate pool. This range can be reused in other FTE communities that are separated by a router. This range must be large enough to accommodate all of the L1 nodes on this subnet, both now and in the future. If a subnet is later added with a larger number of L1 nodes than the range obtained originally, then a new range must be requested. Existing L1 nodes would not need to have their addresses changed.

For L2 nodes that must communicate with L1 nodes in the reusable address space, a “route add” command must be configured in each such L2 node. A new service has been added for automatic insertion of the static route. This service is loaded with Experion Servers, Console stations and ACEs. The service runs on node startup and queries the server for the address range and subnet mask of the controllers. If the address of the node running the service is not in the range of the controllers, then the static route to the controller will be added to the Yellow interface. The service will test every 10 minutes for changes in the server data base and to be sure the static route is still connected to the Yellow interface. Any errors or problems will be notified in the application event log.

For nodes prior to R300, a static route must be added by hand or by a batch file that runs at node startup. Nodes that do not communicate with the L1 nodes do not need the “route add”. The following example has the L2 address range of 164.1.0.0-164.1.7.255 and the L1 address is 164.0.0.0 – 164.0.2.255. The command for an L2 node would be:

Route ADD 164.0.0.0 MASK 255.255.252.0 164.1.3.10 –p

- 164.0.0.0 is the base address of the L1 subnet programmed in Control Builder
- 255.255.252.0 allows 1024 L1 FTE nodes
- 164.1.1.10 is the Yellow interface IP address of the node being configured with the route add.
- -p makes it persistent across reboots.

The L1 nodes will receive the address range of the L1 nodes and the L2 nodes. The L1 nodes will then calculate and add a static route to their IP stack to enable communication with L2. For releases prior to R300, in order for L1 nodes to communicate with L2, the L2 address range must be a subset of the L1 range so that a subnet mask will allow the L1-L2 connection. For the above example, if the L2 address range is 164.1.0.0 – 164.1.7.255, then the L1 range in the Route Add example would start at 164.0.0.1. A subnet mask of 255.0.0.0 can be set in L1 nodes via Control Builder and communications will be open to the L2 addresses. The range can be larger than the actual L2 address range because communications will not go outside of the FTE community subnet.

Note: the reuse of IP addresses in controllers is incompatible with cross-community peer-peer. The controllers must have a unique address in each community and unique in the Process Control Network. The controller address must be routable to get to the other community and if there are duplicates in the network anywhere this will cause communication problems.

As discussed above, controller nodes with addressing in a separate subnet address range must be protected against the router proxy ARP. R400 introduces a protection method that periodically tests for the presence of a proxy ARP agent. If one is discovered an event will be generated and a system alarm will result. Users that encounter this alarm should have a qualified network technician check the router configuration for the “no ip proxy-arp” configuration on the interface

connecting to a FTE community if the router is a Cisco. Other router types will have different commands that the network technician must configure. They are too numerous to mention in this paper.

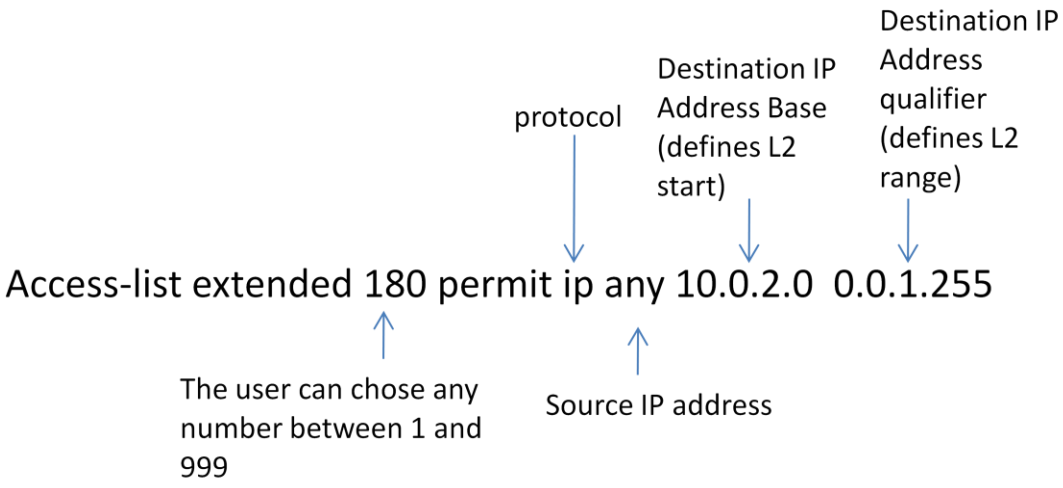
13. Rules for Inter Community Peer-Peer IP addressing and ACLs

The following is an addressing scheme that can be used when configuring a system to have inter-community peer-peer. It is chosen to minimize the number of ACLs that are needed. Consultation with Honeywell Network Services may be necessary to implement the scheme if the implementer is not familiar with routing and subnetting principals.
Note that default gateways must be assigned in the Experion Control Builder for controller devices in each community that participates in the Peer-Peer communication.

- FTE communities are evenly split in IP addressing between L1 and L2 nodes
- Minimum allocation is for 512 L1 nodes and 512 L2 nodes
- By convention, L1 addresses are X.Y.Z.0 to X.Y.Z+1.255 L2 addresses are X.Y.Z+2.0 to X.Y.Z+3.255
- Subnet mask for minimum allocation is 255.255.252.0 both L1 and L2
- Access group must be added to outputs of the routed interfaces at L3

Example Access List for minimum allocation. This subnet base is 10.0.0.0
The L1 range is 10.0.0.0 to 10.0.1.255, the L2 range is 10.0.2.0 to 10.0.3.254 (3.255 is the subnet broadcast address).
64 other subnet bases are possible with this mask scheme:
10.0.4.0, 10.0.8.0…10.0.252.0.

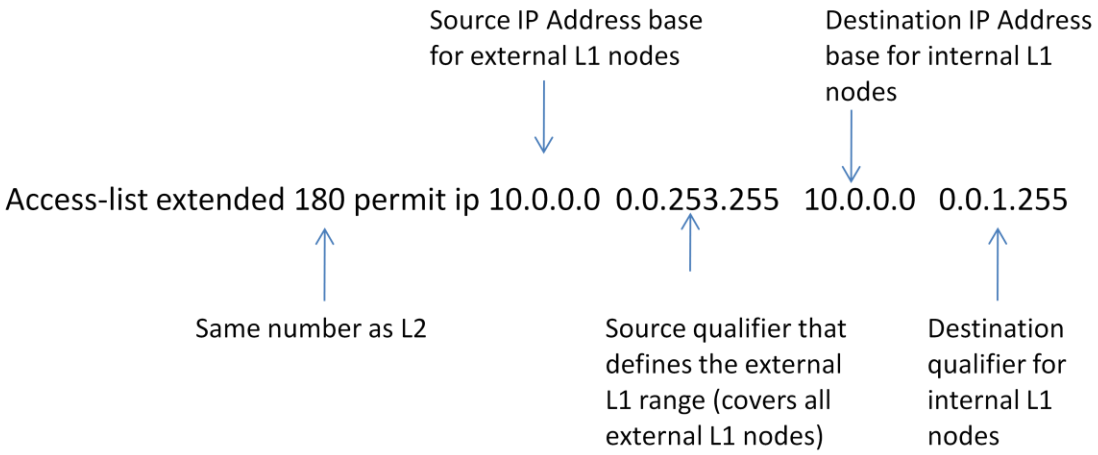
Explanation of L2 Access List



This ACL permits through any TCP or UDP packet that has an unqualified IP address as a source and the L2 range as the destination. The 1.255 in the qualifier (wild card mask) selects the L2 range.

The combination of base address and qualifier for the destination defines a range of 1024 addresses of with 512 permitted for L2 nodes. Thus 64 communities are possible using all of the third octet addresses with this minimal usage addressing scheme.

Explanation of L1 Access List



This ACL permits through any TCP or UDP packet that has an external L1 IP address as a source and the internal L1 range as the destination. The base IP address in combination with the 253.255 in the qualifier (wild card mask) selects the system wide L1 range.
The combination of base address and qualifier for the destination defines a range of 1024 addresses with 512 permitted for L1 nodes. Thus 64 communities are possible using all of the third octet addresses with this minimal usage addressing scheme.

Example Access lists and groups

The access list to permit only L1 to L1 communication for the subnet with base 10.0.0.0 is:
Access-list 180 permit ip any 10.0.2.0 0.0.1.255
Access-list 180 permit ip 10.0.0.0 0.0.253.255 10.0.0.0 0.0.1.255

The interface on the router connecting to this subnet has the access group:
IP access-group 180 out

The access list for the subnet with a base of 10.0.4.0 is:
Access-list 184 permit ip any 10.0.6.0 0.0.1.255
Access-list 184 permit ip 10.0.0.0 0.0.253.255 10.0.4.0 0.0.1.255
IP access-group 184 out

Other addressing schemes are possible, but must follow a similar structure.

14. TPS Upgrade Best Practice

Existing TPS systems have the ability to add Experion capabilities with the ESVT, ES-T, and ACE. TPS nodes that are currently connected to an Ethernet Plant Control Network (PCN) can be connected to the FTE network in one of 3 ways.

- The PCN is a stand alone network, that is, it has only control system nodes connected to the switch(es). In this case, the top of the PCN network can be connected to the top of the FTE switch tree. The yellow switch is recommended.
- The PCN is part of a plant wide network. In this case, the FTE network must be connected to the L3 network through the existing router with the required filtering described in this document on the interface that connects to the FTE network. If the plant wide network is a single network, meaning there is no router, or the existing router does not have the required filtering capability, then the FTE network must connect to L3 through a firewall with the same required filtering.
- A conversion of the PCN to FTE. In this case, qualified FTE switches must replace existing PCN switches.

15. Example Cisco Router Configuration Statements

In order to configure the FTE community filtering requirements in Cisco routers the following configuration commands are used. Cisco uses an Access Control List (ACL) to describe what should pass or not pass through an interface.

Below is an example of a set of ACLs used to accomplish the filtering:

access-list 101 permit tcp 10.0.0.0 0.0.0.255 any established	Established connections are allowed in the whole FTE community subnet The range of addresses in this FTE community is 10.0.0.2-255.
access-list 101 permit udp host 225.7.4.103 any access-list 101 permit udp any host 225.7.4.103	The DSA multicast address, 225.7.4.103 is allowed to pass in both directions.
access-list 101 permit ip 10.0.0.0 0.0.0.240 any access-list 101 permit ip any 10.0.0.0 0.0.0.240	The server range is 10.0.0.2-15.
access-list 101 permit udp any any eq domain	Access to a domain controller TCP port is allowed.
access-list 101 permit udp any any eq 88	Access to a Kerberos server is allowed
access-list 101 permit udp any any eq 389	Access to a LDAP server is allowed
access-list 101 permit IP any any eq IKE	Key exchange for secure communication
access-list 101 permit ESP any any	Secure communication use the Encapsulated Secure Payload protocol
There is an assumed “deny all” at the end of the list. This means that any other address range is denied access.	

Router interfaces connected to FTE communities MUST NOT have VLANs associated with them. The following is a typical interface configuration

interface FastEthernet0/3	This example has a connection to a 3560 interface in the third fastethernet port.
No switchport	This configuration statement will create a routed port for the FTE community
duplex full speed 100	The speed and duplex if the interface is fixed to avoid problems with autosensing.
ip address 10.0.0.1 255.255.255.0	The FTE community’s default gateway address is 10.0.0.1. The subnet mask of 255.255.255.0 will allow traffic in this range to pass to the ACL filters
ip access-group 101 out	Access-group 101 uses the ACLs described above in access-list 101
no ip proxy-arp	Proxy arp must be disallowed to avoid possible issues

16. Switch Configuration Files

Overview

After installation, a FTE Qualified switch pair must be configured for FTE using the switch's command line interface and the correct switch startup configuration file. Switch configuration files, which are copied to the hard drive when the FTE Driver package is installed, are used to configure the various switch and port options as listed in the table below. Additionally, the configuration files contain Quality of Service parameters that are attached to the ports. Updates to the configuration files between releases can be found at the On Line Service web site. The files can be found by going to www.honeywellprocess.com select the support tab, then select latest downloads. In the search box, enter FTE_switch_configuration. In the results select FTE Switch Configuration Files. This will begin the download of the latest files.

Note: R400 does not contain Hyperterminal for use in serial configuration of switches and download of configuration files. Experion R410 includes a version of Hyperterm for use on Experion nodes. Use of laptops for serial communications does not pose a security hazard as long as the node is not connected to the FTE network.

Experion switch and port options

For a current list of switches and the number of ports for each Honeywell part number refer to the Fault Tolerant Implementation and Overview Guide.
This document is available on the Honeywell Process web site and is available in the Experion PKS Documentation PDF set.

Configuration Order for Switch Ports

The chosen configuration file defines the switch options and how each switch port is configured. Uplink ports are configured first, FTE Bridge ports are configured second, and Full Duplex 100 Mbps ports are configured third. The following table summarizes the switch port configuration settings. Complete descriptions of the switch configuration files can be found in the FTE Overview and Implementation Guide found in the Experion Knowledge Base.

Care must be taken in the use of 10/100/1000 switch interfaces that are available on some switch types or through SFP modules. The speed and duplex of these connections are not set in the configuration files due to the variablity of connection requirements in projects. The speed for connection of a SFP to a 100 Mbps interface on another switch must be set to the required value of 100/full duplex to ensure that the two ends of the connection arrive at the proper speed/duplex and stay there. Failure to configure these parameters on both ends of the connection can lead to outages while the switches negotiate. These outages will come and go leading the user to believe the connection is working properly but later an outage or network slowing will occur.

Configuration Order	Port Type	Spanning Tree	Status	Duplex	Speed
1st	Uplink ports	Uplink Fast	Enable	Full	100 Mbps
2nd	FTE Bridge ports	Fast	Enable	Full	Auto
3rd	FTE	Fast	Enable	Full	100 Mbps

More Information

For more information on any of Honeywell's Products, Services, or Solutions, visit our website www.honeywell.com/ps, or contact your Honeywell account manager.

Automation & Control Solutions
Process Solutions
Honeywell
2500 W. Union Hills Dr.
Phoenix, AZ 85027
Tel: +1-602-313-6665 or 877-466-3993
www.honeywell.com/ps

WP-07-02-ENG
June 2008

Honeywell