Honeywell

Experion PKS

Server and Client Planning Guide

EPDOC-X128-en-431A
February 2015

Release 431

Document	Release	Issue	Date
EPDOC-X128-en-431A	431	0	February 2015

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Contents

About this guide

This guide contains high-level planning and design topics for Experion servers and clients, as well as for controllers other than Process Controllers.

Revision history

Revision	Date	Description
A	February 2015	Initial release of document.

Introduction

This guide contains high-level planning and design topics for Experion servers and clients, as well as for controllers other than Process Controllers.

Related documents

The following documents complement this guide. You should read them before you start detailed planning and design tasks.

Document	Description
Network and Security Planning Guide	Contains networking, security, and systems integration information applicable to Experion.
Control Hardware Planning Guide	Contains planning and design topics applicable to Process Controllers.
Overview	Provides a comprehensive overview of Experion, including basic concepts and terminology.
Software Change Notice (SCN)	Contains last-minute information that was not able to be included in the standard documents. It may include important details that could affect your planning or design decisions.

Enterprise models

The section provides an introduction to *enterprise models*. Enterprise models provide structure to support:

- Organizing your system.
- Structuring your view of alarms.
- Defining the scope of user views and control rights.

This section also includes guidelines for designing enterprise models, as well as examples that illustrate 'best practice' design principles.

Related topics

“About enterprise models” on page 12
“About asset models” on page 13
“About assignable assets and scope of responsibility” on page 14
“About system models” on page 15
“About network models” on page 16
“About generic displays” on page 17
“Guidelines for designing enterprise models” on page 18
“Guidelines for determining the optimal topology for your plant” on page 22
“Example enterprise models and topologies” on page 24
“Implementing an enterprise model” on page 26
“About point data in a DSA system” on page 29
“Installation and configuration tasks” on page 158
“Enterprise Model Builder” on page 160

About enterprise models

An enterprise model provides a means of organizing your system around key entities in your enterprise, such as plant equipment.

An enterprise model provides:

- A hierarchical structure that makes it easier for users to navigate their way through your system.
- A simple and intuitive means of implementing *scope of responsibility*—that is, systematically managing the access rights of operators (or Stations) to various parts of your system.
- The mechanism to enable and disable alarming for selected equipment.

An enterprise model is a framework that includes a set of specialized models, such as the asset and system models, each of which represents one aspect of your system.

About asset models

An *asset model* forms the core of an enterprise model: it is a hierarchical representation of your assets, similar to the one shown in the figure below.

An *asset* represents a particular physical item, such as a piece of plant equipment, a production line or a building.

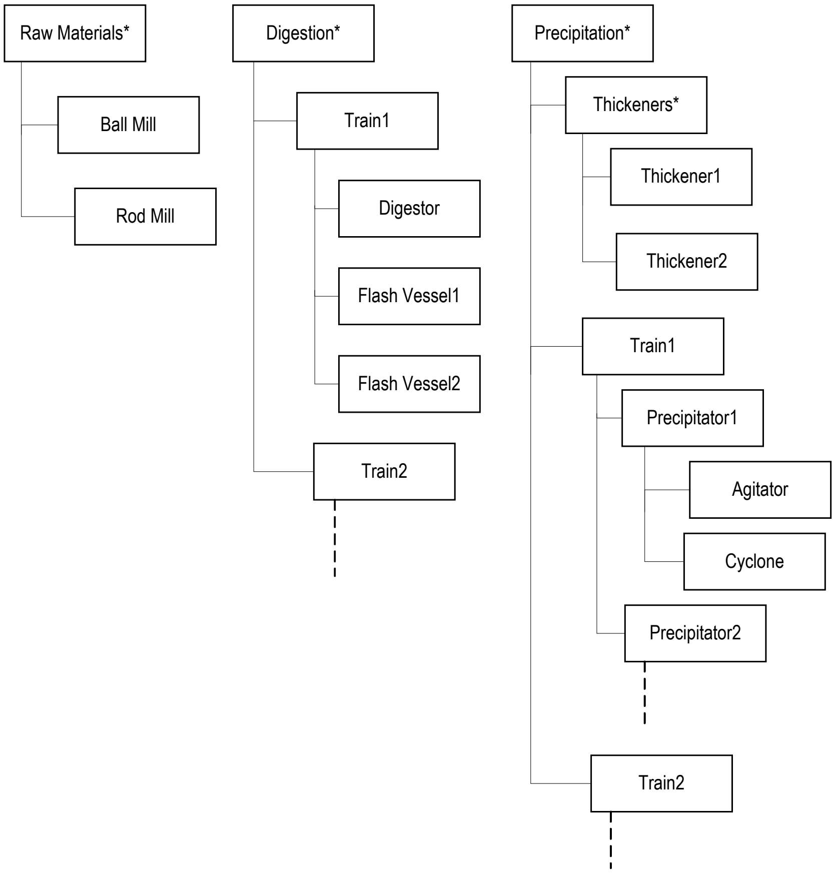


Figure 1: A typical asset model

Related topics

“Guidelines for designing asset models” on page 18

About assignable assets and scope of responsibility

An asset model is not just a logical representation of your physical assets and how they relate to each other. It also provides a framework for defining *scope of responsibility* (SOR)—that is, assigning specific assets to specific operators (or Stations).

An asset that you can assign to an operator (or Station) is called an *assignable asset*. By default, all top level assets in your asset model are assignable assets. If appropriate, you can also define assets at other levels as assignable assets.

When you give an operator (or Station) access to an assignable asset, you also give access to its child assets (except those which have been defined as assignable assets).

If an asset is changed from *non-assignable* to *assignable*, any scope of responsibility that was previously inherited is cleared. As a result, control of this asset is temporarily lost until the asset is included in the operator's or Station's scope of responsibility.

By assigning assets to operators, you not only restrict what assets they can control, you also restrict what they see. For example, if an operator calls up the Alarm Summary it will only display alarms related to assets that have been assigned to that operator. The associated asset on system components can also be used to control which system alarms are displayed to operators, based on their SOR.

Attention

Scope of responsibility does not apply to point data on custom displays. If you want to limit the visibility and use of point data on custom displays, you should assign an appropriate security level to the point or the display during configuration of the custom display.

Related topics

"Guidelines for designing asset models" on page 18

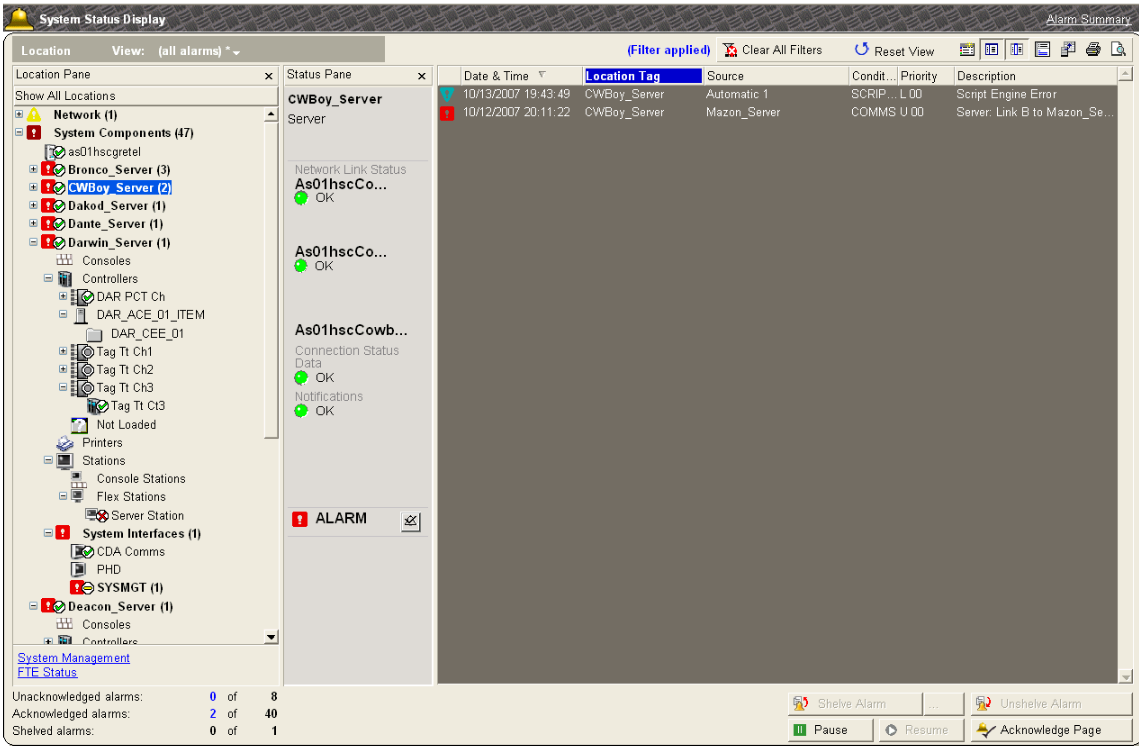
"Custom displays" on page 122

About system models

A *system model* represents the Experion-related aspects of your system, namely:

- Experion server(s).
- Stations, channels, controllers, system interfaces and printers that are associated with those servers.
- If appropriate, servers that are connected to, but not part of, your Experion system (for example, servers on your business network).

After you have configured your system and all its components, you can see a graphical representation of your system model in the System Status display.



	Date & Time	Location Tag	Source	Condit...	Priority	Description
	10/13/2007 19:43:49	CWBoy_Server	Automatic 1	SCRIP...	L 00	Script Engine Error
!	10/12/2007 20:11:22	CWBoy_Server	Mazon_Server	COMMS	U 00	Server: Link B to Mazon_Se...

Unacknowledged alarms:	0	of	8
Acknowledged alarms:	2	of	40
Shelved alarms:	0	of	1

Figure 2: A typical system model, as shown in the System Status display

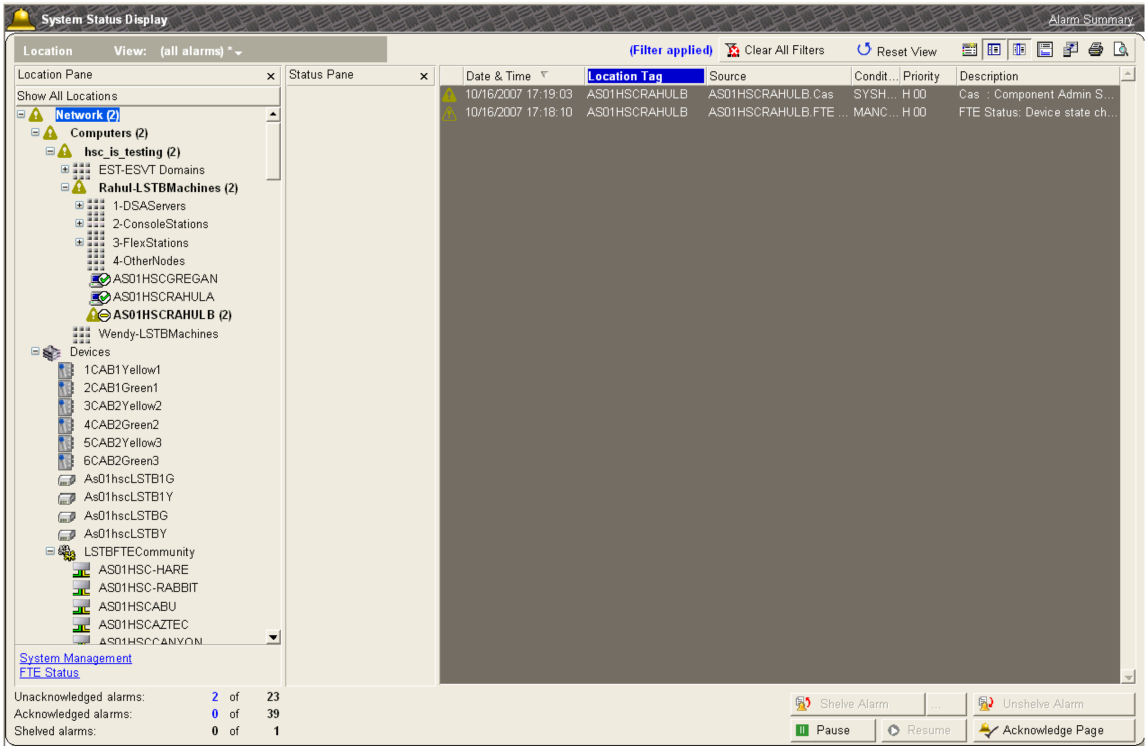
About network models

A *network model* (also called a *network tree*) is a graphical representation of the nodes in your network, which can include the following:

- Computers that host applications such as Experion server, Station or Application Control Environment (ACE).
- Collections of computers such as workgroups, domains, and Organizational Units.
- Devices such as switches and routers.
- Collections of devices and computers, called *FTE communities*.

A network tree enables you to view the status and events related to your computers and network equipment in the System Status display.

To learn more about designing a network that meets your networking and security requirements, see the *Network and Security Planning Guide*.



Date & Time	Location Tag	Source	Condit...	Priority	Description
10/16/2007 17:19:03	AS01HSCRAHULB	AS01HSCRAHULB.Cas	SYSH...	H 00	Cas : Component Admin S...
10/16/2007 17:18:10	AS01HSCRAHULB	AS01HSCRAHULB.FTE ...	MANC...	H 00	FTE Status: Device state ch...

Unacknowledged alarms:	2	of	23
Acknowledged alarms:	0	of	39
Shelved alarms:	0	of	1

Figure 3: A typical network model

About generic displays

If you have many identical assets, such as a series of holding tanks, you can use one *generic display* to show information about each tank. (Generic displays work in a similar manner to point detail displays—that is, when you call up a generic display, you need to specify the asset whose details you want to view.) For information on generic displays, see the *HMIWeb Display Building Guide*.

Note that, in order to make use of generic displays, you must develop a systematic naming convention.

For example, you might have the following asset model:

```
\assets\precipitation\train1\precipitator1
\assets\precipitation\train1\precipitator2
```

Each precipitator might have 2 points (whose tag names are *VLV001* and *VLV002* respectively). For a generic display, you would use the same item name for the points (for example, *Valve*):

```
\assets\precipitation\train1\precipitator1\Valve
\assets\precipitation\train1\precipitator2\Valve
```

You can then create a generic display that references *Valve*.

- When you call up the generic display by referencing *assets\precipitation\train1\precipitator1*, you will see data for *VLV001*.
- When you call up the generic display by referencing *assets\precipitation\train1\precipitator2*, you will see data for *VLV002*.

Guidelines for designing enterprise models

The following topics contain guidelines for designing enterprise models.

Related topics

"Guidelines for designing asset models" on page 18
"Guidelines for defining scope of responsibility" on page 19
"Naming rules for assets" on page 20

Guidelines for designing asset models

This topic provides guidelines for designing an asset model.

Ensure that your asset model reflects reality

Ensure that your asset model reflects the logical and physical design or structure of your plant. For example, if your site consists of two distinct plants (say, Plant North and Plant South), each with their own control room, then you would define *Plant North* and *Plant South* as your top-level assets.

Keep your asset model as simple as possible

Keep your asset model as simple as possible, and with as few levels as possible. In particular:

- Only define an item as an asset if you want to be able to use it for filtering or navigational purposes.

  For example, define as assets any items that you want to include in Location Pane of the Alarm Summary, so that users can easily navigate (or filter) alarms. Similarly, define as assets any items that will help users navigate (or filter) report data.
- Use as few levels as possible—avoid using more than five.

  Although you can have up to 10 levels, the deeper and more complicated your model, the more cumbersome and therefore less useful, your model will be—in terms of both operation and maintenance.

Bear in mind the following constraints

- An asset model cannot include more than the maximum number of assets, which is documented in the *Experion Specification*.
- Assets (like points) constitute 'tags' in an Experion system, and therefore count towards the total number of tags (or points) on a server. Note, however, that assets do not count towards the server's *licensed* point count.

Details of a server's point counts are available on the Server License Details display (see the topic titled "Checking your Experion license" in the "Configuration overview" section of the *Server and Client Configuration Guide*).

Develop a systematic and user-friendly naming convention for your assets

You need to develop a systematic and user-friendly naming convention, which complies with the naming rules for assets. A well-designed naming convention makes it much easier for operators to navigate their way through your system, and to respond to alarms.

A systematic naming convention is also essential if you want to make use of generic displays—for example, use the same display for every holding tank in your plant.

Define appropriate assets as assignable assets

An assignable asset is one that can be assigned to an operator or Station for the purposes of scope of responsibility.

As a general rule, we recommend that you restrict assignable assets to the two top levels of your asset model. (By default, assets at the top level are assignable.)

If you make a lower level asset assignable, you should, for the sake of simplicity, also make all its ancestors assignable. Otherwise, it may be harder to understand the behavior of the assignment displays.

An asset model must not include more than the maximum number of assignable assets, which is documented in the *Experion Specification*.

You should only change an asset from assignable to non-assignable (or from non-assignable to assignable) before you engineer your data points. If you make such a change after you have engineered your data points, you will need to reconfigure your scope of responsibility displays.

Related topics

"About asset models" on page 13

"About assignable assets and scope of responsibility" on page 14

"Example enterprise models and topologies" on page 24

"About point data in a DSA system" on page 29

Guidelines for defining scope of responsibility

It is essential that you define scope of responsibility (SOR) so that operators can access those parts of the system for which they are responsible.

Experion system security comprises both:

- Windows operating system security
- Station security: Station-based or operator-based

System security enables you to control who has access to the system and to control what users can do within the system when access is granted.

> **!** **Attention**
> Logging on to Windows does not necessarily grant permission for access to an Experion application, such as Station. You therefore need to configure user access to Experion separately to configuring Windows user accounts.

When configuring security for your site you need to consider:

- What type of Station security you want to use.

  Do you want to use Station-based or operator-based security?
- What access operators require within Experion.

  You may want to restrict operators from controlling certain parts of the system.
- If you choose operator-based Station security, what type of operator accounts do you want to use:
  - Traditional operator accounts
  - Integrated accounts using either domain Windows accounts or local Windows accounts
  - Windows group accounts using either domain Windows groups or local Windows groups
- Whether you want to use Signon Manager.

  If Signon Manager is to be used, you need to choose operator-based security with integrated accounts.
- How you implement Windows security.
- What type of Windows accounts you require.

Profiles

You define Scope of Responsibility (SOR) by creating *profiles*. A profile can be assigned to an `oper` account, which is related either to an individual Windows account or a Windows group account.

Profiles provide a convenient means of managing operator access rights. A profile specifies:

- The assets that can be accessed.
- The times during which those assets can be accessed.

By defining an appropriate set of profiles to each operator, you can manage operator access in a systematic manner.

For more information about configuring scope of responsibility, see the topic "Configuring system security" in the *Server and Client Configuration Guide*.

Naming rules for assets

Each asset has three names:

- A *tag name* (also called a *point ID* or *point name*). A unique name, which is used by the system to identify the asset. The tag name must be unique across the DSA system.
- An *item name*. A descriptive (user friendly) name for the asset. Unlike the point name, the item name only has to be unique with respect to its siblings (other items that share the same parent item).

  For example, you can give many assets the item name of 'Mainvalve' provided each asset has a different parent.
- A *full item name* (also called an *enterprise model name*). A unique name, which consists of the tag name and the names of all its ancestors within the asset model.

  A full item name has the same structure as the full path name of a file on a network. The following example is the full item name of an asset named ‘Agitator’:

  ```
  /Assets/Precipitation/Train1/Precipitator1/Agitator
  ```

Asset names must follow certain naming rules:

- Tag names must be unique.
- Tag names and item names can contain up to 40 single-byte or 20 double-byte alphanumeric characters, with at least one alpha character.
- Tag names and item names are not case-sensitive: *`Cooling Tower1`* and *`cooling tower1`* represent the same asset.
- The first character of a tag name and an item must not be any of the following characters:
  - At sign (@)
  - Dollar sign ($)
  - Space
- Tag names and item names cannot contain any of the following characters:
  - Asterisk (*)
  - Backslash (\)
  - Braces { } (rule applies to item names only)
  - Brackets [ ]
  - Caret (^)
  - Colon (:)
  - Comma (,)
  - Double quote (")
  - Equals (=)
  - Forward slash (/)
  - Greater than (>)
  - Less than (<)
  - Parentheses ( )

  - Period (.)
  - Question mark (?)
  - Semi colon (;)
  - Single quote (')
  - Space (rule applies to tag names only)
  - Tabs
  - Vertical bar (|)
- The last character of a tag name and an item must not be a space.
- A *full item name*:
  - Must not be longer than 200 characters
  - Must be unique

Guidelines for determining the optimal topology for your plant

This section provides guidelines for determining the optimal topology for your plant.

Keep your topology as simple as possible

As a general rule, we strongly recommend that you keep your topology as simple as possible—the more complicated your topology, the harder it will be to efficiently engineer, maintain and operate your plant.

Obviously, the simplest topology is a single-system topology that contains every server (and clusters of servers) in your plant.

Determine you security and business needs

When choosing your topology, you also have to take into account your security and business needs. For example, if your system also includes level 3 and level 4 applications, or a firewall, the optimal topology will be significantly different from a system that does not include such items.

For more information, see the *Network and Security Planning Guide*.

Reasons for choosing a multi-system topology

Although, a single-system topology is generally the preferred topology, there are several reasons why a multi-system topology may appropriate.

Ease of engineering

A multi-system topology may be appropriate if you have separate teams working on different clusters, or if you are commissioning separate parts of your plant at different times.

A multi-system topology will also minimize the impact of any engineering errors—for example, if you accidently delete an asset, only the system you are working on will be affected.

Note, however, if the systems share significant numbers of assets, you need to consider the extra work required to keep the systems synchronized. (In some sites, they have edited their asset models on a weekly or daily basis to maintain this synchronization.)

Multiple domains

A multi-system topology may be appropriate if your plant spans multiple domains—that is, not all servers or clusters belong to the same domain.

For example, if a server or cluster is in another domain, the security policy may prevent you from being able to directly configure the server/cluster, or download the enterprise model. Also, it may be difficult to control access to Station or Configuration Studio.

If you want a single-system topology that spans multiple domains, you must ensure that:

- The password for your Windows *mngr* account is the same for all nodes in the system.
- If you use integrated accounts (combined Windows account and operator ID), every account that has *ENGR* security level is recognized in every domain.

Firewall between network levels

If you need to communicate between network levels—for example, between level 2/3 and level 4, or between level 2 and level 3—and you have a firewall between these levels, you have several options:

- Open the firewall to the extent that it allows downloads from the EMDB to all relevant clusters.

  Note that your network security policies may not allow this solution.
- 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 multi-system topology, with at least one system for the lower levels and one system for the higher levels.

  The disadvantage of this approach is that you will need to manually keep your enterprise models sufficiently synchronized to allow the sharing of assets, point data and alarms.

Plants with different releases of Experion

A multi-system topology may be appropriate if different parts of your plant use different releases of Experion. For example, you want to expand you plant, but do not want to upgrade Experion on the existing plant (at least until you have fully commissioned your new equipment).

Large or complex plants

A multi-system topology may be appropriate if your plant is complex or very large, or if large parts of the model are not relevant to particular clusters.

By dividing your plant into several systems, you can simplify both engineering and operational tasks for each system.

Determining the appropriate location for the Enterprise Model Database (EMDB)

The Enterprise Model Database (EMDB) is the database that defines your system.

When you install Experion PKS on a server node, the EMDB is installed by default but you can choose whether you want the EMDB activated on that node.

When deciding on the location of your EMDB bear in mind the following:

- You only need one server (or redundant pair of servers) in your system (or DSA nodes) to host the EMDB. The EMDB is downloaded to all the servers in your system when you have finished engineering it.
- You can have multiple systems. For each EMDB, you need to add the servers from the other system(s) that you need to access. It is important to mark those servers as “external” to your system so that you do not accidentally download your Enterprise Model to those servers that need to use the Enterprise Model from their own system.
- You can also decided to host the EMDB on a single server node or a redundant pair that is not running on process. For example, you could have the EMDB on level 3 of your system. For more information about the levels in an Experion system, see the “Network Security” section in the *Network and Security Planning Guide*.

Tip

Note that once you have activated the EMDB on a server node, you can deactivate it using a post-installation tool. For details see “Managing the activation of an Enterprise Model database” in the *Supplementary Installation Tasks Guide*.

Example enterprise models and topologies

The following topics contain example models and topologies that illustrate 'best practice' design principles.

Related topics

“Guidelines for designing asset models” on page 18

An asset model for a simple system

Scenario

Your plant includes milling, digestion and precipitation processes.

You want an asset model that accurately represents the three processes, identifies the main plant items, and allows you to assign operators to specific processes.

In the case of the precipitation process, which requires more operator skill, you want to be able to separately assign the thickener equipment to specific operators.

Solution

You design the asset model shown in the following figure.

An asterisk next to an asset indicates that it is assignable. Because *Raw Materials*, *Digestion* and *Precipitation* are top level assets, they are assignable by default. Because, you want to be able to assign the thickeners to specific operators, you also make *Thickeners* assignable.

With this design, you can assign either or both *Precipitation* and *Thickeners* to operators, as appropriate. For example, if you only assign *Precipitation* to an operator, that operator will have access to all assets below it, except for the *Thickeners* branch.

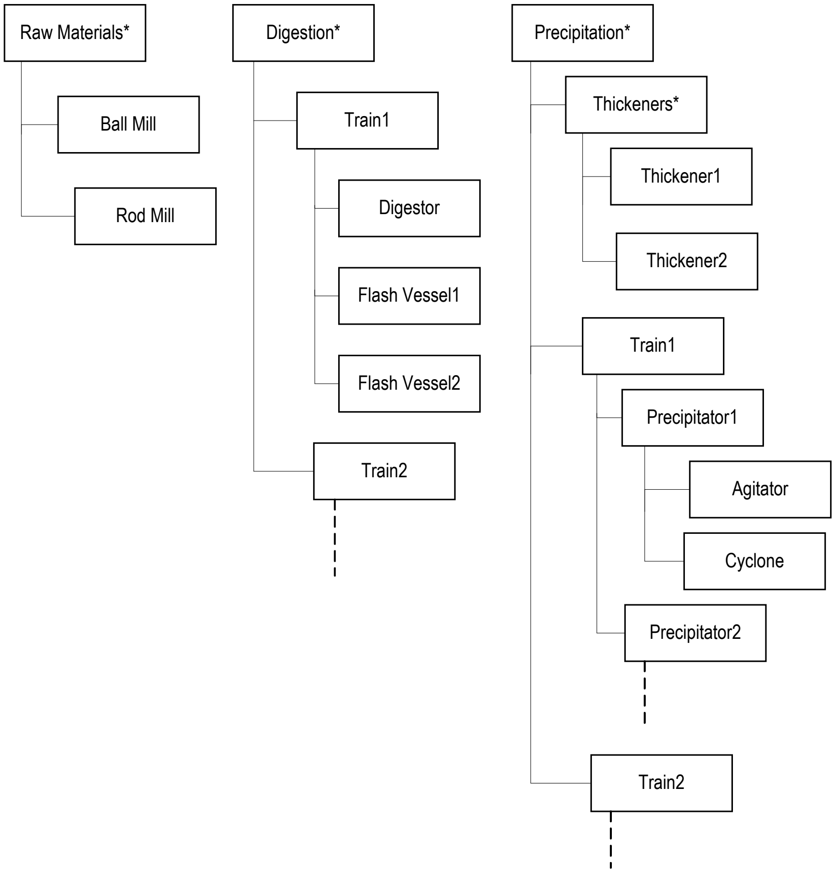


Figure 4: The asset model for a simple system

Implementing an enterprise model

The following table summarizes the major steps involved in implementing an enterprise model.

Task	Done
Familiarize yourself with the concepts, guidelines and examples included in this section. In the case of networking and security, you also need to read the *Network and Security Planning Guide*.	
Define your system name using Enterprise Model Builder. See the *Enterprise Model Builder User's Guide*.	
Define your servers using Enterprise Model Builder. See the *Enterprise Model Builder User's Guide*.	
Define your asset model using Enterprise Model Builder. See the *Enterprise Model Builder User's Guide*.	
Define your points, Stations, channels, controllers and printers using the appropriate tool (Quick Builder or Control Builder). When building each point, ensure that you specify the parent asset. See the *Quick Builder Guide* or *Control Building Guide*.	
Build your network model. See the “The Network tree” section of the *Server and Client Configuration Guide*.	
If you use Station-based security, assign assets to Stations. See the “Configuring system security” section of the *Server and Client Configuration Guide*.	
If you use operator-based security, define profiles, and then assign profiles to operators. See the “Configuring profiles for scope of responsibility” topic in the “Configuring system security” section of the *Server and Client Configuration Guide*.	
Assign assets to reports. See the “Reports” section of the *Server and Client Configuration Guide*.	
If appropriate, define alarm groups using Enterprise Model Builder. See the *Enterprise Model Builder User's Guide*.	
If appropriate, create generic displays. See the “About generic displays” topic in the “About display types” section of the *HMIWeb Display Building Guide*.	

Servers

This section describes how to determine your server requirements.

Issue	Comments
Redundancy	Decide whether you need server redundancy.
Distributed system	Decide whether you need a distributed system.
eServer	Decide whether you want an *eServer*, which gives casual users read-only access to displays and reports.
PHD	Decide whether you want an integrated PHD server, and whether you want PHD to store long-term history.
Remote Engineering and Station Server	Decide whether you want a Remote Engineering and Station Server, which enables remote devices to access Station and Experion configuration tools.
Server scripts	Decide whether you can use *server scripts* to perform specialized tasks.
Server names	Define the server name(s).
Servers and the Enterprise Model Database (EMDB)	Decide which server will be used to store your system's EMDB.
ESM Server	Decide which server will host the ESM Server, which is required for ESM tools, such as Installation Builder and Diagnostic Studio.
Defining and maintaining installation and network settings for your server(s)	When you have decided on the kind of servers you need, you can use Installation Builder to gather and deploy computer and network configuration information for those servers. The data collected by Installation Builder can be used to perform installation and pre-configuration tasks such as automating the software installation process or maintenance tasks such as changing DNS settings. See the *Installation Builder Users Guide*.

Related topics

“Server redundancy” on page 28

“Distributed System Architecture” on page 29

“eServer” on page 31

“PHD” on page 32

“Remote Engineering and Station Server” on page 33

“Server scripts” on page 34

“Naming rules for computers” on page 35

“Servers and the Enterprise Model Database” on page 36

“ESM Server” on page 37

Server redundancy

You can improve system availability with server redundancy.

In a redundant server system, Experion is installed on both servers, which are identically configured and connected through a LAN.

Database synchronization, which is achieved through the LAN, requires a significant bandwidth. Consequently, you should isolate the servers from heavily-loaded parts of the LAN and protect them from unusual loads.

Experion uses *software arbitration* to determine which server acts as primary. With software arbitration, each server polls the other through the LAN to determine whether the other server has failed.

Attention

Not all Experion components use the arbitration approach. The Enterprise Model Database (EMDB) and Engineering Repository Database (ERDB) are located on the Preferred Secondary Experion server (server B). If this Preferred Secondary Experion server is not available, the system is considered in a degraded state and no changes are allowed to be made to either database.

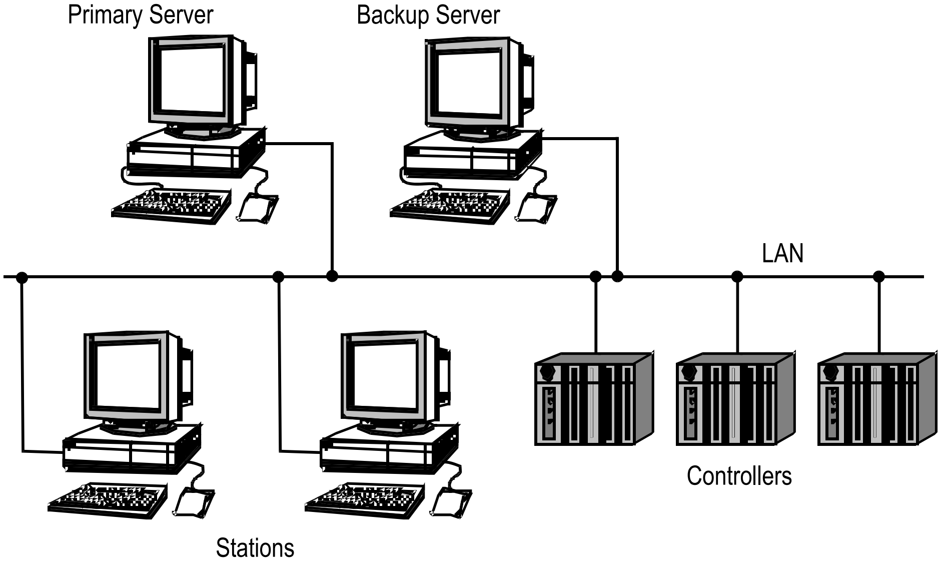


Figure 5: Typical redundant server system

Distributed System Architecture

Distributed System Architecture (DSA) is an option that enables multiple Experion server systems to share data, alarms, alerts, messages, events, and history without the need for duplicate configuration on any server.

DSA is appropriate for:

- Large-scale plant-wide systems in which the servers are connected through a high-speed LAN
- Geographically-distributed systems in which the servers are connected through a WAN (DSA has been designed to minimize network traffic, and supports WANs with speeds as low as 64 Kbps.)

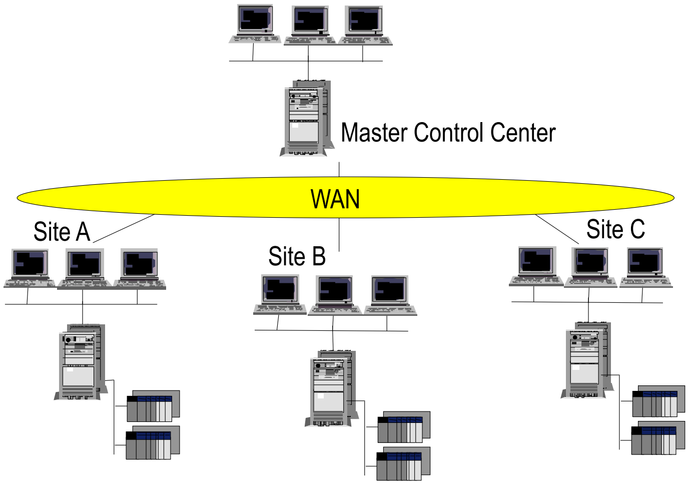


Figure 6: Typical geographically distributed system

For more information about DSA, see 'Configuring Distributed System Architecture' in the *Server and Client Configuration Guide*.

Related topics

“Point IDs and Distributed System Architecture (DSA)” on page 77

Inter-release support

DSA interoperability works between the current release and previous releases of Experion. For example, you can have a DSA system in which some servers are running the current release while others are running the previous (or an even earlier) release of Experion.

Please consult the *Experion PKS Software Change Notice* for specific details about which releases are supported.

DSA and firewalls

If there is a firewall in your DSA system other than the default Windows Firewall, you will need to ensure that the necessary ports are opened in the firewall to enable DSA communications between the DSA client and server nodes.

For information on DSA communication through a firewall and Windows security enhancements, see the *Network and Security Planning Guide*.

About point data in a DSA system

DSA provides global access to point parameter data on all servers in the system. Each server provides automatic dynamic caching of remote data for all of its clients, so that clients access their local server for all data. In general, clients do not access remote servers directly. However, some process data is accessed directly; for example, chart visualization via a Process Detail display.

DSA data access works as follows:

1. When one of its clients requests data for a point that is not already in the local server's database, the local server asks the servers in the system for the data owner of the point.
2. When the data owner is determined, the local server subscribes to the remote server from which it obtained the data and automatically creates a cache reference (known as a 'local cache point') in the local database.
3. While the subscription is in effect the data owner uses 'report by exception', only sending data to the caching server when there is a change. When the data is no longer referenced by any of its client Stations or applications, the subscribing server cancels the subscription to the data owner. This subscription mechanism ensures maximum efficiency both on the servers and over the network.

How DSA affects your total point count

The cached points created by DSA do not count against the licensed point count for a given server. They do, however, count towards the total maximum number of points per server.

Note that you can reduce the number of DSA points on a server by disabling DSA subscription to the system model and system alarms on a remote server. This setting is useful if you are approaching the maximum number of points on a server in a DSA system. For more information, see 'Configuring servers to subscribe to data and alarms' in the 'Configuring Distributed System Architecture' topic in the *Server and Client Configuration Guide*.

You can check the current number of DSA points (and other types of unlicensed points) on the Server License Details display. See 'Checking your Experion license' in the 'Configuration overview' topic in the *Server and Client Configuration Guide*.

DSA-specific rules and restrictions

The following rules apply where you have DSA-connected servers:

- Every point that will be accessed from more than one server must be assigned to an asset.
- When creating a new point, it can have the same tag name (point ID) as a point on another server, but it cannot have the same tag name as a point on the same server, or the same tag name as any existing asset or alarm group within your Enterprise Model.

  When creating a new asset or alarm group, it cannot have the same tag name as any existing asset or alarm group within the same system connected via DSA, or the same tag name as any existing points on any of the servers connected via DSA.

  So, for example, you can have the tag name `FIC123` on `ServerNorth` as well as on `ServerSouth` because Experion will identify the first as `ExperionServerNorth:FIC123` and the other as `ExperionServerSouth:FIC123`, thus making each tag name unique within the system. You cannot, however, have an asset or alarm group called `FIC123` because assets and alarm groups are downloaded to every server in the system, and downloading an asset with the tag name `FIC123` would conflict with the existing `FIC123` points on `ServerNorth` and `ServerSouth`.
- System tables (such as the message, acronym, and reason tables) that reference an item by number must be identical on every server.

Related topics

"Guidelines for designing asset models" on page 18

"eServer" on page 31

"Enterprise models" on page 11

"Points" on page 75

eServer

An eServer is a special Experion server that gives casual users read-only access to displays and reports using a browser such as Microsoft Internet Explorer.

An eServer also simplifies administration because it consolidates the management, security and licensing of casual user accounts.

An eServer provides two levels of access:

- Premium.

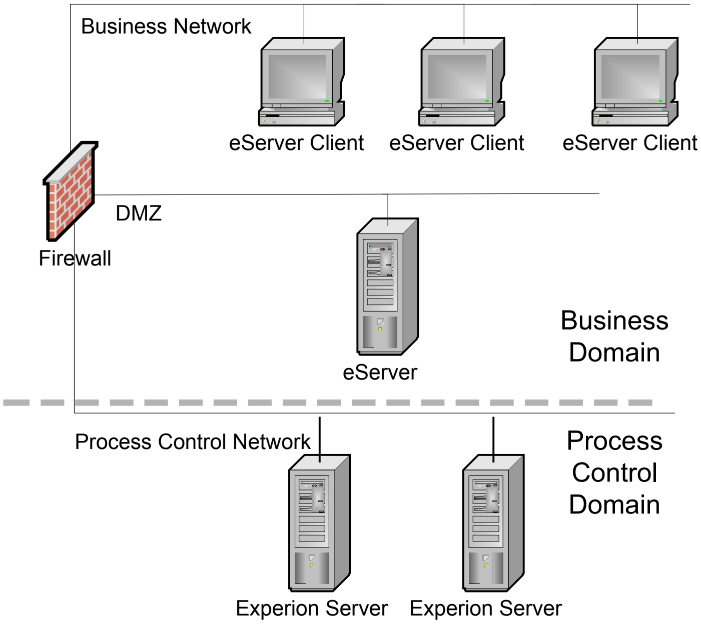
  Provides access to displays that are updated in the normal manner.

- Standard.

  Provides 'snapshots' of displays that are not updated. (To check for changes to data, the user must request a new snapshot by using the browser's refresh function.)

An eServer license allows an unlimited number of standard access connections. Premium access connections are purchased separately.

The eServer software must be loaded on a separate computer, not on one of the Experion servers in your process control network.



From a networking point of view, an eServer is a separate server in a DSA system, and requires a DSA license for each server that it subscribes to.

For more information about eServers, see 'Configuring eServer' in the *Server and Client Configuration Guide*.

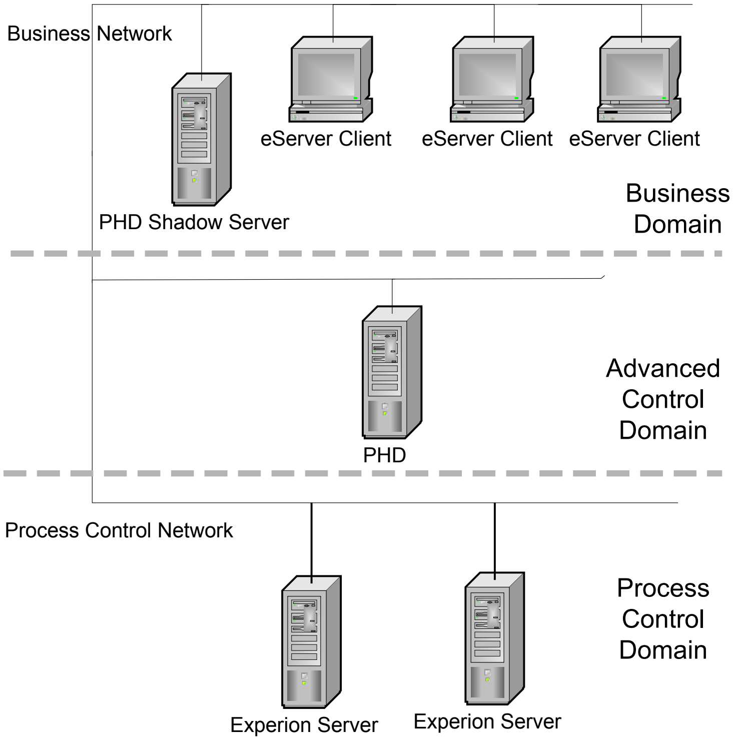
For information about the security aspects of eServer, see the *Network and Security Planning Guide*.

Related topics

"About point data in a DSA system" on page 29
"Stations" on page 53
"Displays" on page 119
"Mobility" on page 60
"Remote Engineering and Station Server" on page 33

PHD

Process Historian Database (PHD) collects, stores, and replays continuous and other historical plant data. While PHD resides on a separate node from Experion servers, they can interact, enabling PHD to store long-term history data. PHD provides a more compact storage mechanism.



Short-term history collection

When PHD is used, Experion should be configured to store around ten to thirty days of history—depending on your business requirements. History beyond this time window can be stored using PHD.

Long-term history collection

When long-term history collection is migrated to PHD, your analytical applications must draw their data from PHD rather than Experion. Ensure that all key applications can effectively use PHD history data sources prior to discarding the history in Experion.

Remote Engineering and Station Server

A Remote Engineering and Station Server is a computer that supports remote or mobile access to Station and to the Experion configuration tool, Configuration Studio.

You can set up a Remote Engineering and Station Server to enable remote access to either eServer Premium displays (Mobile Access for eServer Premium) or to full Station functionality (Mobile Access for Station).

Planning considerations

In planning for the number of Remote Engineering and Station Server nodes that you might need for your site, you should bear in mind the following:

- A Remote Engineering and Station Server can be configured to support either Mobile Access for eServer Premium or Mobile Access for Station (but not both). That is, you need to set up separate Remote Engineering and Station Servers for each type of access.

  A Remote Engineering and Station Server that provides Mobile Access for Station can, however, also be used to provide remote access to Configuration Studio.
- The maximum number of concurrent remote access sessions that a Remote Engineering and Station Server supports is 5.

Attention

- Within this maximum number of 5 concurrent sessions you can have a maximum of 5 concurrent connections to Station or 4 concurrent connections to Configuration Studio (or a mix of both types of connections provided that you do not exceed the individual limits for each type of connection). Note, however, that you cannot run both Station and Configuration Studio within the one session.
- Although you can run 4 concurrent connections to Configuration Studio, only one of those connections can run the Quick Builder component of Configuration Studio at any one time.
- Because access to Station is provided within Configuration Studio as one of the configuration tools, a remote device connecting to Configuration Studio does not need a separate connection to Station.

For information on installing and configuring a Remote Engineering and Station Server, see 'Installing Remote Engineering and Station Server' in the *Supplementary Installation Tasks Guide* and 'Configuring Remote Engineering and Station Server' in the *Server and Client Configuration Guide*.

Related topics

“eServer” on page 31

“Mobility” on page 60

Server scripts

You can add extra functionality to your system with *server scripts*. A server script runs when its associated event occurs—for example, when:

- A point changes state
- An operator acknowledges an alarm
- The server starts
- A report is generated

Server scripts can also include:

- *Periodic* scripts, which run at specified intervals while the server is running
- *Library* scripts, which perform specialized functions when called by other server scripts

Server scripts don't block point processing, and don't impact other server functions because they run at a low priority.

Note that server scripting has been optimized for relatively short scripts (less than 30 lines), and is not designed for implementing control strategies (which should be done in the controller). If a task is computationally intensive, or requires extensive file handling, you should write a custom application in Visual C/C++ or Visual Basic.

For more information about server scripts, see the *Server Scripting Reference*.

Related topics

"Points" on page 75

Naming rules for computers

Every Experion node (for example, Experion server, Console Station, and Flex Station computers) must have a unique name and IP address. The unique name must comply with the following rules:

- The length of the node name must comply with the table below.
- The name must begin with an alphabetic character, such as a to z, or A to Z.
- The name must not contain spaces or other non-standard characters.
- The names of redundant server pairs consist of a common ‘base name’ (which must follow the other naming restrictions), plus an ‘A’ suffix for the primary server and a ‘B’ suffix for the backup server.

  For example, if the base name of the redundant servers is HSSERV:

  – The name of the primary server is HSSERVA.

  – The name of the backup server name is HSSERVB.
- The node name must not end with ‘A’ or ‘B’. (The use of A and B as the last letter in a name is reserved for naming redundant servers.)
- To avoid potential confusion, the node name should not end with a ‘0’ or ‘1’, as these numbers are used in `hosts` files to identify redundant links.

Table 1: Length of node name for FTE networks

Node type	FTE
Flex Station, Console Station, Console Extension Station, Collaboration Station	15 characters Example: *HSCSTN01*
Redundant Experion server	14 characters[1] Example: *HSCSVR01A*
Non-redundant Experion server	15 characters Example: *HSCSVR01*

Table 2: Length of node name for Dual Ethernet networks

Node type	Dual Ethernet
Flex Station, Console Station, Console Extension Station, Collaboration Station	14 characters[2] Example: *HSCSTN010*
Redundant Experion server	13 characters[3] Example: *HSCSVR01A0*
Non-redundant Experion server	14 characters[4] Example: *HSCSVR010*

[1] The last character is reserved for A/B redundant server suffix.

[2] The last character is reserved for 0/1 redundant link suffix.

[3] The last two characters ares reserved for A/B redundant server suffix and the 0/1 redundant link suffix.

[4] The last character is reserved for 0/1 redundant link suffix.

Servers and the Enterprise Model Database

The Experion Enterprise Model Database (EMDB) comprises the engineering definitions of your system components, assets, and alarm groups.

EMDBs are created as part of an Experion installation procedure, which requires that you identify the node(s) on which you want to install the EMDB. You therefore need to consider the following questions before installing Experion:

- On which server (or redundant server pair) should the EMDB reside?
- Do you require more than one EMDB per system?

Attention

- If you choose to install the EMDB on a redundant server pair, you must install the EMDB on both server A and server B.
- Although it is possible to have multiple EMDBs, it is recommended that you only have one EMDB in an Experion system.

ESM Server

The ESM server maintains the node configuration details that are used by the Installation Builder and Diagnostic Studio.

You can have only one ESM Server in a system, and the ESM Server must be located on a server-grade computer. During the installation of Experion nodes, you can choose to install the ESM Server on an Experion node, or you can install an ESM Server on a non-Experion node from the ESM application media.

Networks

This section provides high-level information on networking issues.

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

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

Network planning considerations

In planning your Experion network, your considerations should include the following issues.

Issue	Comments
Domains or workgroups	Select the most appropriate structure. For more information, see the *Network and Security Planning Guide*.
Network topologies	Select the most appropriate network topology. For more information, see the *Network and Security Planning Guide*.
Network security	Determine your network security requirements. For more information, see the *Network and Security Planning Guide*.
Experion security features	Determine your Experion security requirements and decide what type of security you need to implement. For more information, see the *Network and Security Planning Guide*.
Network redundancy	Decide whether you need redundant networks.
Process Controllers	Determine the networking requirements of your Process Controllers.
Controllers other than Process Controllers	If you have controllers other than Process Controllers, determine how you are going to connect them to the network.
TPS	If you have a TPS system, decide whether you want to integrate it with Experion. For more information, see the *Integrated Experion-TPS User's Guide*.

Related topics

"Network redundancy" on page 40

"Process Controllers" on page 41

"Integrating TPS systems" on page 153

Network redundancy

You can improve system availability with network redundancy.

Network redundancy is appropriate where increased availability of the network is desired. (Ideally, the redundant links should be physically separated.)

Fault Tolerant Ethernet (FTE)

Honeywell's Fault Tolerant Ethernet (FTE) provides redundancy and a highly available networking scheme using commercial network interface cards (NIC) and standard Ethernet hardware (switches).

For more information about FTE, see the *Fault Tolerant Ethernet Overview and Implementation Guide*.

Process Controllers

Experion supports supervisory level communications over Honeywell's Fault Tolerant Ethernet (FTE) network. It also supports supervisory level communications over a ControlNet network or Ethernet network using a ControlNet Interface (CNI) module or Ethernet module, respectively.

There are two different types of supervisory communication:

- At level 3 there is the supervisory communication between the server and client.
- At level 2 there is the downstream supervisory connection to the controllers on the Experion Process Network (EPN).

Attention

You cannot mix the supervisory network types on an Experion Process Network (EPN). For example, if your server is currently using a ControlNet supervisory network to communicate with Level 2, you cannot add a Fault Tolerant Ethernet (FTE) supervisory network to the server for simultaneous communication with different controllers.

You can connect Process Controllers to the server using Ethernet or ControlNet, using single or redundant links.

For more information about the networking options for Process Controllers, see the *Control Hardware Planning Guide*.

For more information about the networking security, see the “Network security” chapter of the *Network and Security Planning Guide*.

Time synchronization

The following topics are important for understanding and planning the time synchronization requirements of your Experion PKS system.

Related topics

“Experion time requirements” on page 44
“About time protocols” on page 47
“Planning your time hierarchy” on page 49
“Planning considerations for time synchronization” on page 51

Experion time requirements

Reliable and coordinated time is an important element in an Experion system. It is used in many aspects of the system including:

- control functions
- redundancy options
- intersystem communications of supervisory systems

Supported time protocols

When deploying a topology, the time protocols supported should be considered.

Device	CDA client	SNTP client	NTP client	PTP client[5]	CDA server	SNTP server	NTP server	PTP server
C300	X	X		X				
Series C FIM4 and FIM8	X	X		X				
PGM	X	X		X				
Safety Manager			X	X				X[6]
Wireless Device Manager			X				X[7]	
IEC 61850 Interface Module	X	X		X				
PMD		X	X					
C200	X							
RTU[8]		X						
CISCO switches		X	X					
Moxa switch (IEC 61850 compliant)		X	X	X			X[9]	X[9]
Rugged com switch (IEC compliant)		X	X	X			X[9]	X[9]
Windows client			X				X	
Windows server[10]			X		X[11]		X	
Windows domain controller			X				X	

[5] **PTP IEEE-1588 version 1 and PTP IEEE-1588 version 2 are supported for Safety Manager devices. For all other devices, only PTP IEEE-1588 version 2 is supported.**

[6] Downlink only

[7] Limited to servicing Field Device Network(FDN) only

[8] Also supports DNP3 for time synchronization

[9] Limited to IEC 61850 networks only

[10] Including ESXi hosts

[11] With Experion PKS Server install

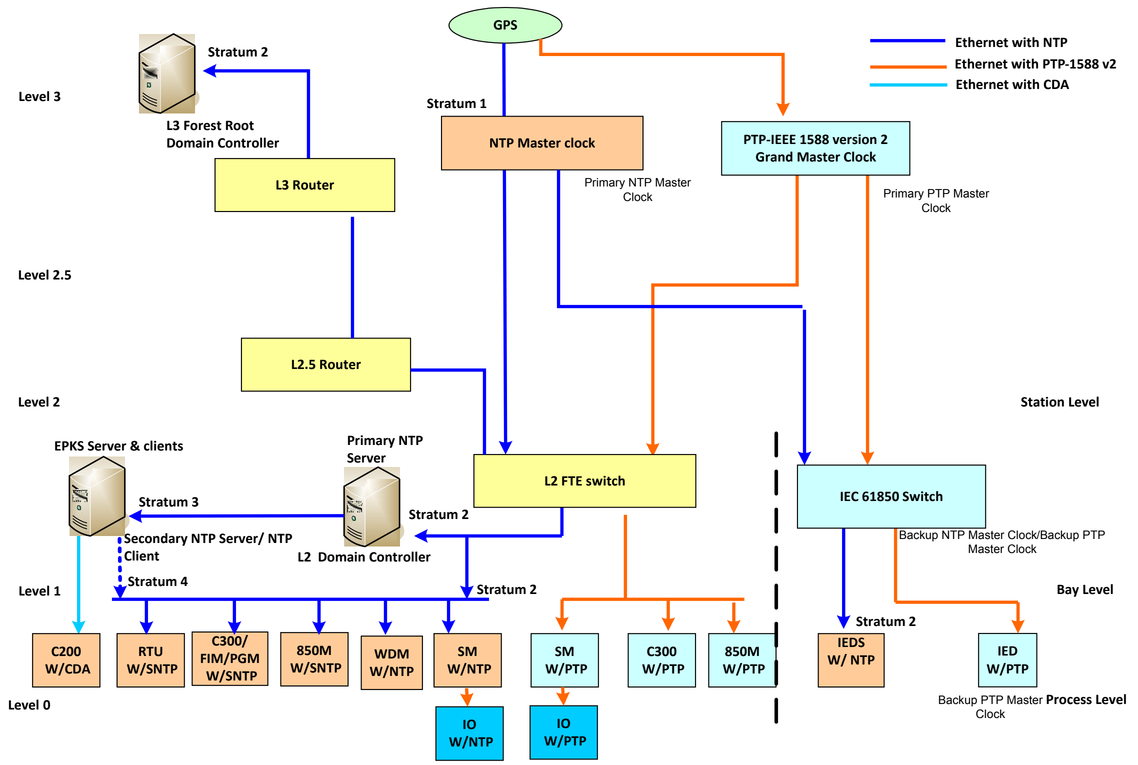


Figure 7: Typical time distribution topology that is supported by Experion connected devices.

Time synchronization in workgroups and Windows domains

By default, workgroups synchronize once a week and Windows domains synchronize during logon or authentication, or once every 8 hours or so if not logged in. Within a Windows domain, computers auto-configure themselves for time distribution.

For more information, see http://technet.microsoft.com/en-us/library/cc749145(WS.10).aspx.

The default time synchronization mechanisms for workgroups and Windows domains do not meet control system specifications, which require localized, high-quality time synchronization.

Level 1 network

The C300 Controller, Series C FIM4, FIM8, PGM, IEC 61850 Interface Module, and Safety Manager require high-quality time served from a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) Server. C200 controllers receive time through CDA from the server.

The quality of time determines how tightly events from different devices can be correlated, especially with regard to digital Sequence of Events (DI SOE). For DI SOE, therefore, it is recommended that you use a high quality external time source such as an IEEE-1588 (Precision Time Protocol)-based time server.

The most stringent requirement for time synchronization at level 1 is from controllers that need high-resolution, digital sequence of events. An example of this requirement is in the electric utilities where thousands of digital input points are monitored. Each state change is time stamped to a minimum resolution of 1 ms. These state changes are logged. After certain faults, such as a generator going offline, the log is frozen for later analysis to see which condition led to the fault. Examples are turbine imbalance, drop in frequency of the grid, circuit breaker trips, and so on. Critical physical and electrical events follow each other over a short period of time and the log is used to identify which event happened first and caused the rest. Typically the cause is used to back-charge the responsible party.

Level 2 network

At level 2, time is a gating factor used in many supervisory functions such as:

- redundancy
- event processing
- system monitoring

Time stamping is also used in diagnostic messages. For example, Safety Manager notifies Experion of all abnormal changes in system behavior by means of time-stamped diagnostic messages.

Summary

Both levels provide important and critical functions to an overall system that is being used to control a plant's processes. System events can be generated from either the hardware side (level 1) or from the supervisory side (level 2). Therefore, time synchronization between the two network levels also needs to be coordinated, ideally, using the same source. This mitigates against messages and events being mishandled, regardless of where they are sourced from.

About time protocols

Simple Network Time Protocol (SNTP) is a proper subset of Network Time Protocol (NTP), which uses the same packet format. As a subset, SNTP gets time from an NTP server, but does not run complex filtering and control algorithms to extract the best time from multiple sources and precisely set the local clock increment rate. SNTP only measures round-trip-delay and sets the local clock when it drifts beyond internal limits.

Time protocols and Microsoft Windows

All supported Microsoft Windows operating systems use NTP. Each domain controller in a Windows Server 2003 or 2008 domain, by default, is an NTP server. The Active Directory provides a hierarchical time infrastructure. Each system added into the Active Directory/domain synchronizes time with a time source in the domains hierarchy.

About setting up time synchronization in your Experion PKS control system

Because the default Windows NTP implementation is not set up for the tolerances needed for control systems, Honeywell recommends that you use the `NTPConfig` tool to configure time synchronization on your Windows nodes. The `NTPConfig` tool corrects the tolerance deficiencies and converts the Active Directory default settings to be compatible with control system requirements. To overcome the tolerances, parameters are updated to maintain more stringent time synchronization.

If your control system is integrated with a Windows domain, it is recommended that you use the domain controller as the time source for *all the clients within the domain* (this is the default setting). As domain controllers are typically not on a network that is accessible to the control system itself, the controllers within the process control should be configured to get their time from an Experion server that has been set up as an NTP server acting as a secondary NTP server, which gets its time from the domain controller.

Time protocols and time servers for Experion PKS controllers

The C300 uses SNTP or PTP to attain the time, but includes its own proprietary ability to adjust the clock increment rate to that of the time source so that fewer actual adjustments (bumps) are necessary (similar to the functionality of NTP).

When plant-wide correlation of C300 DI-SOE is required,PTP must be provided.

As a client, Safety Manager supports the NTP protocol but also supports the PTP time protocol, which is used for synchronization over its own SafeNet network.

Precision time protocol (PTP)

The IEEE-1588 Precision Time Protocol provides high-precision time with low overhead. Unlike NTP, it is only a Local Area Network protocol, requiring a local time server, known as an IEEE-1588 Grandmaster. PTP supports multiple Grandmasters for availability. Typically, Grandmasters get their reference time from GPS, but can also get time from other GPS devices using one of the standard coaxial cable protocol connections. Multiple units from the same manufacturer may even share a GPS antenna. PTP is a UDP Multicast protocol, so it adds some network traffic.

Time source hierarchy

The Series C controllers and interfaces have a time source hierarchy. When the better time source becomes unavailable, they degrade to a less-accurate source. From highest to lowest precision:

- PTP (if enabled)
- SNTP
- CDA Server Protocol

Time source configuration

SNTP is used when the IP addresses of one or two NTP servers are configured in Control Builder System Preferences. SNTP Server 1 is tried first. If unavailable, SNTP Server 2 is tried. PTP is used when individual devices are configured in Control Builder to use it. Once enabled, PTP is self-configuring.

PTP Grandmaster configuration notes

PTP defines synchronization profiles for various applications. We use the default profile. The basic settings are synchronization every two seconds, and using multicast for round-trip-time determination.

Planning your time hierarchy

Implementing a time strategy that is appropriate for a process control system involves using a time hierarchy where the root of the hierarchy is the most reliable time source.

Windows domains, by default, implement a hierarchy of time distribution across the domain. The domain controller that is the PDC Emulator is the node that synchronizes with a reliable external source.

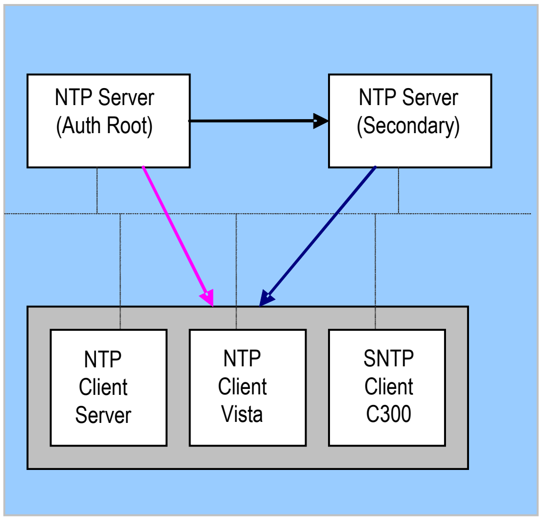
Ideally, all the control systems nodes are linked together in a hierarchy of time critical usage. In most cases, it may be better to set up one or two secondary network time protocol (NTP) servers that service all the control systems NTP clients on the local network. This provides mitigation against requirements on the network being available to keep the time consistent and attain accurate time.

Your organization may already have a time hierarchy in place that can be used as a source from which you can then branch off for the control system. Regardless of the source of time, all topologies should include local NTP servers that serve time in the control system.

Workgroup topology with no external source

In the following diagram, redundant Experion servers are set up as redundant NTP servers. All time clients, such as Flex Stations, Console Stations, and C300 controllers, receive time from the primary Experion server. If this server fails over, time is served by the backup Experion server.

This topology uses the internal CMOS clock of the authoritative server as the time source. This time source is not as accurate and will create deviations in time seen throughout the hierarchy. Systems with strict requirements on sequence of events should not implement this topology.

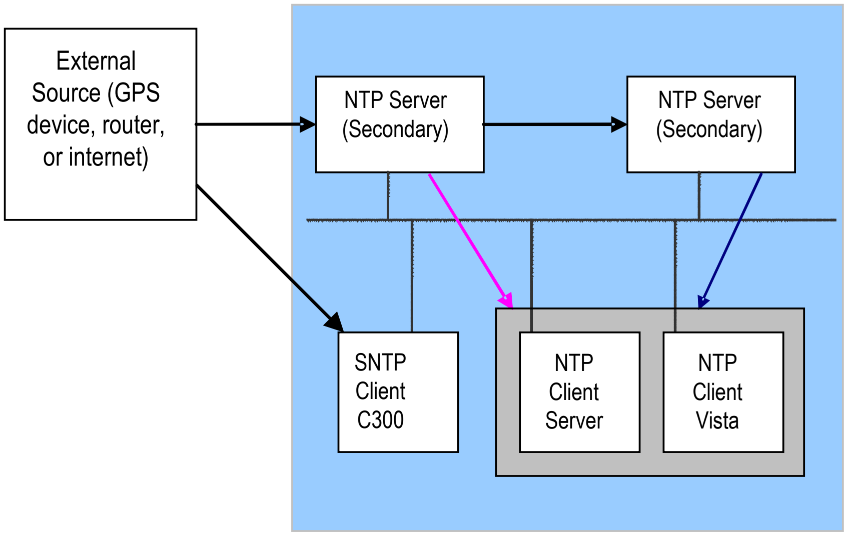


Workgroup topology with external source

In the following diagram, the primary Experion server receives time from an external source. The redundant Experion servers are set up as NTP servers which serve time to all time clients, such as Flex Stations, Console Stations, and Safety Manager. If the primary Experion server fails over, time is served by the backup Experion server. An external source serves time to the C300 controller.

This topology creates a dependency on the network infrastructure between the control system and the external source. The reliability of this network should be taken into consideration when planning this time hierarchy.

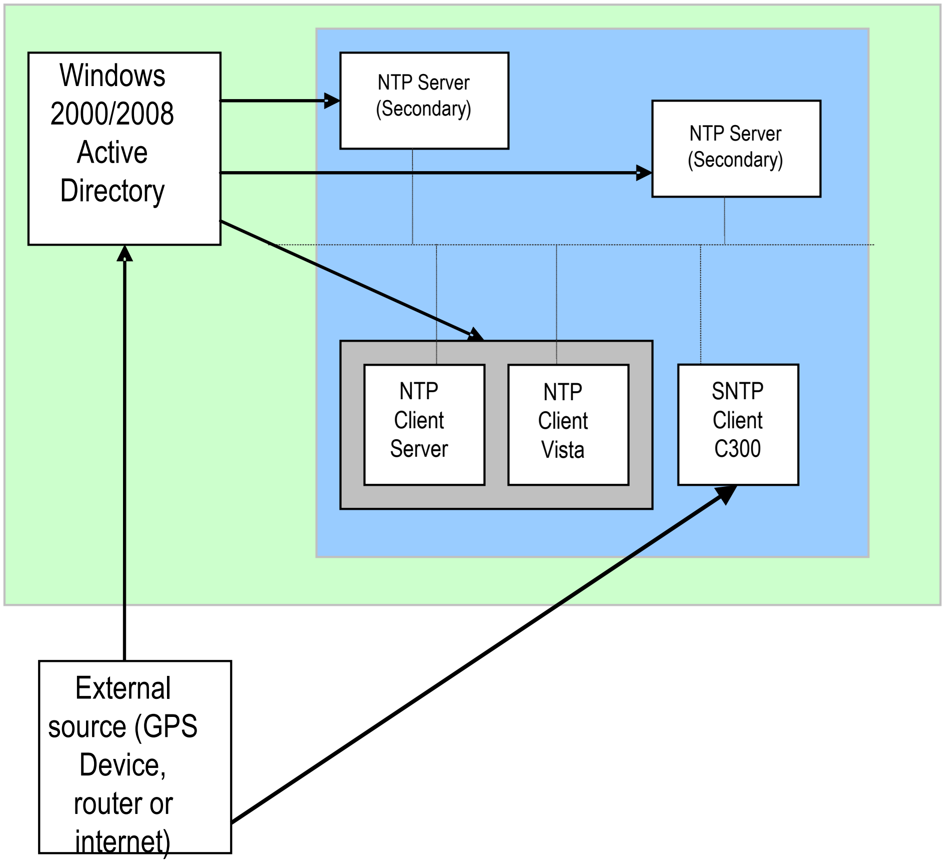
If the network between the external source is reliable or local, then direct access to the external (or local) device is recommended. This means that you only need one secondary server. This is highly recommended for SOE configurations.



Domain topology

In the following diagram, the domain controller receives time from an external source. The domain controller serves time to the redundant Experion servers, Flex Stations, and Console Stations. An external source serves time to the C300 controller.

You should verify that the Active Directory/domain you link to uses a reliable external time source. If an external source is not used, the internal CMOS of the domain controller (or PDC Emulator) is used as the time source. This time source is not as accurate and will create deviations in time seen throughout the hierarchy. Systems with strict requirements on sequence of events should not implement this topology.



Planning considerations for time synchronization

- Controllers and CEEs obtain the start and end of Daylight Saving Time (DST) from Experion servers. For controllers and CEEs to automatically change to DST, the Experion server's clock must be selected to automatically adjust clock for daylight savings changes. DST changeover in the Experion server's clock triggers the controllers and CEEs to change to DST, regardless of whether it’s done automatically by the operating system or enabled manually by the user within the DST period.
- For controllers, CEEs, and Experion servers in the same time zone, whenever DST starts or ends, the controllers and CEEs clocks are adjusted either forward or backward by 1 hour.
- The start and end of DST is always identified from the Experion server. In the case where controllers, CEEs, and Experion servers are not in the same time zone; controllers and CEEs will shift by one hour (irrespective of any time zone the controller or CEE is in and also irrespective of if DST is applicable for controller or CEE time zone) at the start and end of DST (applicable as per server time zone).
- For controllers and CEEs that are in different time zones to the Experion servers, Honeywell recommends not to use **Automatically Apply DST** option and to manually change the 'Daylight Savings Time' on these controllers and CEEs.

  For controllers and CEEs that are in the same time zone as the Experion servers, you can use the **Automatically Apply DST** option. Therefore, the 'Automatically Apply DST' option can be applied to specific controllers and CEEs within an Experion cluster.

Stations

This section describes how to determine your Station requirements. (Station is Experion's user interface.)

Issue	Comments
User types	Identify the user types and assess their respective needs.
Read-only access by casual users	Determine whether an eServer, which provides read-only access to displays and reports, would satisfy the needs of users such as managers and production controllers.
Flex Stations	Flex Station is the standard type of Station. It typically runs on a standard computer, and is suitable for most users and most tasks.
Console Stations	If you have Process Controllers and don't want to suffer loss of view if the server fails, you need Console Stations.
Mobile Stations	If users want access to data as they move around the plant, then you should consider Mobile Station.
Defining and maintaining installation and network settings for Stations	When you have decided on the kind of Stations you need, you can use Installation Builder to gather and deploy computer and network configuration information for those Stations. The data collected by Installation Builder can be used to perform installation and pre-configuration tasks such as automating the software installation process or maintenance tasks such as changing DNS settings. See the *Installation Builder Users Guide.*
Simultaneous view of several displays	Determine whether users (especially operators) need to simultaneously see several displays.
Loss of view during operator changeover	Decide whether you need to use the Signon Manager option so that Station keeps running when, for example, operators change shift.
Specialized hardware	Determine whether any users (especially operators) need specialized hardware, such as multi-monitor consoles, membrane keyboards and touch-screen displays.
Security requirements	Based on user types, work practices and site layout, determine the most appropriate security setups for Stations and Windows. See the *Network and Security Planning Guide*.
Display update rates	Determine the rate at which you want displays to be updated.
Displays	Determine your display requirements.

Related topics

“Identifying user types and assessing their needs ” on page 55
“Connection options for Flex Stations” on page 56
“About Console Stations and Consoles” on page 57
“Mobility” on page 60
“Multiple-window Station configurations” on page 61
“Station update rates” on page 62
“Signon Manager ” on page 63

“Specialized Station hardware” on page 64
“Determining your Station requirements (an example)” on page 65
“eServer” on page 31

Identifying user types and assessing their needs

Before you can determine your Station requirements, you must first identify each user type, and then assess their respective needs.

Typical user types include: operators, maintenance engineers, managers and production controllers.

Operators generally need dedicated Stations, whereas maintenance engineers may only need access to a Station for a few minutes, two or three times a day. Other users, such as managers and production controllers, may only need read-only access to trend-related displays and reports.

Connection options for Flex Stations

There are two ways of connecting a Flex Station to the server:

- **Static**. A permanent, dedicated connection. This is the recommended connection type for Flex Stations used by operators.
- **Rotary**. An 'as required' connection. This is the recommended connection type for users who do not need full-time access to the server, or who need remote access (typically through a modem).

  Rotary connections are advantageous from a licensing viewpoint because the license specifies the maximum number of simultaneous Station connections.

About Console Stations and Consoles

Console Stations and Consoles are advisable in an environment where continuity of view is paramount and where it is important to minimize the impact of a server being unavailable.

About Console Stations

Console Stations provide direct access to process data as well as alarms and messages from CDA sources such as Process Controllers, FIM, IOLIM, and ACE nodes. This direct access provides a continuous view of your process, even if the Experion server is unavailable (for example, during a server failover). Consequently, there is no loss of view of critical data and alarms when the server fails, and so an operator can still control and monitor the process.

During server outages, any specific chart visualization access directly to the Engineering Repository Database (ERDB) view is not available unless at least one of the servers is available. Other views, such as Detail Displays, remain available at all times.

A Console Station is also connected to an Experion server. After you configure the connection to the Experion server, the server database files are replicated to the Console Station. This means that configuration of items such as process points is only done once.

Although a Console Station provides direct access to data, alarms and messages, some functions, such as reporting, history and events collection, are still provided by the Experion server. Therefore, if the Experion server is unavailable these functions are not available on the Console Station. For details, see the “Functions available on the Console Station” and “What happens when the Experion server is unavailable” topics in the “Configuring Console Stations and consoles” section of the *Server and Client Configuration Guide*.

Attention

Console Stations do not report any CNET or CNI-related notifications. This is because the Network Diagnostic Manager (NDM) that is responsible for reporting CNET or CNI-related notifications is not enabled on Console Stations. NDM runs only on primary servers or non-redundant servers. For more information about NDM, see the “NDM Overview’” topic in the “Alarm and Event Processing” section of the *Control Hardware Notifications Theory Guide*.

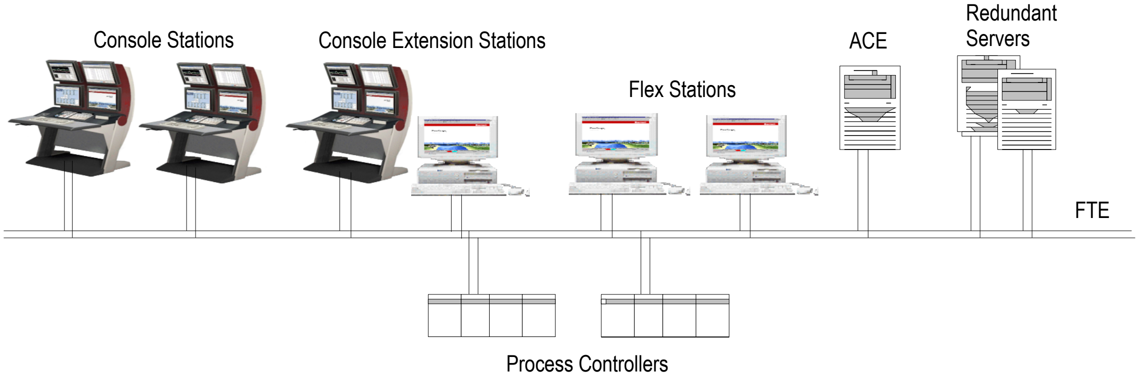
About Console Extension Stations

A Console Station can also have clients connected to it. These clients are called *Console Extension Stations*. A Console Extension Station connects to a Console Station in the same way that a Flex Station connects to an Experion server. A Console Extension Station has the same functionality as a Console Station. For each Console Station, you can connect up to three Console Extension Stations.

A Console Station and Console Extension Station can operate in the following environments:

- Distributed system architecture
- Icon Series Console environment
- Multi-window environment

The following figure shows an example architecture including Console Stations.



Licensing

For more information about Station licensing, contact your Honeywell representative.

Consoles

A *Console* is a logical grouping of Console Stations and Console Extension Stations constituting a single workspace for an operator.

In general, the Console Stations and their Console Extension Stations that make up a Console are not just a logical grouping but are grouped together in the same physical location. The Stations that make up a Console may well be mounted in a single piece of control room furniture, which provides a workspace for a single operator.

A Console is associated with a single Experion server, and can include the following combinations:

- A Console Station with a Console Extension Station
- Multiple Console Stations
- Multiple Console Stations with Console Extension Stations

Sample scenarios

A typical Console might consist of the following equipment in a single control room:

- Two Console Stations
- One Console Extension Station (connected to Console Station 2)
- An operator entry panel connected to each Station
- Six screens (individual CRTs)
- Multi-window configuration with SafeView

This configuration provides redundancy and thus has the advantage of increasing Console capacity and robustness because the Console will continue to operate in the event of a single Console Station failing. Having additional Stations in the Console also meets the need for a large number of concurrent displays.

If necessary, you can also configure Consoles to cover the need for a remote Station. For example, you can set up a Console that includes a Station (either Console Station or Console Extension Station) in a remote location (outside the control room). This provides a degree of safety and enables plant operations to continue in the event that the control room can not be used. Within the control room the Console equipment can consist of a mix of Console Station and Console Extension Stations as described in the previous scenario.

Alarm and message acknowledgement in Consoles

In general when an alarm is acknowledged or silenced on one Station (whether it is a Console Station or a Flex Station), the alarm is acknowledged or silenced on all Stations in that system. By contrast, the default setting for a system with a Console is for alarms to have to be acknowledged on every Console in the system. You can, however, change this default setting within a server system so that when an alarm is acknowledged on one

Station (whether Console or Flex) it is acknowledged on all Stations, including Console Stations within a Console.

For more information, see the 'Configuring Console Stations and consoles' section in the *Server and Client Configuration Guide*.

Mobility

There are several solutions for mobility and remote access to Experion data.

A remote device can be:

- A handheld or similar mobile device on a wireless network.
- A computer on a remote network.
- A computer that is not on your Experion process network (for example, a computer that is connected to your business network).
- A computer that is not running the Microsoft Windows operating system.

Considerations for selecting a mobility access solution:

- If you need access from a small screen on a mobile or handheld device, use eServer Mobile Access.
- If you need full Station capabilities on a larger screen, use Mobile Station.
- If you need eServer Premium Access functionality from a client that does not meet all of the requirements of eServer Premium Access, use Mobile Access for eServer Premium.
- If you need simple, lightweight access to Station displays, use eServer Standard Access.

The following table identifies the requirements and characteristics for each mobile access solution.

Solution	Node requirements	Characteristics	Zero client
eServer Standard Access	eServer	Business and field users. Typical desktop screen size. Read only access.	Yes
eServer Premium Access	eServer	Business and field users. Typical desktop screen size. Read only access. Live updates and trends.	No. Requires a small installation.
eServer Mobile Access	eServer	Field users mainly. Designed for small screens, such as handheld devices.	Yes
Mobile Station	Remote Engineering and Station Server (RESS)	Field users mainly. Full Station capabilities for field users. Typical desktop screen size. Read and write access. Can also be used for remote access to Configuration Studio.	Yes
Mobile Access for eServer Premium	eServer and a Remote Engineering and Station Server (RESS)	Business and field users. Typical desktop screen size. Read only access. Live updates and trends.	Yes

Related topics

"eServer" on page 31

"Remote Engineering and Station Server" on page 33

Multiple-window Station configurations

There are two Station configurations that provide a multiple-window setup:

- *Multi-window Station*. A Flex or Console Station that uses SafeView to manage several windows (typically two or four), each of which can contain a separate display.

  Multi-window Station enables you to control the placement of displays in the various windows. For example, you may want the Alarm Summary in the top-left window, trends in the top-right window and point detail displays in the bottom-right window.
- *Multiple static Station*. A computer that has up to four instances of Flex Station running simultaneously. Each instance requires its own static connection to the server.

In practice, both setups require specialized hardware, such as the Icon Series Console.

Multiple-window Station and tabbed displays

You can enable tabbed displays on either of these configurations. With tabbed displays, operators can call up multiple displays in individual tabs within a Station window without having to close an existing display.

Related topics

"Icon Series Console" on page 64

Station update rates

In an Experion system there are a number of different update rates that you can configure, all of which are taken into account when determining the 'actual update rate' that is visible to an operator. For example, you can configure the rate at which:

- The Experion server subscribes to data from devices
- Station receives updates from the Experion server
- Individual custom displays are updated.
- The values of individual parameters on a custom display are updated

When planning your system it is recommended that you specify the longest practical update rate to reduce the load on the server. This is a particularly important consideration if a Station uses a remote or low-bandwidth connection.

For more detailed information about the various types of update rates and how they are used to determine the 'actual update rate', see the topic 'Understanding update rates' in the 'Customizing Stations' section of the *Server and Client Configuration Guide*.

Related topics

"Displays" on page 119

Signon Manager

If you use integrated security, and want to keep Station running during user changeovers - for example, when operators change shift - you need to use the Signon Manager option. (Without Signon Manager, the outgoing user must close Station and log off Windows; and the incoming user must log on and restart Station.)

Signon Manager is also recommended if you have a multiple static Station because it enables users to simultaneously log on/off each instance of Station.

If you have installed a supported smart card reader, Signon Manager can be configured so that operators not only have to use a smart card for authentication but may also be required to enter a PIN as well as a password.

Note that Signon Manager requires integrated security.

Note however that when using the Integrated Keyboard (IKB) to change the security level within Station, the Experion security level also still applies and the higher of the two will be the resulting security level and is what is shown in Station status bar. To enable the keyswitch functionality, Signon Manager must be installed and running on the node (even if using Station based security).

For more information about Signon Manager, see the topic 'About Signon Manager' in the *Server and Client Configuration Guide*.

Specialized Station hardware

In general, Station runs on a standard computer, with a PC keyboard, monitor, and mouse. However, Station supports most Windows-compliant peripherals such as trackballs and touchscreens, as well as two specialized keyboards:

- **Operator Entry Panel (OEP).** This is a membrane-style keyboard with dedicated function keys. It is suited for use by operators in harsh environments.
- **Integrated Keyboard (IKB).** This consists of a standard keyboard combined with dedicated function keys and built-in trackball. It is suited for use by operators who need a large number of function keys in addition to a standard keyboard.
- **Experion Touch Panel.** This is a touch panel that can be configured to have IKK or OEP features. The Experion Touch Panel is constrained to landscape orientation. It is suited for use by operators and engineers to monitor and control the site.

Attention

The IKB and the OEP keyboard are not compatible with Experion Electronic Signatures. You cannot use either of these keyboards with Experion Electronic Signatures.

Icon Series Console

For demanding tasks, you can use Honeywell's Icon Series Console, which includes up to four flat-panel monitors and an OEP.

Either of Station's multiple-window configurations is suitable for use with an Icon Series Console.

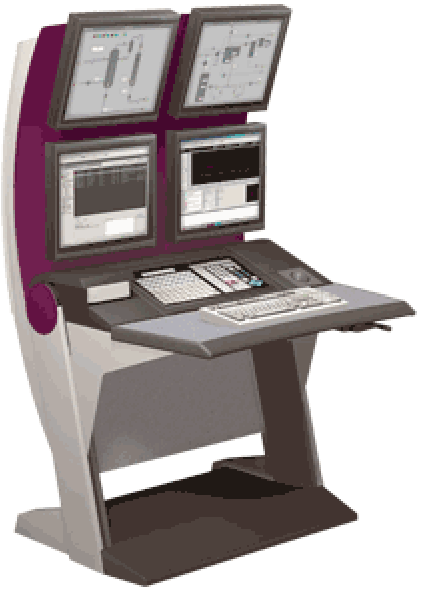


Figure 8: An Icon Series Console

Related topics

“Multiple-window Station configurations” on page 61

Determining your Station requirements (an example)

The following example shows how to determine your Station requirements.

Your configuration and Station requirements are as follows:

- The site has a control room, staffed with two operators. It is essential that both operators can always see the Alarm Summary and some critical trend displays.
- Maintenance engineers need access to Stations on the production line, and have suggested five suitable locations.
- The two production controllers need one Station in their office. After hours, one of them is always on call—consequently, they both need Station at home.

The following Stations meet the requirements:

- Two Console Stations in the control room. Each Station is fitted with four monitors, and uses Multi-window Station and SafeView to ensure that the critical displays are always visible.
- Five rotary Stations on the production line.
- One static Station in the production controllers' office.
- Two modem-connected rotary Stations at the homes of the production controllers.

Because of the anticipated usage levels of the rotary Stations, you decide you only need a license for six Stations: three static (includes the two Console Stations) and three rotary.

Printers

This chapter describes how to determine your printer requirements.

Issue	Comments
Alarm printing	Alarm printers are typically located near Stations used by operators—for example, in the control room. Alarm printing requires a 132-column dot matrix printer that has been qualified for use with Experion.
Reports	Reports can be printed on any suitable printer. Typically, each report is directed to the most convenient printer on the network. For example, an alarm report might be printed on the printer in engineering office.
Display captures	If you need to capture display contents, such as trends, you should consider a color printer.

Controllers

Experion supports a wide range of controllers in addition to Process Controllers. This chapter describes issues you need to consider in order to integrate these controllers with your Experion system. (The *Control Hardware Planning Guide* contains planning information for Process Controllers.)

Issue	Comments
Experion-specific documentation	Read the interface reference for each type of controller you want to integrate with Experion.
Monitoring and control strategies	Configure the controllers so that they do not impose excessive communications or processing loads on the server.
Connection options	Determine how you are going to connect the controllers to the server.
Scanning strategies	Determine the server's data update requirements, and then design a scanning strategy that minimizes the communications load.

Related topics

“Interface references” on page 70
“Monitoring and control strategies” on page 71
“Connection options” on page 72
“Scanning strategy” on page 87

Interface references

There is a separate interface reference for each type of SCADA controller supported by Experion. These references include integration details, such as connection and configuration options, that may affect your design and planning decisions.

If Quick Builder is used to configure a controller, the interface reference is also included in Quick Builder's help.

Monitoring and control strategies

Attention

Do not include the server in any control loops because potential delays, caused by communications traffic or heavy server loads, may seriously affect your plant's operation.

You should configure controllers so that they do not impose excessive communications or processing loads on the server. It is important to remember that the server's primary tasks are to:

- Monitor system activity
- Start/stop processes
- Generate reports
- Provide data to other systems

Connection options

The way in which you connect a controller to the server depends on several factors, including your plant's layout and the controller's communication port(s). (Note, however, that your choice may depend on restrictions specified in the interface references.)

Network connections

If a controller has a network port, you can connect it directly to the network.

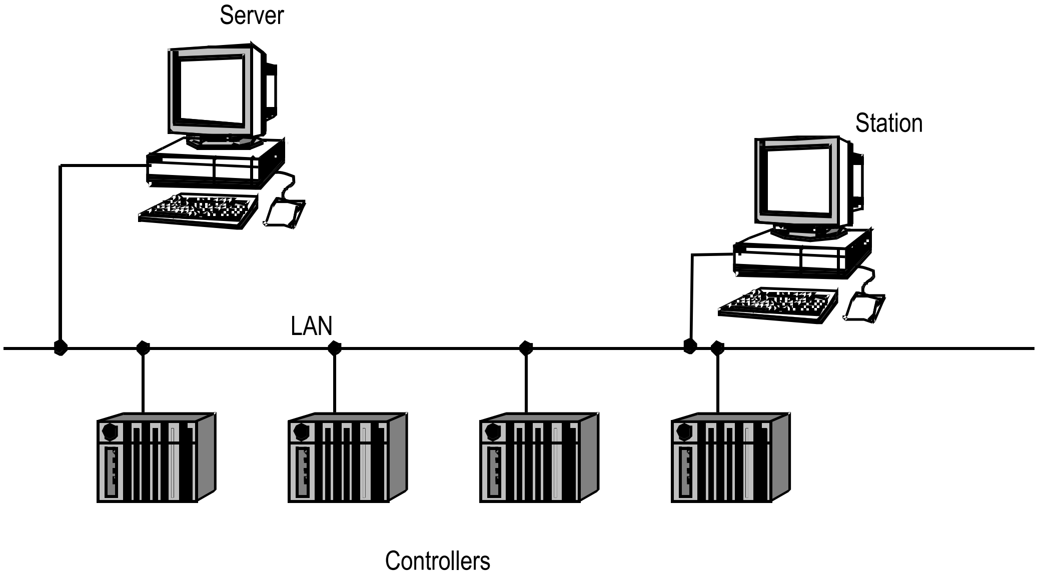


Figure 9: Controllers connected directly to the network

Experion also supports a number of proprietary networks, such Fault Tolerant Ethernet (FTE) and ControlNet. For more information about these networks, see the *Network and Security Planning Guide*. For a list of supported proprietary networks, see the *Overview*.

Redundant connections

If you have network redundancy, you may be able to connect some controllers using redundant connections. To check whether your controllers support redundant connections, see the manufacturers' documentation and the Experion interface reference for that controller or communication protocol.

Direct serial connections

If you have a small system, you can connect controllers to the server's serial ports.

Note that you can add more serial ports to the server with a *serial adapter*. An advantage of serial adapters is that they provide a choice of interfaces, such as RS-422 and RS-485, which are suitable for medium-distance links.

For a list of qualified serial adapters, contact your local Honeywell representative.

Indirect serial (terminal server) connections

You can connect controllers to the network through a *terminal server*. (A terminal server allows you to connect several controllers to the 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.

Tip

Be aware of the difference between the similar sounding terms 'Terminal Servers' and 'Terminal Services'. They are quite different terms referring to different technologies and are not interchangeable.

A Terminal Server is a hardware device for connecting one or more serial communication controllers (terminals) with an ethernet network.

Windows Terminal Services (now known as Remote Desktop Services) refers to software which provides remote desktop connection of Windows-based computers over a network.

Terminal servers are particularly useful if you have a:

- Plant-wide LAN, and you want to connect controllers to the LAN—as shown in the following figure.
- Geographically-dispersed controllers on a WAN.

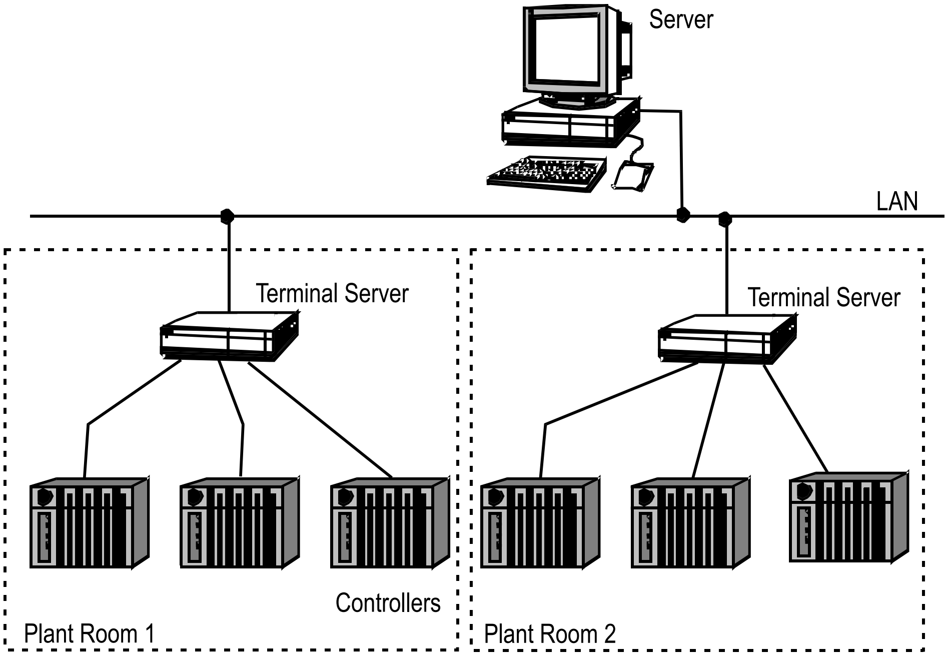


Figure 10: Typical system with terminal servers

Terminal servers and server redundancy

If you have redundant servers, you must use terminal servers to connect controllers that only have serial ports. (Unlike the controllers, terminal servers can automatically switch communications to whichever server is running as primary.)

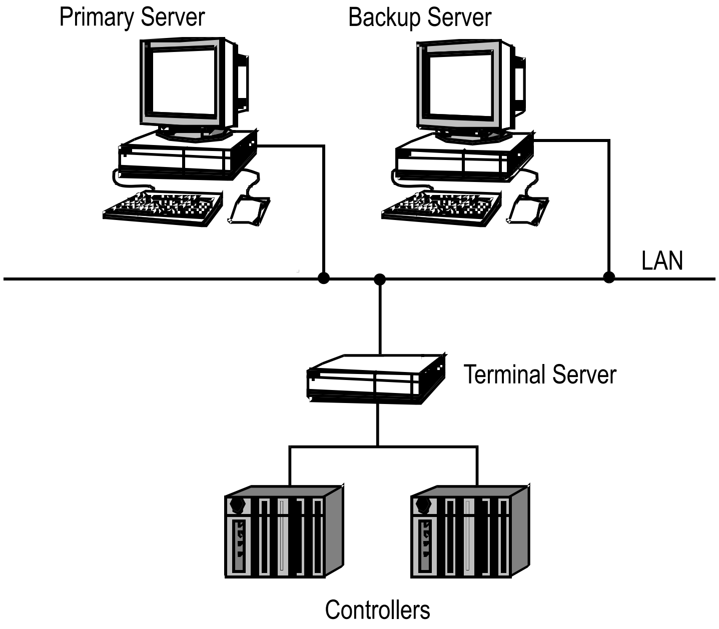


Figure 11: A terminal server in a redundant server system

Modems

You can use modems to connect controllers located at remote sites, such as reservoirs.

If you only require infrequent scanning—as in the case of a reservoir—you could use a dial-up modem. If you require more frequent scanning, you could use a modem in conjunction with a leased line.

Note that you can also use modems to connect remote Flex Stations—for example to give engineers after-hours access from home.

Specialized links

If modem connections are not suitable, you can also use radio, satellite or other specialized links. In such cases, discuss your requirements with your local Honeywell representative.

Points

This section describes how to determine your point requirements.

Tip

If you want to use a user-defined data format, you must define the format on the server. See the section titled "About user-defined data formats" in the *Server and Client Configuration Guide* for more information.

Issue	Comments
Point names	Develop a consistent naming strategy for your points.
Point types	If you have controllers other than Process Controllers, you need to understand the purpose and capabilities of Experion's inbuilt point types (called *standard* points).
System interfaces	Experion includes a number of high-level interfaces—called *system interfaces*—that allow it to exchange data with other applications or subsystems without the need for separately defining points.
Algorithms	Determine whether you need to use any algorithms.
Scripts	Determine whether you can use *server scripts* to perform specialized tasks on points.
History collection	Determine your history collection requirements.
Groups	Determine which points need to be grouped and displayed together.
Trends	Determine which point parameters need to be displayed in a graphical manner.
Scanning strategy	Develop an appropriate *scanning* strategy. (Scanning is the process by which the server reads from/writes to memory locations in controllers other than Process Controllers.)
Number of points	Estimate the number of points you require—the number determines your licensing requirements.
Multiple servers	If you have multiple servers, review information on point data in a DSA system.

Related topics

"Point naming conventions" on page 76
"Standard point types" on page 78
"System interfaces" on page 80
"Algorithms" on page 81
"History collection" on page 82
"Groups" on page 85
"Trends" on page 86
"Scanning strategy" on page 87
"Estimating the number of points required" on page 90
"Server scripts" on page 34
"About point data in a DSA system" on page 29

Point naming conventions

All points within your system have a *tag name* (also called a *point ID* or *point name*) and an *item name*. Tag names must be unique, whereas item names can be duplicated as long as the resulting full item name is unique.

When a point is created, it is given a unique tag name, for example, POINT01 or POINT02. This identifier is used in Experion whenever it is necessary to refer to a point in the server (for example, on a custom display or in a report).

Point names must follow certain naming rules:

- An item name cannot match the item name of any other point belonging to the same parent asset.
- Tag names must be unique within the cluster server.
- Tag names and item names can contain up to 40 single-byte or 20 double-byte alphanumeric characters, with at least one alpha character.
- Tag names and item names are not case-sensitive: *`POINT01`* and *`Point01`* represent the same asset.
- The first character of a tag name and an item must not be any of the following characters:
  - At sign (@)
  - Dollar sign ($)
  - Space
- Tag names and item names cannot contain any of the following characters:
  - Ampersand (&)
  - Asterisk (*)
  - Backslash (\)
  - Braces { } (rule applies to item names only)
  - Brackets [ ]
  - Caret (^)
  - Colon (:)
  - Comma (,)
  - Double quote (")
  - Equals (=)
  - Forward slash (/)
  - Greater than (>)
  - Less than (<)
  - Number sign (#)
  - Parentheses ( )
  - Percent (%)
  - Period (.)
  - Question mark (?)
  - Semi colon (;)
  - Single quote (')
  - Space (rule applies to tag names only)
  - Tabs
  - Vertical bar (|)
- The last character of a tag name and an item must not be a space.
- A *full item name*:
  - Must not be longer than 200 characters
  - Must be unique

It is also important for both engineers and operators that points are named in a consistent and 'user-friendly' manner. You might, for example, consider:

- Basing the names on existing documentation, such as schematics and wiring diagrams, so that users can easily switch between documents and displays.
- Using the same prefix for related points, so that users can easily find related points.
- Starting each part of a name with a capital, to improve readability. For example: *Boiler1Temp*.

Examples

- **Using a device name prefix**. All points associated with *Boiler 3*:

  ```
  Boiler3Temp
  Boiler3InValve
  Boiler3OutValve
  ```

- **Using recipes**. A recipe is used to control a *unit* called *B5*. (A unit is typically something like a chemical cracker.) The recipe includes the following *ingredients* (each ingredient contains a value that is downloaded to the unit): *WATER*, *ACID*, and *START*.

  You need to create the following points for unit *B5*:

  ```
  B5WATER
  B5ACID
  B5START
  ```

Point IDs and Distributed System Architecture (DSA)

With DSA, you can have more than one point with the same point ID (or tag name) provided that the name is unique to a given server and that the points do not belong to the same asset.

If points with duplicate IDs (tag names) are created, then they can be distinguished by prepending the tag name with the server alias. If, for instance, there are two points with the duplicate tag name *FIC123* on servers *NorthPlantSrv* and *SouthPlantSrv*, then the prepended tag names of each point would be *NorthPlantSrv:FIC123* and *SouthPlantSrv:FIC123*. The prepended tag name can be used wherever normal tag names are used (for example, in an HMIWeb display).

Two important restrictions for points with duplicate tag names are:

- They must not belong to the same asset.
- Their prepended tag name (for example, *NorthPlantSrv:FIC123*) must not exceed 40 characters.

Related topics

"Distributed System Architecture" on page 29

Standard point types

Experion provides the following types of *standard* (SCADA) point that are used to exchange data with controllers other than Experion Process Controllers.

Standard point type	Use
Analog	Continuous values, such as temperature or pressure.
Status	Digital values (on and off).
Accumulator	Totalizer values.
Container	A user-defined point type that allows you to treat a group of related points as if they were one point.

Standard points have a composite data structure that can represent several field values as parameters. For example, you only need one analog point for a control loop that maintains the temperature of an oven, because the point's data structure includes the following *parameters* (data items):

- Process variable (PV) to record the current oven temperature
- Output variable (OP) to change the temperature of the oven
- Set point (SP) to specify the correct oven temperature
- Mode (MD) to change the loop from manual to automatic control

User-defined parameters

You can increase the functionality of a standard point by defining your own parameters to store custom data. For example, you may want to store a value generated by a script, or record the serial number of the device associated with the point.

For more information about standard points, see the topic titled "Understanding and configuring points" in the *Server and Client Configuration Guide* and 'Building and configuring points' in the *Quick Builder User's Guide*.

Data quality

For point parameters values acquired by the server's OPC scan task, the OPC Quality of the value is also stored. When no OPC Quality is available, Experion sets the quality according to the following rules.

1. If the value is not a number (NaN), the quality is set to *UNCERTAIN*.
2. If there is a communications error, the quality is set to *BAD* with a substatus of *Comm Failure*.
3. If neither of the above is true, the quality is set to *GOOD*.

Container points

A *container point* ties together a set of related points so that they can be managed as if they were one point. Container points not only speed up configuration tasks, they also make it easier for operators to manage your system.

A container point is, in effect, a user-defined point type that matches your data requirements for a particular type of device or process. For example, if you have fifty identical compressors, you could create a new type of container point called 'compressor', and then create one compressor point for each compressor.

For each type of container point, you must:

- Define its structure in Quick Builder
- Create a *point detail display* in Station (A point detail display shows run-time values and configuration settings for a particular type of point, and is functionally equivalent to the point detail displays supplied with Experion.)

You may also want to create a matching *faceplate*. (A faceplate is a specialized popup that shows a subset of the details shown on the point detail display—typically the point's run-time values and control settings. A faceplate appears when an operator clicks an object that is linked to a point.)

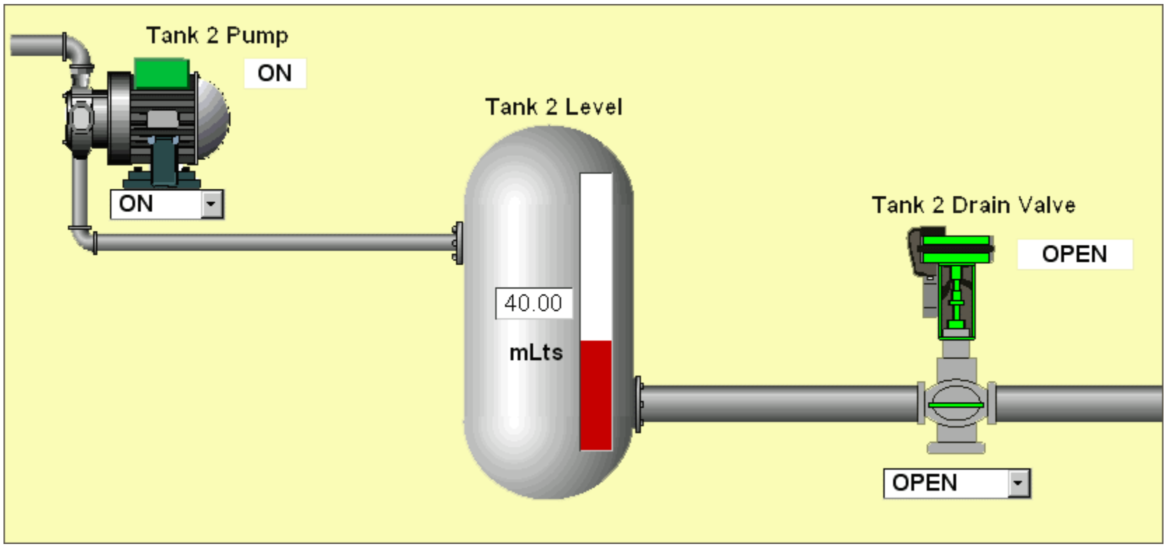


Figure 12: Typical point detail display

For more information about container points, see 'About container points' in *Quick Builder*.

Related topics

"Quick Builder" on page 161

System interfaces

Experion includes a number of high-level interfaces—called *system interfaces*—that allow it to exchange data with other applications or subsystems without the need for separately defining points.

The database structure of system interface—called *flexible points*—is determined by the application/subsystem, rather than by Experion.

The documentation for each system interface contains Experion-specific information, such as integration issues and connection options, that may affect your design and planning decisions.

For more information about the OPC Interface, see the “Configuring OPC” section of the *Server and Client Configuration Guide*.

For more information about TPS Integration, see the *Integrated Experion-TPS User's Guide*.

Algorithms

An algorithm extends a point's functionality by performing additional processing, or initiating an action. Experion provides two types of algorithms:

- **PV**. Gathers/manipulates data, the result of which is usually stored in the point's PV.
- **Action**. Initiates an action—such as requesting a report—when the point's PV changes value.

  Note that you should use algorithms with discretion, because attaching them to numerous points may adversely affect the server's performance.

For a description of each algorithm, see 'Algorithms' in *Quick Builder*.

History collection

Experion can be configured to store the values of point parameters at predetermined intervals to create a history of process values. This process is known as history collection.

Experion provides two different ways of collecting and storing historical data for point parameters:

- Periodic history
- Exception history

The historical data collected by Experion can be used for:

- Third-party applications via the Experion OPC HDA Server and ODBC driver.

Tip

When connecting a third-party historian (such as PI) to Experion, it is strongly recommended that you use the OPC HDA server rather than the OPC DA server, because the HDA server will prevent duplicate load on the control network. Also, all point parameters collected into the third–party historian should be assigned to Experion history.

- Operational purposes, like trend monitoring (in the case of periodic history).
- Collection and analysis by enterprise historians, like PHD servers.

Because the data from both periodic history and exception history is readily accessible to specialized historians, the transmission of Experion history data places no additional load on your control network.

Related topics

"System displays" on page 120

Periodic history

Periodic history collects and stores numerical data at predefined regular intervals. Periodic history data is generally used for operational purposes such as trend monitoring but is also collected for historical analysis.

Experion has a comprehensive range of collection rates for periodic history. These collection rates provide a high degree of flexibility in moderating the load on your control network.

- *Fast history* stores snapshots of a point parameter at short regular intervals. You can choose from 8 different collection rates. By default, the fastest collection rate is 5 seconds but this can be changed to 1 second if necessary.
- *Standard history* stores snapshots at slightly longer intervals, ranging from 1 minute to 30 minutes. The fastest standard history collection rate of 1 minute can be changed to 30 seconds if necessary. In addition to storing snapshots, standard history also calculates and stores average values, based on the standard history snapshot rates. The default averages are: 6-minutes, 1-hour, 8-hours, and 24-hours.
- *Extended history* stores 1, 8, and 24-hour snapshots.

If you need to further customize the periodic history collection intervals, please contact your Honeywell technical representative.

Note that history collection is synchronized to the system time. For example, the 6-second collection occurs at 6, 12, 18 (and so on) seconds after the minute boundary on the system.

Exception history

While periodic history is used for *numerical* data and primarily for operational purposes, exception history is currently only available for *string data* collected for analysis by enterprise historians such as PHD servers.

Like periodic history, exception history scans point parameter values at predefined intervals and offers a comprehensive range of scanning intervals: with exception history you can choose from up to 16 different scanning rates. Unlike periodic history, however, exception history is based on sampling rather than regular collection: it only stores the scanned values when they are different to the last stored value. This not only helps to minimize the database size but also the load on the control network.

The default collection rates for exception history are:

- 5, 10, 15, 30, and 60 seconds
- 5, 10, 15, 30, and 60 minutes
- 2, 4, 6, 8, 12, and 24 hours

If you need to customize the exception history collection intervals, please contact your Honeywell technical representative

Offset groups

If you are collecting standard periodic history or exception history for TPS point parameters you can control the impact of history collection on the LCN by assigning point parameters to a history offset group. An offset group is used to specify a predefined delay, which enables the data collection to be staggered. This helps to reduce the impact of history collection processes on the performance of the underlying control system. You can choose from 16 default offset groups.

Note that offsets are not reflected in the time stamps for stored data. For example, if there is a 15-second offset and the data is collected at 8:00:15, the data is still time-stamped as if it had been collected at the beginning of the interval, that is, at 8:00:00.

Storage requirements for history samples

Experion stores history values in physical files. The storage requirements for history collection are detailed below. However, note that it may not be possible to configure the maximum number of history parameters available. For more information about the maximum number of point parameters for which you can collect history, contact your Honeywell representative.

Periodic history

There are five history files for standard history - one for the snapshots and four for the averages. There is a single history file for fast history, and there are three history files for extended history.

Use the following formula to determine your total storage requirements (in bytes) for periodic (that is, standard, fast, and extended) history:

```
(((N1+N2+N3+N4+N5+5)*(PS*7+8))+((N6+1)*(PF*7+8))+((N7+N8+N9+3)*(PE*7+8)))*2
```

Where:

Variable	Description
N1–N5	The number of samples retained by each of the standard history files (*N1* = 1-minute snapshots, *N2* = 6-minute averages, and so on).
N6	The number of samples retained by the fast history file.
N7–N9	The number of samples retained by each of the extended history files (*N7* = 1-hour snapshots, *N8* = 8-hour snapshots, and *N9* = 24-hour snapshots).
PE	The number of point parameters with extended history.
PF	The number of point parameters with fast history.
PS	The number of point parameters with standard history.

Exception history

Exception history is stored in a set of two data files. Exception history requires at least 1.6 GB of free disk space: this allows for two data files of 500 MB each, as well as extra space when performing archiving operations.

Archiving history samples

You can configure each history file to hold up to 100,000 samples for each parameter. In the case of fast history, the history file fills up very quickly. For example, if you set the fast history interval to 1 second, then 100,000 samples represents just over one day.

Note that there is a limit to the size of each history file and that the number of samples stored decreases as the number of parameters increases. Furthermore, the more samples you add, the greater the impact on the server's system memory and CPU. For optimum performance, especially in a redundant server system, it is recommended that you configure an individual history file to be no greater than 500 MB in size (this is the default setting).

If you need to keep more than the maximum number of samples that each history file can accommodate, you must configure the History Archive Manager to archive the history files at appropriate intervals. Typically, history files are archived to another disk on the server, a file server or to recordable media such as DVDs or CDs. While it is possible to estimate when the files for periodic (that is, fast, standard, and extended) history files will be 'full', as there is a constant collection and storage rate, it is not possible to do this with exception history files as samples are only stored when their value or quality varies from the last stored value or quality.

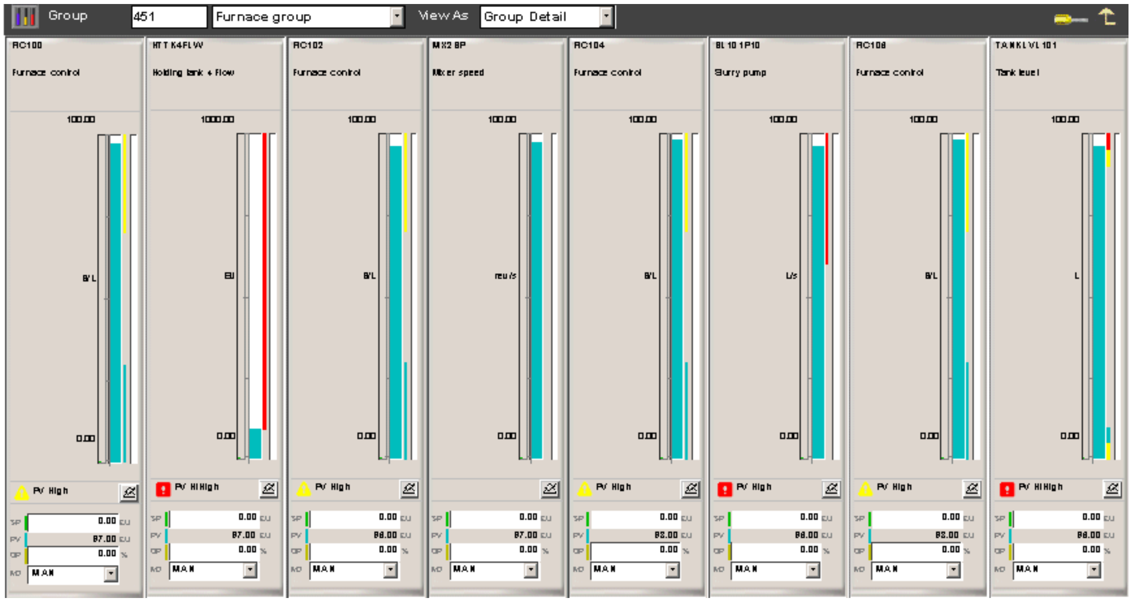
Attention

If trend displays on Station need to access historical information that has been archived, the archives should be located on the server otherwise there will be performance issues. See 'Configuring a trend' in the chapter on 'Group and trend displays' in the Server and Client Configuration Guide.

Groups

You can make it easier for operators to interpret system activity by grouping related points.

Each group can contain up to eight points, and each point in the group has its own faceplate that shows the values of the major parameters.



Group 451 Furnace group View As Group Detail

RC100	HTTK4FLW	RC102	MX2BP	RC104	BL101P10	RC108	TANKLVL101
Furnace control	Holding tank + Flow	Furnace control	Mixer speed	Furnace control	Slurry pump	Furnace control	Tank level
100.00	1000.00	100.00	100.00	100.00	100.00	100.00	100.00
B/L	EU	B/L	rev/s	B/L	L/s	B/L	L
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
PV High	PV HiHigh	PV High		PV High	PV High	PV High	PV HiHigh
SP 0.00 EU	SP 0.00 EU	SP 0.00 EU	SP 0.00 EU	SP 0.00 EU	SP 0.00 EU	SP 0.00 EU	SP 0.00 EU
PV 87.00 EU	PV 87.00 EU	PV 88.00 EU	PV 87.00 EU	PV 82.00 EU	PV 88.00 EU	PV 82.00 EU	PV 88.00 EU
OP 0.00 %	OP 0.00 %	OP 0.00 %	OP 0.00 %	OP 0.00 %	OP 0.00 %	OP 0.00 %	OP 0.00 %
MD MAN	MD MAN	MD MAN	MD MAN	MD MAN	MD MAN	MD MAN	MD MAN

Figure 13: Typical group

Related topics

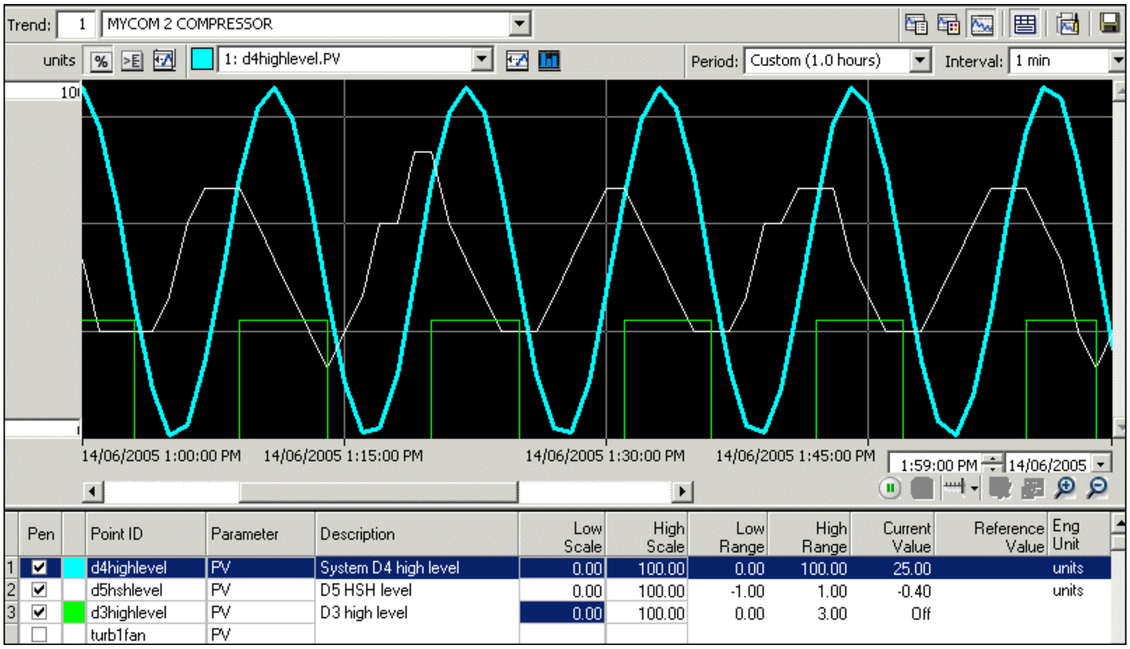
"System displays" on page 120

Trends

Trends display historical process values in a graphical manner. In many instances, trends provide operators with the best means of understanding system activity.

Depending on your database size, you can define up to 1,000 trends.

In order to make a trend meaningful, you need to select the appropriate type of history collection for each point parameter. For example, you need fast history for rapidly changing parameters, but extended history for slowly changing ones.



Trend: 1 MYCOM 2 COMPRESSOR

1: d4highlevel.PV

Period: Custom (1.0 hours) Interval: 1 min

	Pen		Point ID	Parameter	Description	Low Scale	High Scale	Low Range	High Range	Current Value	Reference Value	Eng Unit
1	☑	🟦	d4highlevel	PV	System D4 high level	0.00	100.00	0.00	100.00	25.00		units
2	☑		d5hshlevel	PV	D5 HSH level	0.00	100.00	-1.00	1.00	-0.40		units
3	☑	🟩	d3highlevel	PV	D3 high level	0.00	100.00	0.00	3.00	Off		
	☐		turb1fan	PV								

Figure 14: Typical trend

A standard trend displays historical data for up to 32 points as line graphs. In addition to the line graph, you can choose to display numeric history for the points in the trend as well as events associated with the points in your trend.

You can configure your trend so that the data is displayed as:

- A bar graph for up to three points
- An X-Y plot for two analog points, with one point's values plotted against the other.

Related topics

“System displays” on page 120

Scanning strategy

Scanning is the process by which the server reads from/writes to memory locations in controllers other than Process Controllers.

Each item of controller data to which the server needs read/write access is defined in the server as a point parameter. For example, the temperature of a boiler would typically be represented in the server as the PV (process variable) of an analog point.

An efficient scanning strategy provides the required level of monitoring and control, while keeping system load to a minimum.

Issue	Comments
Basic principles	Ensure that your strategy conforms to the basic principles.
Scanning techniques	Use scanning techniques that are appropriate to your needs.
Scan optimization	Optimize your scanning strategy, so that you minimize the load on the server.

Related topics

“Controllers” on page 69

Basic principles of scanning

Keep these two basic scanning principles in mind when designing your scanning strategy:

1. **Limit control to starting/stopping processes**

   The Experion server is not designed to be included in control loops—potential communication delays and heavy server loads may result in unreliable system activity. (The Experion server is designed primarily to collect data, and to present it in a meaningful way to users.)
2. **Limit data extraction to useful information**

   You should only extract data from controllers that is useful to operators, or is required for a specific purpose (trending, auditing, and so on).

Scanning techniques

Experion supports the following *scanning* techniques. (Scanning is the process by which the server requests point parameter values from controllers.) You can use several scanning techniques on the same controller, providing they are supported by that controller.

Scanning technique	Comments
Demand	The server only scans a point parameter when requested by an operator, a report, or an application. For more information about demand scanning, see the topic titled "Demand scanning" in the "Points" section of *Server and Client Configuration Guide*.
Dynamic	The server performs 'Once-off' dynamic scanning, accelerated dynamic scanning, or periodic dynamic scanning when an operator calls up a display or requests it for a controller. For more information about dynamic scanning, see the topic titled "About dynamic scanning" in the "Points" section of *Server and Client Configuration Guide*.

Scanning technique	Comments
Exception	The server polls the controller for any change-of-state data. Exception scanning is thus triggered by events, not time. Exception scanning is: • Not supported by all controllers • More difficult to implement than periodic scanning because it usually requires additional logic in the controller, additional configuration in Experion, or both
Periodic	The server scans a point parameter at the specified interval. For example, if a parameter's scan period is 15 seconds, the server scans the associated controller every 15 seconds for the parameter's value. You can choose from a range of standard scan periods, ranging from seconds to minutes, and you can assign a different scan period to each parameter. Periodic scanning: • Is supported by most controllers • Is simple to implement • Places a predictable, but potentially heavy, load on the server
Scheduled	The server scans a point parameter at scheduled periods. Electronic Flow Measurement (EFM) only. For more information about Electronic Flow Measurement, see the "Configuring Electronic Flow Measurement (EFM)" section of *Server and Client Configuration Guide*.

Unsolicited messaging

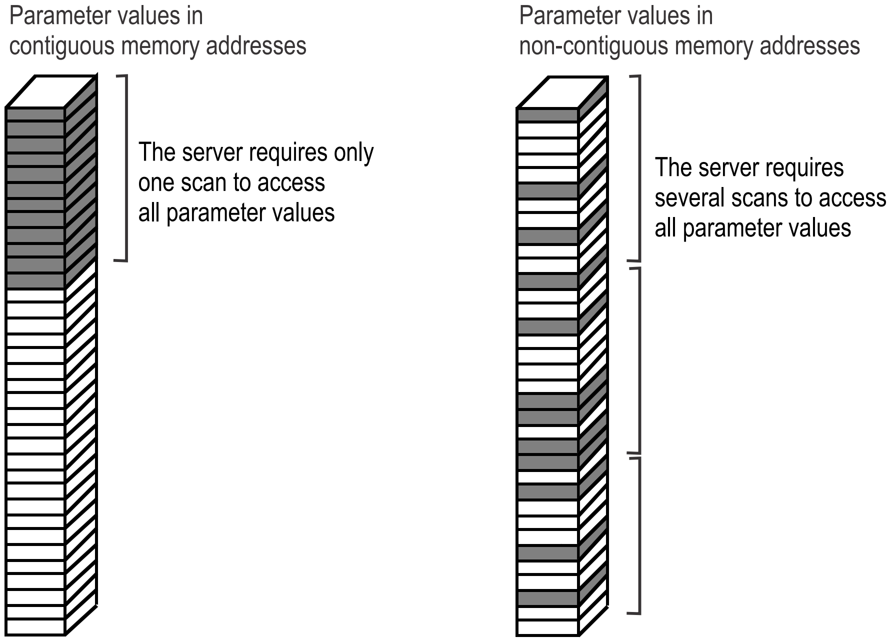
Some controllers support *unsolicited messaging*, where the controller, rather than the server, initiates a communications session. Unsolicited messaging can substantially reduce communications traffic, especially if the values do not change frequently.

Check the manufacturer's documentation to determine whether a controller supports unsolicited messaging.

Scan optimization

To optimize scanning:

- Use unsolicited messaging if the controller supports this feature, and values change infrequently.
- Use periodic scanning if values change frequently.
- Choose a scanning period appropriate to the values being scanned. For example, you do not need to scan a temperature every 5 seconds if it changes only slightly over an hour.
- Minimize the number of scan packets as follows:
  - Specify the minimum number of scan periods for a given controller because the server requires a separate scan for each scan period. For example, you might only need two scan periods for a particular controller: a short one for a few critical values, and a long one for all other values.
  - For each scan period you use, specify the longest period that is acceptable to your needs.
  - Arrange parameter value addresses so that they occupy contiguous addresses in the controller's memory, as shown in the following figure. If parameters occupy contiguous addresses, the server can access many parameters in a single scan—the exact number is controller-specific.


Parameter values in
contiguous memory addresses
The server requires only
one scan to access
all parameter values
Parameter values in
non-contiguous memory addresses
The server requires
several scans to access
all parameter values

Estimating the number of points required

Based on your analysis of your system and the role that you want Experion to perform, estimate the number of points you need to define. Use this figure, with an appropriate safety margin, to determine your licensing requirements.

Remember that the composite nature of Experion points means that you do not need one point per I/O value.

System Status Network tree

This section describes Network Tree planning considerations.

Topic	Go to
About the System Status Network tree	"About the System Status Network tree" on page 92
About System Event server and System Performance Server	"About System Event Server and System Performance Server" on page 93
Identifying a network topology	"Identifying a network topology" on page 94

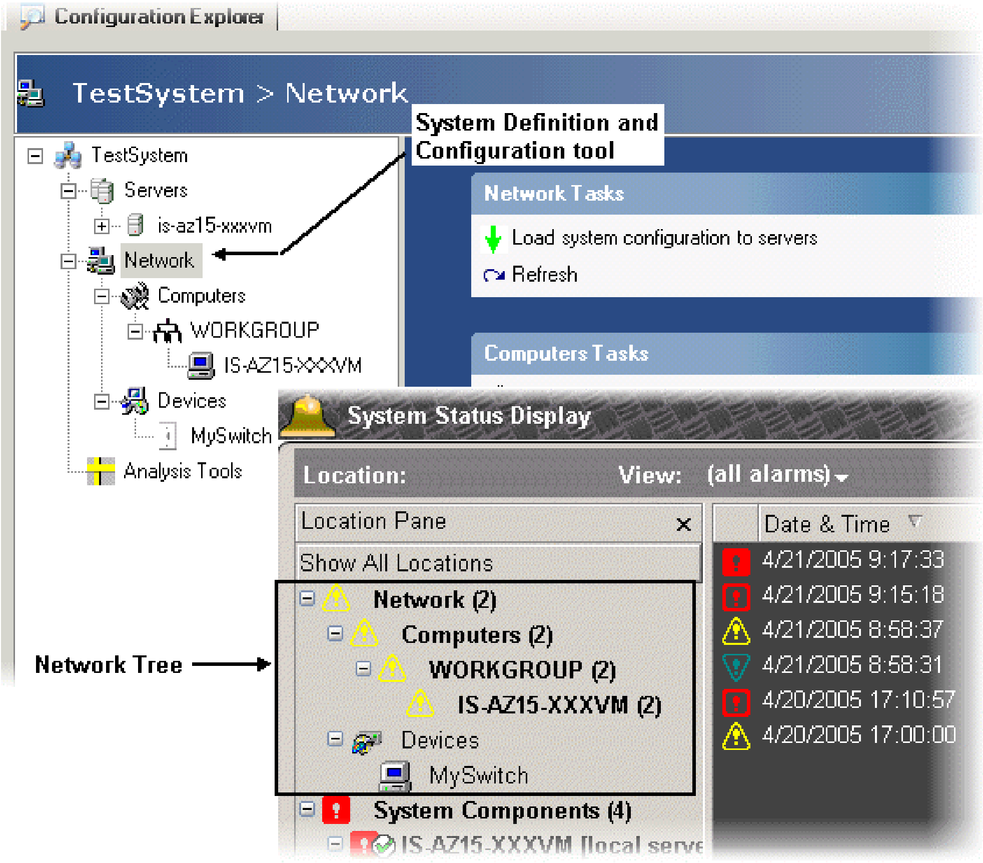
Related topics

"About the System Status Network tree" on page 92
"About System Event Server and System Performance Server" on page 93
"Identifying a network topology" on page 94

About the System Status Network tree

This section describes the Network tree planning considerations so that you are able to view computers and network equipment and their events from the System Status display. You use specific tasks in Configuration Studio to define network equipment. After you download these definitions, the Network tree in the System Status display is built and visible to operators with the appropriate scope of responsibility assignment.

In order to view event and performance data for the items appearing in the Network tree, you deploy the Experion System Event Server and System Performance Server.



About System Event Server and System Performance Server

The System Event Server (SES) is an Experion system component that issues Windows events as OPC alarms or events to a subscribing OPC client such as the System Status Display. The System Status display shows Windows system events through the use of the SES. The SES is integrated with the Experion Alarm and Event subsystem. The integration means, for example, that an operator can acknowledge a system alarm from the System Status display in the same manner that a process alarm is acknowledged on the Alarm Summary display.

The System Performance Server (SPS) is an OPC Data Access server that retrieves performance and configuration information and allows it to be integrated into operator displays and process applications in a manner consistent with process data access. This kind of information is vital for system monitoring and problem analysis. While third-party tools provide some trending and analysis of computer and network performance information, the SPS provides capabilities that integrate this information into the process control environment.

Note that the scope of SPS is per cluster. By default, all computers added to the network tree in Configuration Studio are automatically assigned to the server that is hosting the Enterprise Model Database (EMDB). These computers need to be reassigned in the multiple cluster server EMDB.

When multiple clusters (or even domains, workgroups or organizational units) are covered in a single EMDB, it is necessary to assign computers to the appropriate SPS . In all cases, this is the local Experion server providing that cluster.

For more information, see the *System Management Configuration Guide*.

Identifying a network topology

Several topologies are shown in this section to illustrate System Status Network tree planning considerations. The topologies include:

- Workgroup
- Domain with no Organizational Units (OUs)
- Domain with OUs
- Multiple domains

Attention

If you are planning to support a Network tree in a Windows domain environment, the following sections imply that you have Active Directory and Dynamic DNS already configured. The topologies are narrowly focused on planning considerations for the System Status display Network tree. For information regarding network and security best practices for Experion systems, refer to the *Network and Security Planning Guide*.

Related topics

"Workgroup topology" on page 94

"Domain with no Organizational Units (OUs)" on page 95

"Domain with Organizational Units (OUs)" on page 96

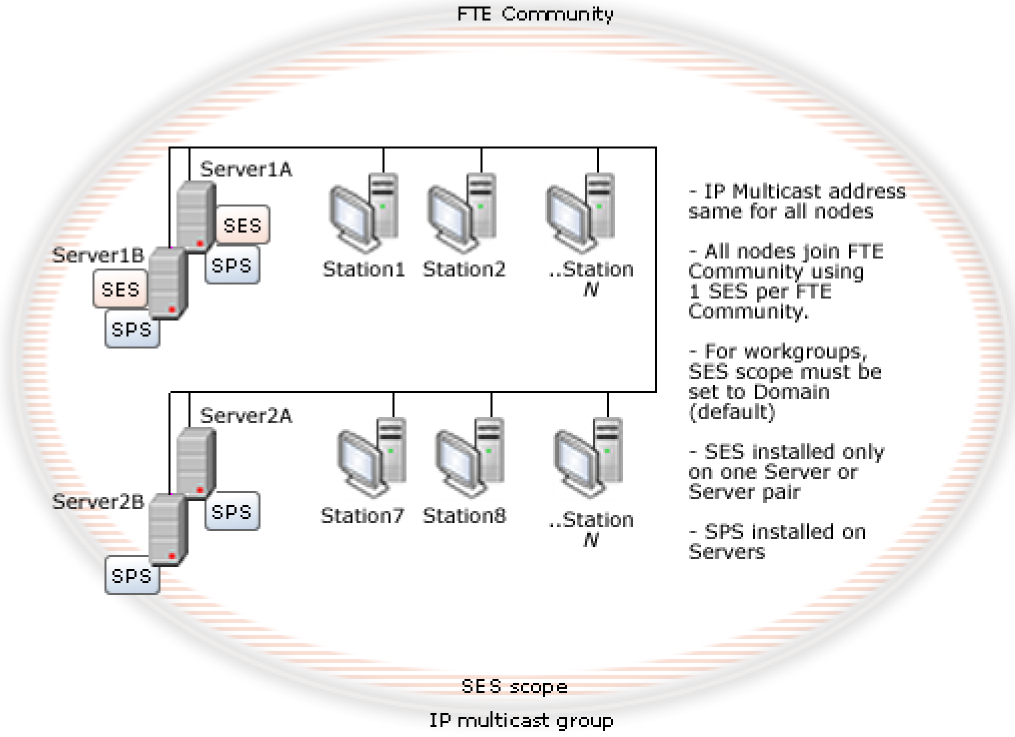
"Multiple domains or multiple workgroups" on page 96

"SES event notification behavior" on page 98

"Network tree planning summary" on page 98

Workgroup topology

In the following figure, a workgroup topology is shown to illustrate planning considerations to support event notifications to the System Status display and its Network tree.

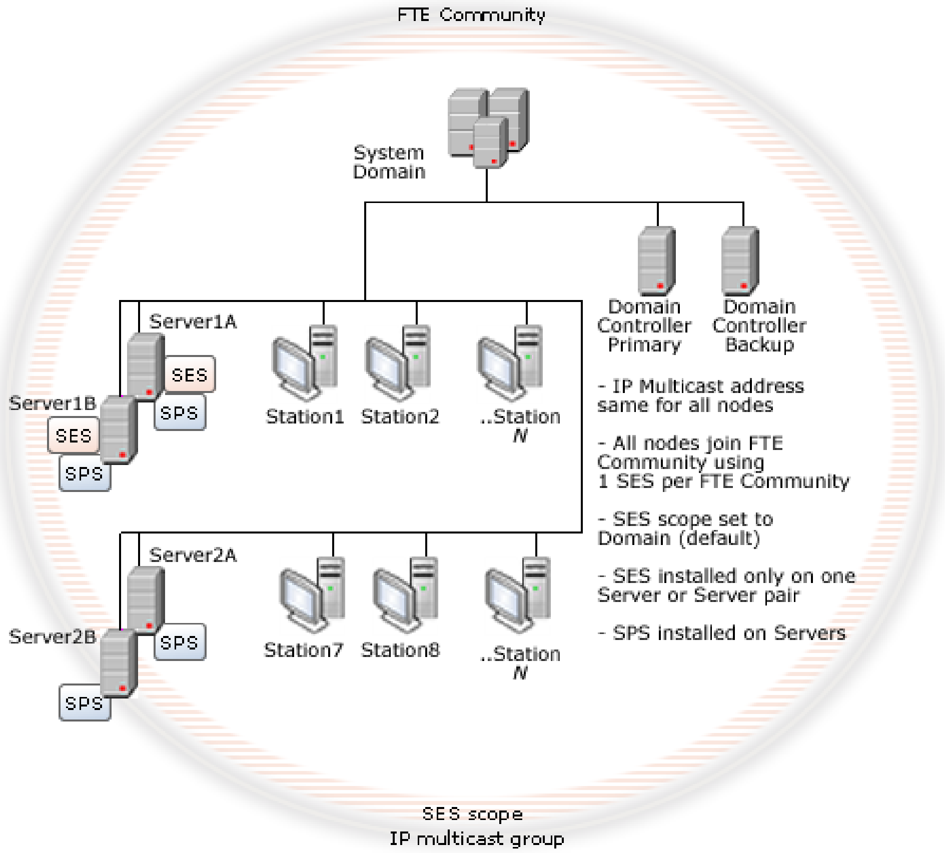

FTE Community
Server1A
SES
SPS
Server1B
SES
SPS
Station1
Station2
..Station N
Server2A
SPS
Server2B
SPS
Station7
Station8
..Station N
- IP Multicast address same for all nodes
- All nodes join FTE Community using 1 SES per FTE Community.
- For workgroups, SES scope must be set to Domain (default)
- SES installed only on one Server or Server pair
- SPS installed on Servers
SES scope
IP multicast group

In this example:

- Redundant Servers support several Stations in the same workgroup topology.
- All nodes belong to the same IP multicast group using the same IP multicast address, which forms them into an FTE Community.
- System Performance Server (SPS) should be installed on all Experion servers.
- The System Event Server is installed on only one of the redundant server pairs.
- The System Event Server scope of '*domain*' (its default setting) is appropriate for this workgroup topology.
- When there are multiple Experion servers in an FTE Community, the Distributed System Architecture (DSA) option should be enabled so that the servers can share SES event data.
- Each server in the FTE Community subscribes to the server hosting the SES.

Domain with no Organizational Units (OUs)

In the following figure, a simple domain with no Organizational Units (OUs) topology is shown to illustrate planning considerations to support event notifications to the System Status display and its Network tree.


FTE Community
System Domain
Domain Controller Primary
Domain Controller Backup
Server1A
SES
SPS
Server1B
SES
SPS
Station1
Station2
..Station N
Server2A
SPS
Server2B
SPS
Station7
Station8
..Station N
- IP Multicast address same for all nodes
- All nodes join FTE Community using 1 SES per FTE Community
- SES scope set to Domain (default)
- SES installed only on one Server or Server pair
- SPS installed on Servers
SES scope
IP multicast group

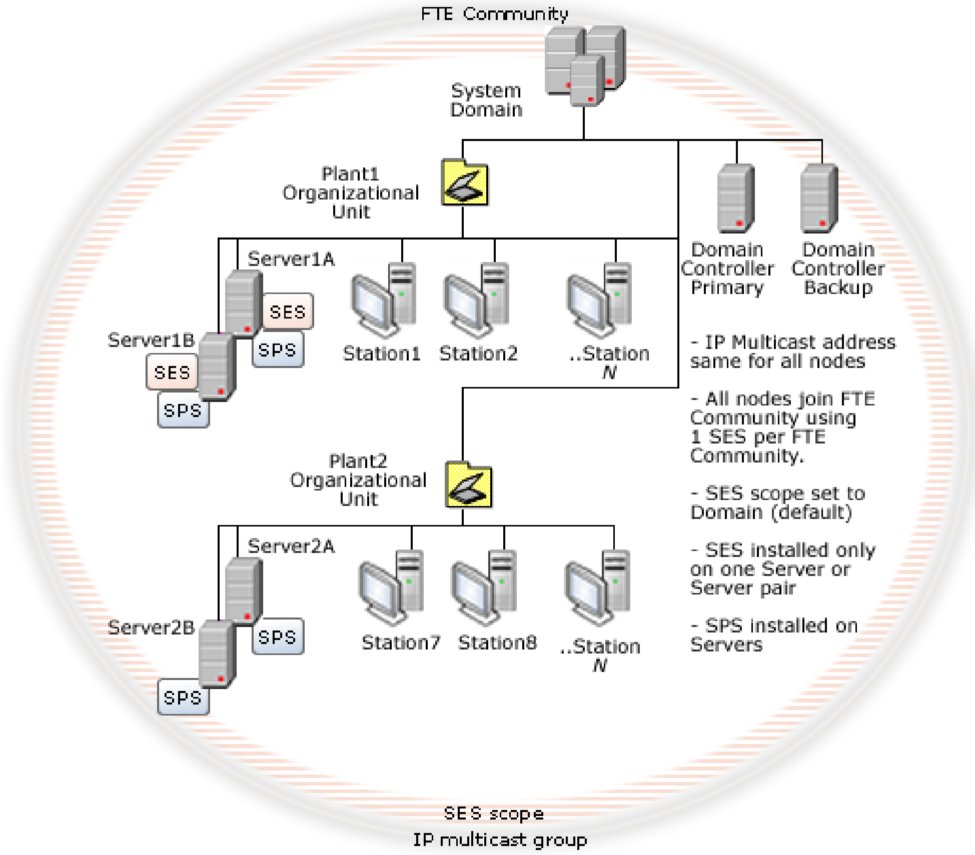
In this example:

- Redundant servers support several Stations in the same domain topology.
- All nodes belong to the same IP multicast group using the same IP multicast address, which forms them into an FTE Community.
- System Performance Server (SPS) should be installed on all Experion servers.
- The System Event Server is installed on only one of the redundant server pairs.
- The System Event Server scope of '*domain*' (its default setting) is appropriate for this topology.

- When there are multiple Experion servers in an FTE Community, the Distributed System Architecture (DSA) option should be enabled so that the servers can share SES event data.
- Each server in the FTE Community subscribes to the server hosting the SES.

Domain with Organizational Units (OUs)

In the following figure, a domain topology using Organizational Units (OUs) is shown to illustrate planning considerations to support event notifications to the System Status display and its Network tree.

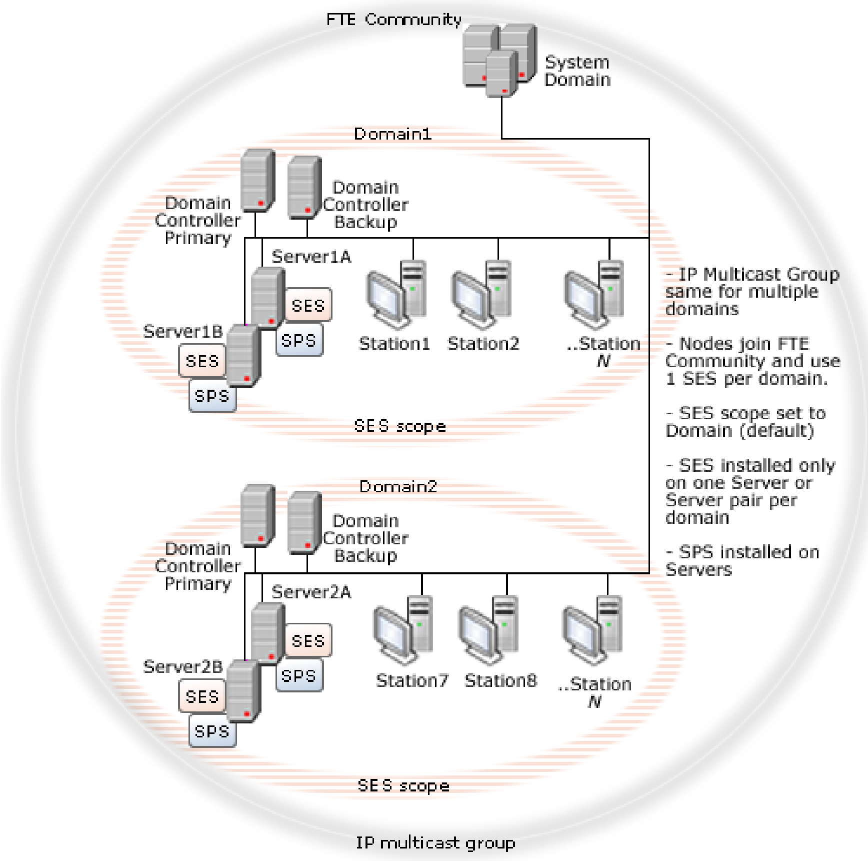

FTE Community
System Domain
Plant1 Organizational Unit
Server1A
SES
SPS
Server1B
SES
SPS
Station1
Station2
..Station N
Domain Controller Primary
Domain Controller Backup
- IP Multicast address same for all nodes
- All nodes join FTE Community using 1 SES per FTE Community.
- SES scope set to Domain (default)
- SES installed only on one Server or Server pair
- SPS installed on Servers
Plant2 Organizational Unit
Server2A
SPS
Server2B
SPS
Station7
Station8
..Station N
SES scope
IP multicast group

In this example:

- Redundant servers support several Stations in OUs in the same domain topology.
- All nodes belong to the same IP multicast group using the same IP multicast address, which forms them into an FTE Community.
- System Performance Server (SPS) should be installed on all Experion servers.
- The System Event Server is installed on only one of the redundant server pairs.
- The System Event Server scope of '*domain*' (its default setting) is appropriate for this topology.
- When there are multiple Experion servers in an FTE Community, the Distributed System Architecture (DSA) option should be enabled so that the servers can share SES event data.
- Each server in the FTE Community subscribes to the server hosting the SES.

Multiple domains or multiple workgroups

In the following figure, a topology using multiple domains is shown to illustrate planning considerations to support event notifications to the System Status display and its Network tree. A topology of multiple workgroups within the same multicast group should follow these same planning considerations.


FTE Community
System Domain
Domain1
Domain Controller Primary
Domain Controller Backup
Server1A
SES
SPS
Server1B
SES
SPS
Station1
Station2
..Station N
SES scope
- IP Multicast Group same for multiple domains
- Nodes join FTE Community and use 1 SES per domain.
- SES scope set to Domain (default)
- SES installed only on one Server or Server pair per domain
- SPS installed on Servers
Domain2
Domain Controller Primary
Domain Controller Backup
Server2A
SES
SPS
Server2B
SES
SPS
Station7
Station8
..Station N
SES scope
IP multicast group

In this example:

- Redundant servers support several Stations in each workgroup or domain topology.
- All nodes belong to the same IP Multicast group using the same IP Multicast address, which forms them into an FTE Community.
- System Performance Server (SPS) should be installed on all Experion servers.
- The System Event Server is installed on one of the redundant server pairs in each workgroup or domain.
- The System Event Server scope of '*domain*' (its default setting) is appropriate for these topologies.
- When there are multiple Experion servers in an FTE Community, the Distributed System Architecture (DSA) option should be enabled so that the servers can share SES event data.
- Each server in the FTE Community subscribes to the server hosting the SES in each workgroup or domain.
- If Server1 and Server2 are DSA connected, duplicate FTE event notifications occur. To eliminate these duplicate FTE event notifications, remove the FTE event filter file (`FTEFilter.xml`) from all but one SES pair.

  The FTE event filter file is located at `C:\HWIAC\Filters\FTEFilter.xml<data folder>\Honeywell\ProductConfig\Filters\FTEFilter.xml`.

  Where `<data folder>` is the location where Experion data is stored. For default installations, `<data folder>` is `C:\ProgramData`. The `C:\ProgramData` folder is a system folder, which means that it is only visible if you select the **Show hidden files, folders, and drives** option button in the **Folder Options** dialog box. To change this setting in Windows Explorer, click **Organize** > **Folder and search options**, and then click the **View** tab.

SES event notification behavior

Events are gathered by the System Event Provider (SEP), part of system management runtime. The events are synchronized on all nodes within the FTE Community and domain. The SES is used to convert these events to an OPC event usable by the Experion server.

If the SES fails, an event is generated by the Experion server indicating that it has lost the connection to the SES. System Events are not viewable until the SES is restarted, or the Experion server fails over to the redundant server. When SES is restarted, it reads all events from the SEP and makes them available to the server. No event loss occurs. If the SEP fails, the SES reports loss of connection with its data source (SEP), and no system events are available. When the SEP is restarted, it synchronizes with another node which has the full set of events. In addition, new events that occurred during the time that SEP was unavailable are read and added to the event list. No event loss occurs.

Network tree planning summary

Honeywell recommends that one of the above topologies be chosen when implementing Experion. Utilizing these topologies will allow for simplified configuration and cater to future system expansion. System expansion is simplified by simply configuring new nodes to use the same IP Multicast address and the same SES already implemented. The planning considerations are summarized in the following sections.

Attention

It is strongly recommended that you implement a topology featuring one SES per cluster server.

For information on implementing this topology, see Technote 234 available on Honeywell HPS Online Support website.

Recommendations

For typical domain and workgroup environments, establishing all nodes to use the same multicast address and SES scope provides you with the most ease of use and flexibility for future growth.

Location of SES

Only one System Event Server (SES) must be installed per FTE Community, per domain. If the Experion servers are redundant, the SES is installed on both servers. The nodes access the SES in their domain as defined from the FTE Community Settings task in Configuration Studio.

Scope of SES

The SES scope default setting of '*domain*' provides synchronization of system events across the domain as restricted by the multicast community.

Enabling event notification for SES

Events are enabled for capturing through the use of the event filter configuration tool. Event filter files are installed on the nodes where the events defined (in the filter file) are logged. For example, the TPN Server event filter file is installed on the node with the TPN Server. FTE filter files are installed with the SES. By default, all FTE events are collected based on the view of the SES node.

DSA

The Distributed System Architecture (DSA) option should be enabled so that multiple servers in an FTE community can share SES event data. Only one server (pair) in the DSA can have the SES component installed and active. The remaining servers need to subscribe to the server (pair) hosting SES to access all system events.

When you first define a server and download this server definition to other servers in the system, the default subscription for the server is disabled and it does not participate in the DSA. After you define a server, you must enable the DSA connection with other servers so that SES event data can be shared.

You need to consider these DSA connections when determining the number of DSA connections to license.

Location of SPS

SPS should be installed on all Experion servers.

Notifications from switches and routers

Any switches or routers from which notifications are to be received are configured to send those notifications to the server nodes on which the SNMP Monitor has been installed.

Auxiliary Status display

SES and SPS auxiliary displays are installed automatically on all Experion nodes as part of the system management software. The Auxiliary Status display should be installed on any other clients needing view of SES or SPS auxiliary status. Other managed component auxiliary displays need to be installed (for example, TPN Server, Redirection Manager) if used within the system.

Alarms and events

This section describes how to determine your alarm and event requirements.

Issue	Comments
Designing alarm systems	Consider and plan your alarm strategy.
Dynamic Alarm Suppression	Decide whether you want to enable *Dynamic Alarm Suppression* to deal with high alarm situations like unit trips by temporarily but automatically removing certain 'flow-on' alarms from normal alarm views.
Alarm and alert shelving	Decide whether you want to enable *alarm shelving*. Enabling alarm shelving allows operators to temporarily remove alarms from normal alarm views. For example, if some equipment is out of action for maintenance, operators can temporarily remove alarms associated with this equipment from their current alarm view. Alerts can also be shelved in the same way.
Alarm prioritization	Formulate a set of rules and guidelines for prioritizing alarms.
Alarm annunciation	Consider your alarm annunciation needs, such as alarm paging, buzzers and horns.
Alarm groups	Decide whether you want to create *alarm groups*. Alarm groups provide an alternative way of viewing alarms, which is not related to your asset model. For example, you could create an alarm group to monitor alarms on all electrical motors in your plant, regardless of their locations within the asset model.
Alarm Tracker	Decide whether you want to create *alarm trackers*. An alarm tracker provides an asset-based, graphical view of alarms over time that helps operators identify and respond to abnormal situations like alarm floods. Alarm Tracker is an Experion license option.
Alerts	Consider using alerts for notifications whose urgency and priority are not high enough to be alarms.
Messages	When defining an alarm for certain types of standard point (status, analog and accumulator), you can assign an appropriate *message* that helps operators understand the significance of the alarm. (The Alarm Summary display only shows basic details—such as the point ID, date/time and priority—which may not be sufficient for operators.)
Events	Consider your *event* storage and archiving needs. (Events include changes in alarms, changes in point status and operator actions.)

Related topics

“Planning and designing your alarm system” on page 103

“Dynamic Alarm Suppression” on page 107

“Alarm and alert shelving” on page 109

“Alarm prioritization” on page 111

“Alarm annunciation” on page 113

“Alarm groups” on page 114

“Alarm trackers” on page 115
“Alerts” on page 116
“Messages” on page 117
“Events” on page 118

Planning and designing your alarm system

It is generally agreed that the purpose of an alarm system is to announce to operators that something is abnormal and that action is (or may be) required in response to that situation.

In an ideal world, operators would only see alarms for process events and states that require specific operator action within a relatively short time. However, even in the most well-designed alarm system, operators may find that the primary alarm summary display includes alarms that are of no immediate operational relevance.

Other problems that can occur in alarm systems are:

- Excessive standing alarms: When alarms are continually on the primary alarm summary display, operators often learn to ignore these alarms. This makes it less likely that operators will see alarms that really do require action.
- Alarm floods: When alarms are raised so quickly that operators do not have enough time to react to them, important alarms that require a prompt response become obscured. In situations like this, the alarm system can hinder rather than support effective operations.

A well-planned and thoughtfully designed alarm system that encompasses a range of strategies and solutions can, however, minimize the number and type of alarms that prevent operators from focusing on and dealing with the most urgent or important alarms at any given time.

The following topics describe:

- Honeywell product solutions that support effective alarm strategies
- Factors that contribute to excessive alarms
- Strategies for dealing with such factors

Honeywell products that support effective alarm strategies

Consider the following Honeywell products when planning your alarm system and strategies for dealing with abnormal situations.

Alarm Configuration Manager

Alarm Configuration Manager (ACM) is a product that is separate but complementary to Experion. The key feature of ACM is its capacity for “holding” designed alarm settings as the master alarm database, and through audit and enforcement, providing a “safety net” to ensure that changes are temporary and that the engineered alarm configuration can always be restored.

With ACM, settings like alarm trip points, priorities, and the disable status can be driven by planned equipment operating modes. ACM also provides tools that support work processes for alarm rationalization and maintenance.

Experion Dynamic Alarm Suppression

Experion Dynamic Alarm Suppression (DAS) is ideal for reducing excessive alarms arising from unplanned compound events like equipment trips. It provides additional capability and convenience above and beyond the current mechanisms of controller logic. Although DAS can be applied to suppress alarms from planned equipment outages, ACM provides a more complete solution for planned outages.

Experion alarm or alert shelving

Experion alarm or alert shelving allows operators to temporarily remove alarms or alerts from the main display when they are nuisance or extraneous alarms or alerts that are not filtered out by other mechanisms.

Other Experion functionality

Within Experion there is a range of other functionality that enables operators to deal with excessive or extraneous alarms. For example, operators can temporarily disable alarms. There is also an Experion alarm configuration option that, when enabled, allows operators at a specified security level to temporarily suppress the audible annunciation of non-urgent alarms.

To help deal with alarm bursts and floods, operators can also use the Alarm Tracker pane on the Experion Alarm Summary. Alarm Tracker is an Experion license option that provides a graphical, time- and asset-based view of alarms. By making it easier for operators to identify “clusters” of alarms on assets within an operator’s scope of responsibility, an alarm tracker helps operators to respond more quickly to excessive process alarms.

While such functionality provides a good basis for dealing with situations that can lead to excessive alarms, ACM, DAS and alarm shelving provide extra capability that can significantly reduce the number of excessive alarms that have no operational relevance. Together all of these tools provide engineers and operators with a good set of complementary functions for reducing excessive alarms in the case of both standing alarms and alarm floods. You can use some or all of these tools based on site needs.

For more detailed information about the functionality described above, see the *Server and Client Configuration Guide*.

Factors that contribute to excessive alarms

The main causes of excessive alarms (and alarms that have no immediate operational relevance) include:

- Alarm design, for example, when the alarm system is not properly rationalized to reduce alarm floods and excessive standing alarms.
- Maintenance issues, for example, when the control system is being modified or when sensors are taken out of service for repair and the alarms related to those sensors are taken out of service at the same time. If no preemptive action is taken in relation to those alarms, standing (and possibly spurious) alarms can appear during repair and testing.
- Changes in equipment mode, for example, when there is a change in the product being manufactured and different operating parameters are required.
- Compound events, for example, when there is a superseding event, like a compressor trip, or when there are multiple related alarms.
- Other causes. This category covers a range of other causes that need to be addressed in a different manner to the causes listed above.

The likely impact of these factors is summarized in the following table.

Cause	Most likely consequence	
	Standing alarms	Alarm floods
Alarm design	X	X
Maintenance	X	
Equipment mode	X	
Compound event		X
Other causes	X	X

Dealing with excessive alarms

Recommended strategies for dealing with excessive alarms are described below.

Reducing unnecessary alarms through good design and alarm rationalization

Good alarm design through effective alarm rationalization is considered a best practice strategy for dealing with excessive alarms resulting either from alarm floods or high numbers of standing alarms.

Effective alarm rationalization removes alarms that do not meet the criterion of a necessary alarm. It does this by ensuring that:

- Only those events or states that require specific operator action within a short time (for example, 15–30 minutes) are configured as alarms.
- If no operator action is required, then that event or state should either:
  - Not be annunciated to the operator, or
  - Be configured as an alert or notification rather than an alarm.
- The attributes of the remaining true alarms (for example, the trip point, priority, dead-band, alarm on/off delay and range extension) are set to provide the best compromise between enabling quick operator action and avoiding nuisance alarms.

One approach to alarm rationalization is to use controller logic to reduce standing alarms and flooding. For example, you might use controller logic to:

- Combine multiple similar alarms into a single robust alarm (for example, by using logic to combine alarms from temperatures on the side of a tank), or
- Cover changing equipment modes, or
- Suppress consequential alarms.

On the other hand, you might consider using Alarm Configuration Manager (ACM) and Dynamic Alarm Suppression (DAS) as more effective alternatives to customized controller logic.

Despite best efforts to rationalize alarms, alarm systems can still suffer from alarms that are of no immediate operational relevance. This might happen, for example, when the documented operator action may not apply due to some circumstance not accounted for in the alarm design process. Rationalization can therefore not entirely prevent excessive standing alarms or alarm floods. Nevertheless it is a key component of (and indeed the very foundation of) a well-designed and effective alarm system.

Dealing with alarms related to maintenance and repair

Often, operators put the point into the Disable or Journal-only state when this occurs, or manipulate some other alarm attribute, such as alarm priority. However, putting an alarm into “maintenance” means that this alarm will no longer protect the process.

The site alarm strategy should therefore identify a work process to:

- Ensure that the loss of the alarm during this period will not cause excessive process risk, and
- Deploy alternative precautions if deemed necessary.

ACM provides a formal way to enforce such a work process.

Another option is to use Experion alarm shelving to:

- Shelve the alarm
- Set the shelving reason to “Maintenance”
- Define the scope of responsibility to ensure that appropriate supervision takes place.

Dealing with alarms related to changes in equipment mode

Even if an alarm system is well rationalized, excessive alarms may arise because a given piece of equipment may operate differently in different situations. This happens sometimes in continuous processes, and very often in batch processes. To deal with this, alarm rationalization must put the alarm trip points at their most conservative settings, possibly resulting in large numbers of standing alarms in situations where those alarm settings are too aggressive.

A good solution is to have a controlled way to change alarm settings by equipment mode. This can be done by what is sometimes called static alarm suppression or mode-based alarming. Options here include:

- Controller logic, where, for example, sequences can be used to manipulate alarm attributes to change trip points, priorities, the journal-only state and the disable/journal-only status appropriately as batch phases progress.

- ACM operating modes which provide a good, well-documented means for configuring and changing alarm settings (alarm enable state, the disable/journal-only status, trip points, and priorities) for each operating mode on an asset or piece of equipment. This allows the alarm settings to be better tailored to the specific operating situations, resulting in far fewer standing alarms.

  Note that while DAS can be useful for suppressing alarms on a device that is out of service, it cannot adjust alarm properties like trip points.

CAUTION

Any solution that affects safety-related or otherwise critical alarms should be carefully considered as well as carefully designed and implemented.

Dealing with compound events: consequential alarms or other multiple alarm situations

Alarms are generally configured to notify operators that action is required in an otherwise normal or quiescent process. However, equipment failure or process upsets can lead to many more alarms than the operator can react to, while only a few of those alarms (for example, "compressor trip") indicate what the operator's main focus should be.

Controller logic can be configured to deal with such situations, but this involves extra engineering costs, and has long-term maintenance risks.

DAS is specifically designed to handle this problem in a clear, documented way. It is similar to "contact cutout" in TPS in that it operates independently of other alarm suppression mechanisms, such as disable and journal-only, which may be manipulated by ACM or by sequences. But it is superior to contact cutout in its flexibility; and it is superior to both contact cutout and controller logic in operator presentation, logging, and documentation. In most cases, DAS can replace the controller logic which may have been configured to meet this need. However, it is recommended that DAS strategies remain simple and straightforward. In more complex cases, controller logic may be used together with DAS to provide the optimal solution. For instance, controller side suppression logic may be useful where sequence of events is deemed important and there is a delay between the reading of the value and alarm generation, as sometimes happens with some server-generated SCADA alarms.

Dealing with alarms resulting from other factors

No matter how much engineering goes into the alarm system, there will always be the potential for alarms that, for a short period of time, are not relevant to an operator, and that the operator would therefore like to hide from the primary alarm summary. Such alarms could be due to a range of factors such as those outlined above, and might relate to alarm situations that have not been completely addressed by the alarm design process. Or they could arise in situations where the operator has taken appropriate action, and the process is recovering, but alarms are not expected to return to normal for some time.

Experion alarm shelving is designed to handle these cases directly, by allowing the operator to shelve alarms (that is, temporarily place selected alarms on the "alarm shelf" off the main display), but allowing these alarms to be quickly and easily called up for reference and crosschecking.

Dynamic Alarm Suppression

Dynamic Alarm Suppression (DAS) is an Experion license option that provides an automated way of temporarily removing alarms from the default (unfiltered) view of the Alarm Summary. Alarms are removed in accordance with a set of rules that you configure. By temporarily removing specific alarms from the Alarm Summary when pre-configured conditions are met, DAS helps operators to focus on the issue at hand or on other more critical conditions in the plant.

DAS is primarily intended to help operators deal with high-alarm situations like trips where multiple alarms related to the same event are triggered in quick succession. It can therefore be a useful strategy for dealing with "downstream" alarms resulting from equipment trips (or even unit shutdowns or startups). For example, if a pump shuts down or a compressor trips, you might want to use DAS to automatically suppress any consequential low-flow (or low-pressure) alarms.

Although suppressed alarms are hidden from the default (unfiltered) view of the Alarm Summary, the number of alarms currently suppressed is shown in the summary statistics at the bottom of the Alarm Summary, and operators can use the **(suppressed alarms)** view to see which alarms are currently suppressed.

DAS can be used for alarms on any of the following point types: CDA, SCADA, TPS, DSA, point server, or third-party OPC.

Attention

DAS should only be used to suppress alarms that are of no direct operational relevance to operators and that do not require an operator response at the time.

Before implementing DAS it is very important that you read the alarm design and application guidelines in the *Server and Client Planning Guide* as well as the configuration guidelines and scenarios in the *Server and Client Configuration Guide*.

Planning and application guidelines for Dynamic Alarm Suppression

Dynamic Alarm Suppression (DAS) is an advanced form of alarm management that should be designed, implemented and tested by appropriate individuals such as the engineers who are responsible for the equipment in question.

Before designing, implementing or modifying an alarm system, it is recommended that engineers familiarize themselves with industry standards such as the EEMUA's *Publication 191 Alarm Systems: A Guide to Design, Management and Procurement*, the ASM Consortium's guideline *Effective Alarm Management Practices*, and the ISA-18.2 standard *Management of Alarm Systems for the Process Industries*.

When planning your system, bear in mind the following:

- As a general principle, keep your DAS strategy simple and conservative to ensure that important alarms requiring operator attention are not inadvertently suppressed.
- A well-designed and well-managed alarm system is an important precondition for alarm suppression. It is therefore strongly recommended that, before implementing DAS, sites:
  - Rationalize alarms and reduce duplication as much as possible.
  - Implement management of change (MOC) for the alarm system. This is particularly important to ensure that a site's alarm suppression strategy is taken into account when, for example, equipment is changed or out for maintenance, or when systems are running in a mode other than the original design.
- In the absence of formalized MOC, it is important to have comprehensive and accurate documentation in place to ensure that subsequent changes in equipment and control strategy do not result in unforeseen (and potentially hazardous) consequences.
- Consider using DAS in conjunction with mode-based alarming using a tool like Alarm Configuration Manager (ACM). While mode-based alarming is not fast enough to deal with suppression, it can be effective for managing alarms under controlled scenarios like when bringing a unit back into service. (Note, however, that care needs to be taken when bringing a unit back into service as removing suppression too early could lead to alarm floods.)

For example, you could use ACM to define an out-of-service or shutdown mode that sets journal-only and other alarm attributes to ensure that any noise on the triggering signals during maintenance or repair does not translate to alarms. You could also use ACM to suspend enforcement on related tags, thereby allowing temporary changes such as the disabling of alarms.

- DAS is best suited for dealing with trips in small units or in fairly distinct equipment. If you want to use DAS for dealing with large scale unit or plant trips, create low-level (that is smaller and thus more easily managed) alarm suppression groups that can operate independently on individual units within the larger unit or plant.
- Although DAS could be used to manage alarm annunciation during planned shutdowns or start ups, changes to known plant states are better addressed with ACM.
- If your site currently uses controller logic, contact cutout, or other mechanisms to achieve suppression or shelving functionality, you might want to consider the advantages of using Experion DAS or Experion alarm shelving. Before making any significant change to your current alarm system, it is of course always important to consider the impact of such a change on operators.

Alarm and alert shelving

Alarm shelving is a form of manual suppression that enables operators to remove individual alarms from the main alarm summary display for a limited time.

Shelving is typically used by operators to hide “nuisance” alarms that are distracting them from other more important alarms. Although multiple alarms can be shelved at the same time, you can only shelve one alarm at a time.

Alarm shelving is most suitable for the following situations and scenarios:

- Dealing with stale or standing alarms such as those arising from instrument malfunction or faulty equipment awaiting repair.
- Background or nuisance alarms such as those arising from unusual weather conditions.
- Dealing with alarms that require action that may take time. For example, an operator may need to change a temperature set point for a process that takes two hours to effect the change. In a case like this, operators can shelve the alarm for two hours, knowing that if the alarm is re-annunciated after that time, there is still a problem that needs to be addressed.

Operators can shelve alerts as well as alarms. The following information about alarm shelving also applies to alerts.

How alarm and alert shelving works

- When an alarm is shelved, Experion automatically:
  - Acknowledges the alarm
  - Silences the alarm
- While alarms are shelved they can be viewed by using the **(shelved alarms)** view on the Alarm Summary or by choosing one of the filters on the Alarm Icon column that show shelved or hidden alarms.
- Depending on how shelving has been configured at a given site, shelved alarms generally do not reappear in the Alarm Summary until their shelving period expires or they are manually unshelved.
- If an alarm returns to normal while it is shelved, it remains shelved until its shelving period elapses or it is unshelved by the operator. When such an alarm is unshelved it automatically disappears from the alarm summary.
- If an alarm recurs while it is shelved, the alarm remains shelved and also remains acknowledged and silenced.

For more information about alarm shelving, see the “Configuring alarm shelving” topic in the “Configuring alarms, alerts, and messages” section of the *Server and Client Configuration Guide*.

What happens when a shelved alarm is suppressed?

If an alarm is either shelved or suppressed, it is hidden from the default view of the Alarm Summary.

Information about the shelved state of an alarm is maintained independently of information about the suppression state of an alarm. However, where an alarm is both shelved and suppressed, information about the suppression state of an alarm is considered to be more important (or of greater interest) than information about its shelving state. For example, in the display of alarm counts and alarm state icons on a custom display, information about an alarm’s suppression state takes precedence over information about its suppression state. See the following scenario for more about the precedence of suppression over shelving.

The following scenario illustrates what happens when an alarm on `POINTA01` has been defined as a “target alarm” in the suppression group `SG01`, and that alarm is currently shelved when suppression group `SG01` is activated.

- The alarm remains shelved until the shelving period expires (or until the alarm is manually unshelved).
- On the Alarm Summary, the alarm:
  - Is included in both the **(suppressed alarms)** and **(shelved alarms)** view.

If the alarm is unshelved while the suppression group is still active, it is removed from the **(shelved alarms)** view but stays in the **(suppressed alarms)** view until the suppression group is deactivated.

  - Shows the **Suppressed** icon (rather than the **Shelved** icon) in the alarm icon column.
  - Is included in the **Suppressed** count (but not the **Shelved** count) in the alarm statistics at the bottom of the Alarm Summary.

- On custom graphics:
  - If there is only one alarm condition currently existing on a point, and that condition is both shelved and suppressed:
    - The point alarm state shows the **Suppressed** icon.
    - The alarm is included in the **Suppressed** alarms count (but not the **Shelved** alarms count) on the point.
  - If there are two alarm conditions currently existing on a point, one shelved and one suppressed, the point alarm state shows the **Shelved** icon.
- On the Location pane of the Alarm Summary, the ToolTip for the asset alarm count:
  - Does not show the **Suppressed** count or the **Suppressed** icon even if the only nonzero alarm count is the **Suppressed alarms** count.
  - Shows the **Shelved** count and the **Shelved** icon if a shelved alarm is the most important alarm on that asset.

Alarm prioritization

It is essential that alarms are correctly prioritized so that operators are able to respond to alarms in a systematic manner. You therefore need to formulate a set of guidelines so that commissioning engineers assign the correct priority to each alarm condition. You also need to take into account 'cascading alarm' scenarios—for example, if a pump failure results in a pressure drop, the pump failure alarm requires a higher priority than the pressure alarm.

Experion prioritizes alarms at two levels:

- **Priority**. The priorities are: *Urgent*, *High*, *Low* and *Journal* (the default)
- **Sub-priority**. These range from *15* (highest) to *0* (lowest)

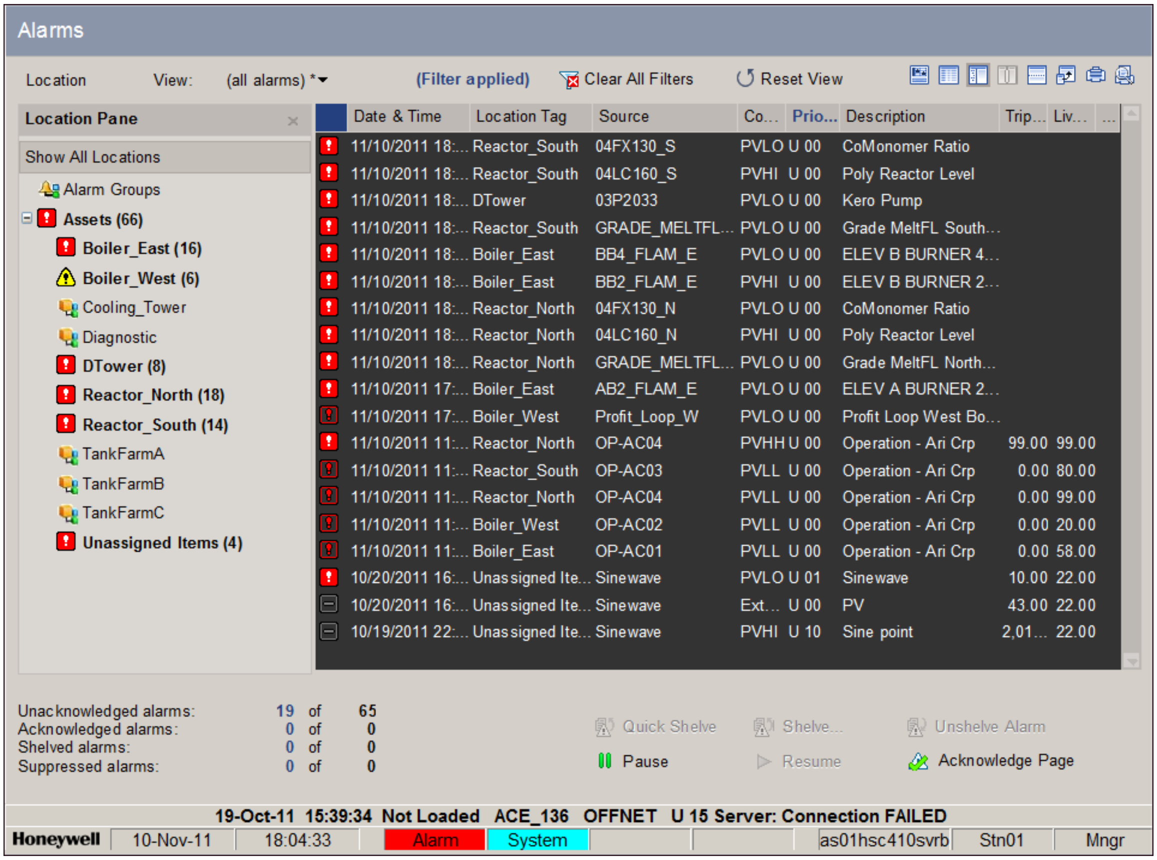
All alarms, except *Journal*, appear in the Alarm Summary and are therefore responded to by operators. All alarms, including *Journal*, are written to the event journal.

System alarms are assigned a Honeywell default priority and sub-priority. These can be adjusted at the server cluster level as required. For more information, see “Configuring system alarm priorities” in the *Server and Client Configuration Guide*.

Views

You can improve alarm management by creating appropriate *views* for operators. (A view shows a particular subset of alarms, and presents the details in a particular way.) The following figure, for example, shows an Alarm Summary that only lists urgent alarms. Note that when a filter has been applied to the Alarm Summary, the **(Filter applied)** indication appears to the left of the **Clear All Filters** button. For more information see the topic “Creating a view of a summary display” in the *Server and Client Configuration Guide*.

It is also possible to restrict the system alarms that are displayed, by selecting the minimum system alarm priority to be visible to the operator, console, Console Station, or Flex Station.



Alarms

Location View: (all alarms) * (Filter applied) Clear All Filters Reset View

Location Pane

Show All Locations

- Alarm Groups
- Assets (66)
  - Boiler_East (16)
  - Boiler_West (6)
  - Cooling_Tower
  - Diagnostic
  - DTower (8)
  - Reactor_North (18)
  - Reactor_South (14)
  - TankFarmA
  - TankFarmB
  - TankFarmC
  - Unassigned Items (4)

	Date & Time	Location Tag	Source	Co...	Prio...	Description	Trip...	Liv...
!	11/10/2011 18:...	Reactor_South	04FX130_S	PVLO	U 00	CoMonomer Ratio		
!	11/10/2011 18:...	Reactor_South	04LC160_S	PVHI	U 00	Poly Reactor Level		
!	11/10/2011 18:...	DTower	03P2033	PVLO	U 00	Kero Pump		
!	11/10/2011 18:...	Reactor_South	GRADE_MELTFL...	PVLO	U 00	Grade MeltFL South...		
!	11/10/2011 18:...	Boiler_East	BB4_FLAM_E	PVLO	U 00	ELEV B BURNER 4...		
!	11/10/2011 18:...	Boiler_East	BB2_FLAM_E	PVHI	U 00	ELEV B BURNER 2...		
!	11/10/2011 18:...	Reactor_North	04FX130_N	PVLO	U 00	CoMonomer Ratio		
!	11/10/2011 18:...	Reactor_North	04LC160_N	PVHI	U 00	Poly Reactor Level		
!	11/10/2011 18:...	Reactor_North	GRADE_MELTFL...	PVLO	U 00	Grade MeltFL North...		
!	11/10/2011 17:...	Boiler_East	AB2_FLAM_E	PVLO	U 00	ELEV A BURNER 2...		
!	11/10/2011 17:...	Boiler_West	Profit_Loop_W	PVLO	U 00	Profit Loop West Bo...		
!	11/10/2011 11:...	Reactor_North	OP-AC04	PVHH	U 00	Operation - Ari Crp	99.00	99.00
!	11/10/2011 11:...	Reactor_South	OP-AC03	PVLL	U 00	Operation - Ari Crp	0.00	80.00
!	11/10/2011 11:...	Reactor_North	OP-AC04	PVLL	U 00	Operation - Ari Crp	0.00	99.00
!	11/10/2011 11:...	Boiler_West	OP-AC02	PVLL	U 00	Operation - Ari Crp	0.00	20.00
!	11/10/2011 11:...	Boiler_East	OP-AC01	PVLL	U 00	Operation - Ari Crp	0.00	58.00
!	10/20/2011 16:...	Unassigned Ite...	Sinewave	PVLO	U 01	Sinewave	10.00	22.00
⊟	10/20/2011 16:...	Unassigned Ite...	Sinewave	Ext...	U 00	PV	43.00	22.00
⊟	10/19/2011 22:...	Unassigned Ite...	Sinewave	PVHI	U 10	Sine point	2,01...	22.00

Unacknowledged alarms:	19	of	65
Acknowledged alarms:	0	of	0
Shelved alarms:	0	of	0
Suppressed alarms:	0	of	0

Quick Shelve Shelve... Unshelve Alarm

Pause Resume Acknowledge Page

19-Oct-11 15:39:34 Not Loaded ACE_136 OFFNET U 15 Server: Connection FAILED

Honeywell 10-Nov-11 18:04:33 Alarm System as01hsc410svrb Stn01 Mngr

Figure 15: A typical Alarm Summary display

Alarm annunciation

Although alarms appear in Station, you need to consider your alarm annunciation needs. Experion provides the following types of alarm annunciation:

- Station-based buzzer or speaker
- External horn or siren
- Alarm paging

Related topics

"Station-based buzzer or speaker" on page 113

"External horn or siren" on page 113

"Alarm paging" on page 113

Station-based buzzer or speaker

Audible alarm notification is appropriate for Stations used by operators; however, it may not be appropriate for Stations used by production controllers and managers.

You can specify the system-wide characteristics of alarm notification, such as the duration of the sound, and the frequency at which the sound repeats if an alarm is not acknowledged. You can also disable audible alarming on particular Stations, as appropriate.

External horn or siren

If there is a possibility that users may not hear a Station buzzer/speaker, you should consider installing one or more horns or sirens.

You can configure up to four *alarm notification* points—one each for *Urgent*, *High*, *Low* or *Any* alarm priority—to control horns or sirens. For example, you could use the *Urgent* point to control a horn, and use the *Any* point to control a buzzer.

Alarm paging

Alarm paging sends a paging message to one or more designated pagers whenever a specified alarm is raised.

You can use either of the following types of paging:

- **Point-based**. You configure the paging requirements for each point whose alarms you want paged.
- **Asset-based**. You configure the paging requirements for each asset.

Paged messages can contain a number of details, including the priority, point ID, point description and associated message (if one has been assigned).

Alarm Paging supports the following protocols:

- Paging Entry Terminal (PET) protocol
- Telocator Alphanumeric Protocol (TAP)
- Universal Computer Protocol (UCP)

Alarm Paging also supports sending messages as:

- E-mail
- SNMP messages

Contact your local Honeywell representative for a list of suitable paging service providers in your region.

For more information see 'Configuring alarm paging' in the *Server and Client Configuration Guide*.

Alarm groups

Alarm groups provide you with an alternative way of viewing alarms, which is not related to your asset model. For example, you could create an alarm group to monitor alarms on all electrical motors in your plant, regardless of their locations within the asset model.

Alarm groups provide the following major benefits:

- They provide additional filtering capabilities in the Alarm Summary.
- They provide *aggregate alarming*—that is, at each level of an alarm group, you can see the number of alarms that exist at that level.
- They allow you to include aggregate alarming parameters in custom displays, so that operators can quickly see how many alarms there are in each section of the plant.

For more information about alarm groups, see the “Alarm Groups and Aggregate Alarming” section of the *Server and Client Configuration Guide*.

Alarm trackers

Alarm trackers provide a graphical, time-based view of alarms on assets within an operator’s scope of responsibility. An alarm tracker is displayed in a pane on the Experion Alarm Summary and provides a convenient way of viewing “clusters” of alarms on individual assets. By grouping alarms in this way, an alarm tracker helps operators to respond more quickly to alarms in abnormal situations like alarm floods.

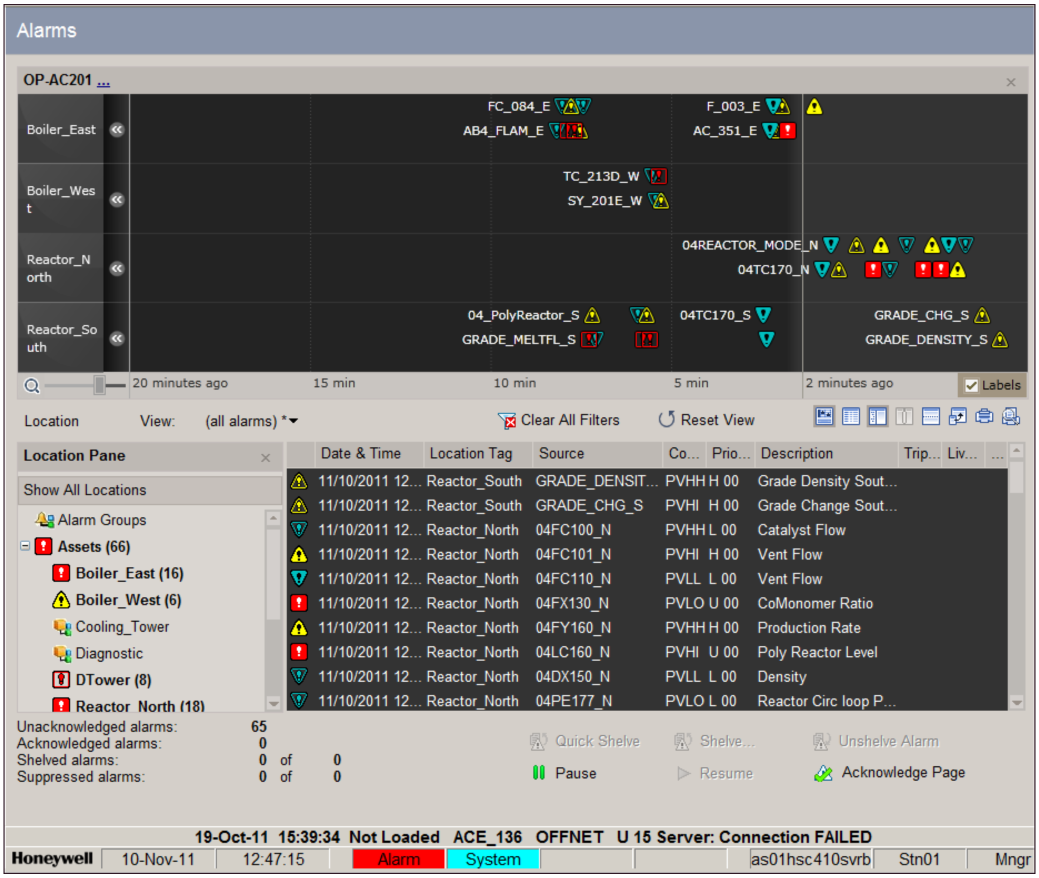
Alarm Tracker is an Experion license option.

Best practice recommendations

If you want to implement alarm trackers at your site, it is strongly recommended that:

- Operators use the Alarm Summary with the Alarm Tracker pane *as their primary display* for an extended period to ensure that they are well experienced in using alarm tracker features in a normal situation before they use it during a major process upset.
- You rationalize the alarm system at your site to ensure that alarm-related displays (especially the Alarm Summary and the Alarm Tracker pane) do not contain more alarms than necessary. For information about alarm design and alarm rationalization, see “Designing alarm systems” in the *Server and Client Planning Guide*.

For information about configuring alarm trackers and assigning an alarm tracker to operators, Stations, Consoles, or Console Stations, see “Configuring alarm trackers” in the *Server and Client Configuration Guide*.



	Date & Time	Location Tag	Source	Co...	Prio...	Description	Trip...	Liv...	...
⚠	11/10/2011 12...	Reactor_South	GRADE_DENSIT...	PVHH	H 00	Grade Density Sout...			
⚠	11/10/2011 12...	Reactor_South	GRADE_CHG_S	PVHI	H 00	Grade Change Sout...			
▽	11/10/2011 12...	Reactor_North	04FC100_N	PVHH	L 00	Catalyst Flow			
⚠	11/10/2011 12...	Reactor_North	04FC101_N	PVHI	H 00	Vent Flow			
▽	11/10/2011 12...	Reactor_North	04FC110_N	PVLL	L 00	Vent Flow			
!	11/10/2011 12...	Reactor_North	04FX130_N	PVLO	U 00	CoMonomer Ratio			
⚠	11/10/2011 12...	Reactor_North	04FY160_N	PVHH	H 00	Production Rate			
!	11/10/2011 12...	Reactor_North	04LC160_N	PVHI	U 00	Poly Reactor Level			
▽	11/10/2011 12...	Reactor_North	04DX150_N	PVLL	L 00	Density			
▽	11/10/2011 12...	Reactor_North	04PE177_N	PVLO	L 00	Reactor Circ loop P...			

Unacknowledged alarms:	65		
Acknowledged alarms:	0		
Shelved alarms:	0	of	0
Suppressed alarms:	0	of	0

19-Oct-11 15:39:34 Not Loaded ACE_136 OFFNET U 15 Server: Connection FAILED

Honeywell | 10-Nov-11 | 12:47:15 | Alarm | System | as01hsc410svrb | Stn01 | Mngr

Figure 16: An example of an Alarm Tracker pane in the Alarm Summary

Alerts

Alerts are notifications whose urgency and priority are not high enough to be alarms.

There are several types of alerts:

- Interactive Instruction alerts, which can be generated by C300 controllers and ACE to indicate to operators that there are tasks that they must complete so that a sequential control module can continue executing. These types of alerts are configured when the sequential control module is configured. For more information on sequential control modules and alerts, see the *Sequential Control User's Guide*.
- User-generated alerts, which can be used, for example, as a reminder to an operator to schedule maintenance for a piece of equipment.
- System-generated alerts, which are notifications of an abnormal condition in the system that could cause problems if the condition is not fixed.

  For example, the gas pressure in Pipe A has been rising steadily over the last couple of days, most probably due to a build-up of waste particles on the inner lining. This is leading to a degradation in process performance. An alert is raised to indicate that pipe cleaning must take place in the next week.

Alerts are incorporated into Experion from a third-party user alert application using a URT connection. For more information, see the “Configuring alerts” section of the *Server and Client Configuration Guide*.

Messages

Messages can be generated to provide additional information to an operator, for example when a point goes into alarm, a message can provide an explanatory note or a procedure.

There are four types of messages:

- Informational
- Confirmable (available if you have Process Controllers or a TPS system)
- Single signature (available if you have Process Controllers)
- Double signature (available if you have Process Controllers)

Informational messages are defined in:

- Configuration Studio if you have standard points.
- Control Builder if you have process points.
- TPS if you have a TPS system.

Confirmable messages are configured in Control Builder or TPS.

Single signature and double signature messages are configured in Control Builder.

For status, analog, and accumulator points you can specify a predefined message to be displayed in the Message Summary when the point goes into alarm.

Each Station displays the message text defined on its local server. If you have a DSA system, the message indexes and text should be the same on all servers to ensure that appropriate messages are displayed for remote points.

Events

An event is a significant change in the status of an element of the system such as a point or piece of hardware. Examples of events are the occurrence of an alarm, an alarm returning to normal, an operator signing on, and a batch process starting.

Event details, which include the source of the event, the condition and a timestamp, can be viewed on displays and included in reports.

Events are initially collected in a system database, and are periodically copied to a Microsoft SQL Server online event database for queries and reporting. The events are kept in database for a specified period, after which they are deleted.

Tip

For Event database replication to complete successfully, ensure that the redundant Server regional settings are the same. If they are not the same, replication will fail.

Event storage and archiving

If you want to retain events for more than a few weeks, you need to use Event Archiving to configure:

- How long events are kept online
- How often events are archived

Event Archiving allows you set up automatic archiving, or to configure an alarm which alerts the operator to archive events at appropriate intervals. Event Archiving enables you to archive events to a network file server or to tape. Archiving to tape uses the Windows Backup program. Events archived to a network file server can be copied to other media such as CD, or included in a system backup.

For more information about Event Archiving, see the “Configuring Event Archiving” section of the *Server and Client Configuration Guide*.

Displays

This section describes how to determine your display requirements.

Issue	Comments
System displays	Experion includes a comprehensive set of *system* displays, which display information in a standardized manner. Some system displays, such as groups and trends, require configuration.
Tabbed displays	Decide whether you want to enable tabbed displays in Station. With tabbed displays operators can have multiple displays open in either single-window Station or within one or more windows of multi-window Station. Tabbed displays in Station work in a similar way to tabbed displays in Microsoft Internet Explorer.
Custom displays	Decide whether you want to create your own (*custom*) displays. Well designed custom displays make it much easier for operators to interpret system activity and to run your plant in an efficient manner.
Custom faceplates	If you have custom points, consider creating your own (*custom*) faceplates to present point data in a manner that is easy for operators to understand.
Web pages and other documents	Station can display Web pages and ActiveX documents, such as Microsoft Word and Microsoft Excel documents. You can also embed Web pages and ActiveX documents in custom displays.
Update rates	You need to select an appropriate update rate for each Station.

Related topics

“System displays” on page 120
“Tabbed displays” on page 121
“Custom displays” on page 122
“Custom faceplates” on page 124
“Display scripts” on page 125
“Display design” on page 126
“Display security” on page 127
“Acronyms” on page 128
“Web pages and other documents” on page 129
“eServer” on page 31
“Station update rates” on page 62

System displays

Experion includes many system displays, which are categorized as follows:

Display type	Description
Configuration	Displays only used during configuration of your system.
Detail	Provides detailed information about a particular point. This information includes current values, scanning, history and so on.
Faceplate	A specialized type of popup window that shows critical information about a point, and provides a convenient means of controlling the point. Many faceplates look like the front panels of the field devices they represent.
Summary	Displays information, such as alarms and events, in list form.
Status	Displays detailed status information about system equipment, such as controllers and printers.

Experion uses most system displays in an automated manner with no additional requirement on your part—for example, when you create a new point, Experion uses the appropriate point detail display to show the point's details.

However, the following types of system display do require configuration:

Display type	Description
Group	Displays major parameter values for up to eight related points.
Trend	Displays historical process values in a graphical manner. The data can be displayed in several ways—such as lines and barcharts—and can track several variables. If you use trends, you need to determine the data collection requirements for each point parameter displayed as a trend.

Related topics

“Groups” on page 85

“Trends” on page 86

“History collection” on page 82

Tabbed displays

Tabbed displays are an optional server wide setting available for single-window Station as well as multi-window Station (SafeView).

With tabbed displays, operators can call up displays in individual tabs within a Station window. Whenever they call up a display, operators can choose to open it in an existing tab or in a new tab.

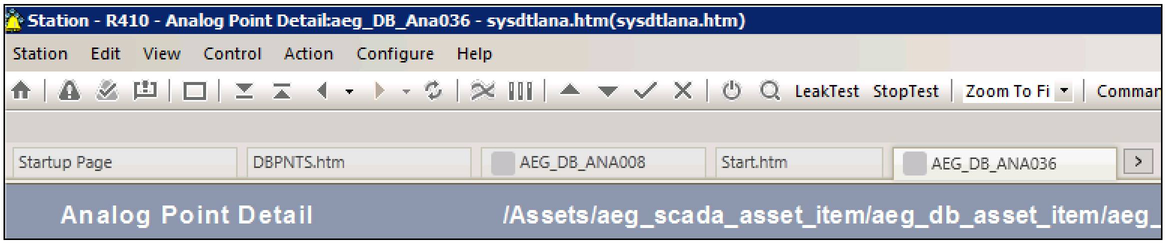


Figure 17: An example of Station with tabbed displays enabled

After opening displays in individual tabs, operators can quickly move between displays by clicking on the tab of the display they want to view. This is particularly useful when operators are dealing with alarm floods or other urgent alarm situations.

The tab of a point detail display and any custom display that is associated with an alarm group, shows an alarm icon representing the “most important” alarm on that display. This means that operators can keep track of alarms even on displays that are not currently on view.

Custom displays

You can make it much easier for operators to interpret and control system activity if you create suitable *custom* displays.

Custom displays are created using HMIWeb Display Builder, a specialized drawing tool, which is supplied with several clip art libraries that cover a range of industries. For example, the clip art libraries include representations of pumps, valves, and so on.

With custom displays, you can insert your own graphics (for example, photographs and layout diagrams) using any of the following formats.

- GIF (*.gif)
- Windows Bitmap (*.bmp)
- JPEG (*.jpg)
- Metafile (*.wmf)
- Portable Network Graphic (*.png)

The following figure shows a typical custom display created using HMIWeb Display Builder.

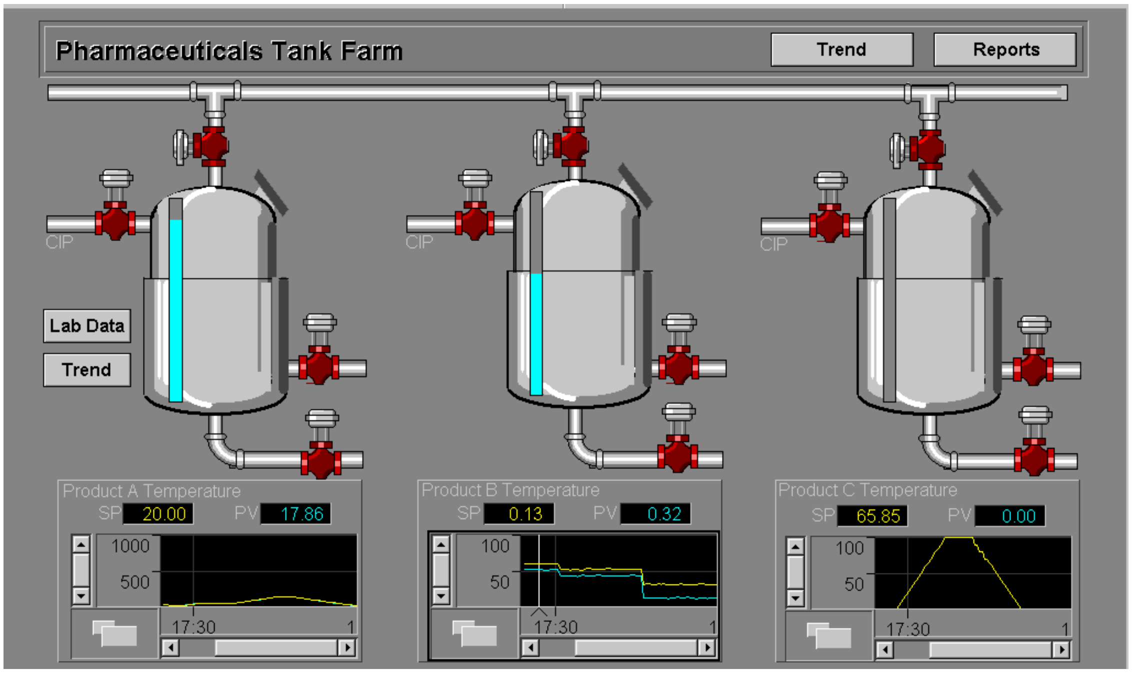


Figure 18: Typical custom display

Custom display features and considerations

In planning your custom displays you might consider the following issues.

Issue	Comments
Display scripts	Decide whether you need to write *display scripts*.
Embedded documents	Decide whether you want to include operational procedures or other information in your displays.
Acronyms	Determine whether you need to define any special acronyms.
Layout and design	Specify the purpose of each display, and establish a set of design guidelines.

Issue	Comments
Assets	You can use assignable assets to restrict access to custom displays to specific operators or Stations.
Integrated alarm help	You can provide operators with integrated alarm help information from an Alarm Configuration Manager (ACM) server.

Related topics

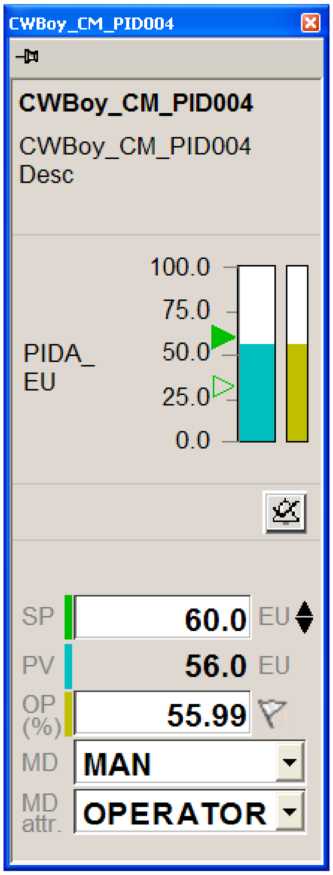
“About assignable assets and scope of responsibility” on page 14

Custom faceplates

A faceplate is a specialized type of popup window that shows critical information about a point, and provides a convenient means of controlling the point. Many faceplates, such as the following example, look like the front panels of the field devices they represent.

If you have any custom point types, you should consider creating your own custom faceplates for these point types.

As with custom displays, you create custom faceplates using HMIWeb Display Builder.



CWBoy_CM_PID004

CWBoy_CM_PID004

CWBoy_CM_PID004 Desc

SP 60.0 EU
PV 56.0 EU
OP (%) 55.99
MD MAN
MD attr. OPERATOR

Figure 19: A typical faceplate

Display scripts

You can add extra functionality to your displays with *display scripts*. For example, you could write a script that runs an animation when an object changes state.

For more information, see the topic 'Display scripting reference' in the *HMIWeb Display Building Guide*.

Display design

When designing custom displays, you should determine:

- The purpose of each display from an operator's point-of-view
- How operators will navigate from one display to another (For example, you could have a 'home' display, showing the entire plant, with a set of buttons to link to other displays that show specific assets or processes.)
- The security requirements of each display (You can use assignable assets to restrict access of a custom display to operators or Stations that have been assigned a specific asset.)
- To provide operators with integrated alarm help information from an Alarm Configuration Manager (ACM) server.

You should present information in an appropriate form, so that it is intuitive and easy to use. Also, consider using a presentation style similar to that used in the system displays, so that operators are not confronted with two presentation styles.

Display security

The data that can be viewed with a system display is primarily controlled by assigning to operators (or Stations) the assets that contain the data. Values can be seen if the asset permissions is `View` or higher. Values can be changed if the access is `Oper` or higher.

With custom displays, however, the security needs to be configured on the display itself. There are two ways to achieve this:

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

Acronyms

An *acronym* describes the meaning of a point parameter's state (or integer value). For example, the acronyms 'Stopped' and 'Running' are much more meaningful in displays than the raw parameter values '0' and '1'.

Experion includes a comprehensive collection of acronyms that are suitable for most purposes (Open/Closed, Manual/Automatic, and so on). However, you can create your own acronyms if needed.

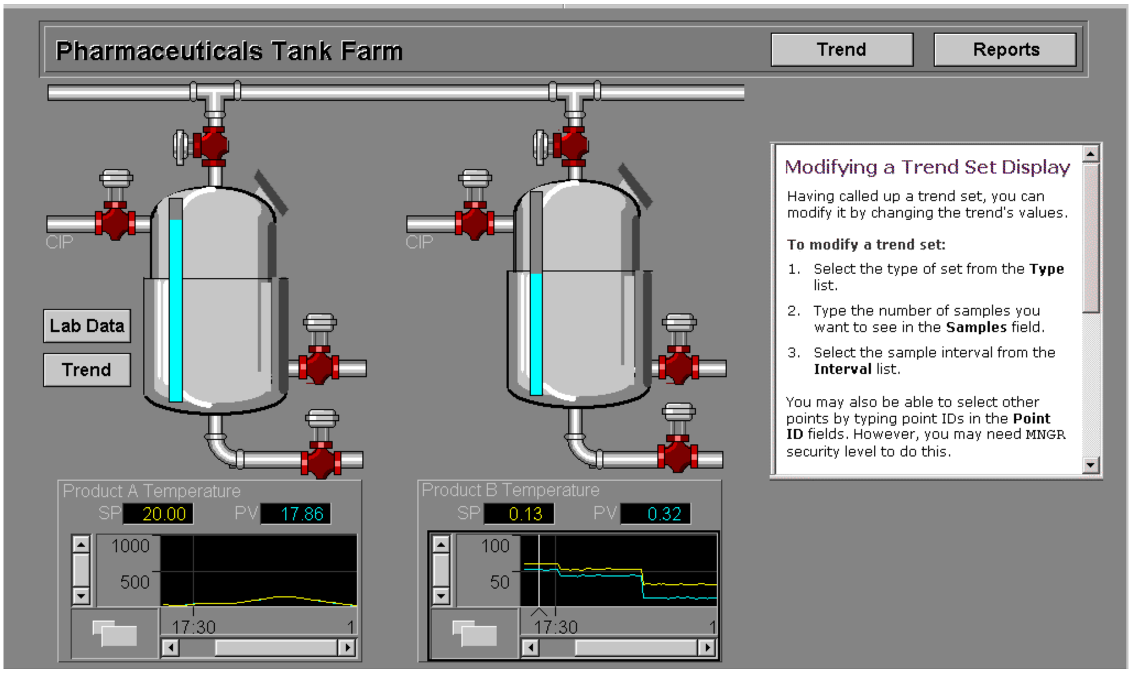
Web pages and other documents

Station can display Web pages and ActiveX documents, such as Microsoft Word and Microsoft Excel. You should therefore consider making operating instructions and other useful information available to users.

Station ensures that users can still monitor alarms while viewing such documents, and provides security features that allow you to restrict access to specified documents and Web sites.

Displays with linked documents

You can also include links to Web pages and ActiveX documents in custom displays, as shown in the following example. If you subsequently update the document, the display is automatically updated because it only includes a link to the document.



Modifying a Trend Set Display

Having called up a trend set, you can modify it by changing the trend's values.

To modify a trend set:

1. Select the type of set from the **Type** list.
2. Type the number of samples you want to see in the **Samples** field.
3. Select the sample interval from the **Interval** list.

You may also be able to select other points by typing point IDs in the **Point ID** fields. However, you may need MNGR security level to do this.

Figure 20: Display with a linked document

Reports

Reports are typically used for:

- Analyzing alarms and events
- Analyzing system activity
- Performing routine tasks (Some of Experion's standard reports perform tasks.)
- Searching for points with specific attributes

Issue	Comments
Standard reports	Check the standard reports supplied with Experion to see whether they meet your needs.
Integrated Microsoft Excel Reports	Enables you to create custom reports that present server data in a Microsoft Excel spreadsheet.
Free Format Reports	If you need to modify a standard report, or create your own standard reports, consider the Free Format Report Writer option.
Output destination	Determine where you want to send your reports. For example, you may want to print some reports, but view others online.
Scripts	Determine whether you can use *server scripts* to perform specialized tasks on your reports.

Related topics

"Standard reports" on page 132
"Integrated Microsoft Excel reports" on page 133
"Free Format reports" on page 134
"Output options" on page 135

Standard reports

The following reports are supplied with Experion. (Some are only available if you have licensed the associated option.)

Report	Description
Alarm and Event	Alarm and event details from the event file. This report enables you to analyze alarms and events that occurred during a specified time span on specific points.
Alarm and Event DSA	Alarm and event details from servers within a DSA. This report enables you to analyze alarms, alerts, and events that occurred during a specified time span on local and remote points on multiple servers.
Alarm Duration	The duration of alarms and events on nominated points during a nominated time span.
Asset Alarm Count Report	The number of alarms on particular assets and the priority of those alarms. You can configure the report to generate alarm counts for assets within the SOR of either the user currently logged on or (if you are logged on at MNGR level) another specified user.
Batch	Batch reports are used to collect history for a set of points and events for an asset for the duration of a production run. A batch report can collect: • One type of history sample (such as 5-second samples or 1-hour averages) for up to 50 points • Events for one asset
Cross Reference	Where points are referenced in the server database. The report lists the following types of references for the nominated points: custom displays, trend displays, algorithms, reports, operating groups, history gates, source address for another point, application program point lists.
Point Attribute	Points that are in a specified state; for example, you can generate a report on all points that are off-scan, have alarms inhibited, have a bad PV, or are in manual mode.
Sequence of Events	Some types of controller can time-stamp events to millisecond resolution. When this capability is used, the server stores the high resolution event information in the server's 'sequence of events' file. This report is based on data extracted from this file.

Integrated Microsoft Excel reports

You can design your own reports in Microsoft Excel and run them from a Station like a standard report.

These reports use either Microsoft Excel Data Exchange or Experion's ODBC driver to access data in the server database. When choosing between Microsoft Excel Data Exchange and ODBC driver, consider the following:

- Microsoft Excel Data Exchange can access all information in the server database, whereas the ODBC driver can only access point, history and event data.
- Microsoft Excel Data Exchange can write to the server database.
- Microsoft Excel Data Exchange has no security, whereas the ODBC driver follows the same security conventions as other reports.

For more information about Integrated Microsoft Excel Reports, see the “Microsoft Excel reports configuration checklist” topic in the “Reports” section of the *Server and Client Configuration Guide*.

Related topics

“Microsoft Excel Data Exchange” on page 142

Free Format reports

The Free Format Report Writer allows you to modify standard reports, and to create your own reports and add them to the list of standard reports.

You can write reports that:

- Get values from point parameters
- Perform calculations on those values (for example, addition, subtraction, multiplication, division, and exponentiation)
- Retrieve historical data to determine summations, maximums, minimums, and standard deviations

  Tip

  Uncertain values can also be included in these reports, if these are needed in your calculations. See the topic titled "Free Format variables reference" in the *Server and Client Configuration Guide*.

- Generate an X-Y plot of the historical values for two points
- Store new values or calculations in the server database or in operating system files

You can also use free format reports to write information back to the server database, providing your needs are simple.

For more information about the Free Format Report Writer, see the topic titled "Free Format reports" in the *Server and Client Configuration Guide*.

Output options

When designing a report, you need to consider how it is to be output. For example, a report that only needs to be viewed online should have a very simple layout.

The output choices are:

- **Print**. Typically used for routine reports, such as weekly reports, that need to be kept or read by users without access to a Station.
- **Online**. Typically used to see a 'snapshot' of a particular part of the system, and then discarded. For example, you may want to check the current status of a particular production line.
- **File**. Suited for further processing by another application. For example, you may want to import the report file into a spreadsheet.

Specialized features

This section describes specialized Experion features that may be of use in your system.

Feature	Comments
Recipes	The Recipe Manager allows you to quickly reconfigure standard processes.
Point Control Schedules	Point Control Schedules enable you to control points on a periodic or one-off basis.
Honeywell Digital Video Manager	Honeywell Digital Video Manager is a Closed Circuit Television product that can be easily integrated with Experion.

Related topics

"Recipes" on page 138

"Point control schedules" on page 139

"Honeywell Digital Video Manager" on page 140

Recipes

The Recipe Manager allows an operator to quickly reconfigure a *unit*—such as a chemical cracker or production line. The Recipe Manager achieves this by downloading a set of predefined values to the unit.

If you have several identical units, operators can download the same recipe to any unit. If appropriate, they can also download scaled values—to control, for example, the size of a production batch.

A recipe can include up 30 *ingredients* (an ingredient specifies a value and the parameter to which it is downloaded). If more than 30 ingredients are required, you can chain recipes together to form a larger recipe. If you require a more sophisticated batch system, ask your Honeywell representative for information about Experion Batch Manager.

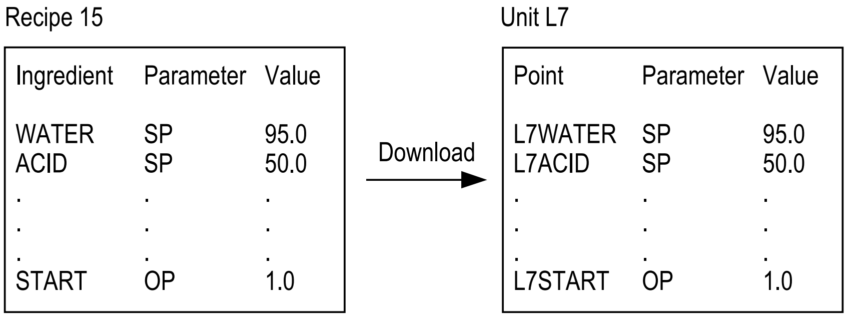
The total number of recipes that can be configured depends on the size of your Experion database.

Point requirements in recipes

The following naming rules apply to points used in recipes:

- The unit's two-character identifier is used as the prefix.
- The ingredient's name is used as the suffix.
- The names must follow the standard point naming conventions.

When downloading a recipe, Experion determines each point ID by combining the unit ID and the ingredient name. The following figure shows what happens when recipe *`15`* is downloaded to unit *`L7`*. In this example, the value of *`WATER`* is downloaded to the SP of point *`L7WATER`*.



Recipe 15

Ingredient	Parameter	Value
WATER	SP	95.0
ACID	SP	50.0
.	.	.
.	.	.
.	.	.
START	OP	1.0

Unit L7

Point	Parameter	Value
L7WATER	SP	95.0
L7ACID	SP	50.0
.	.	.
.	.	.
.	.	.
L7START	OP	1.0

If you want to download a recipe to several units, you need to define an appropriate set of points for each unit. Following from the above example, a unit called *`L8`* requires the following points:

```
L8WATER
L8ACID
.
.
.
L8START
```

Point control schedules

Point Control Schedules enable you control points on a periodic or one-off basis. It also includes the capability of defining holidays and shifts.

For example, you could schedule:

- A pump to switch on at 4 pm and off at 6 pm each work day
- A boiler to close down at midnight on a specific day

For more information about Point Control Schedules, see 'Configuring a point control schedule' in the *Server and Client Configuration Guide*.

Honeywell Digital Video Manager

Honeywell Digital Video Manager (Honeywell DVM) is a Closed Circuit Television (CCTV) product that combines the advantages of digital video with the latest Web and networking technologies.

You can easily integrate Honeywell DVM with Experion because it:

- Uses Station as its user interface, which means that operators can seamlessly switch between Experion and Honeywell DVM displays
- Can initiate recordings in response to Experion alarms and events

For more information about Honeywell DVM, contact your Honeywell representative.

Exchanging data with other applications

Experion includes a number of data exchange options that extend its capability and functionality.

For example, you can export current point parameter values from the server database to a Microsoft Excel spreadsheet, and then perform sophisticated calculations.

Attention

If your system uses *dynamic scanning* to poll data, dynamic scanning is not triggered by applications.

Option	Description
Microsoft Excel Data Exchange	Exports server data to Microsoft Excel spreadsheets. (Microsoft Excel Data Exchange is part of the Open Data Access (ODA) option.)
ODBC Data Exchange	Used to exchange data between the Experion database and an ODBC-compliant database.
ODBC Driver	Primarily intended for reporting, it enables an ODBC-compliant application to access data in the Experion database, such as history, event, and point parameter values. (ODBC Driver is part of the Open Data Access (ODA) option.)
OPC	Experion provides a range of OPC server and client options, each of which has been optimized for a specific purpose.
Network API	Allows you to create applications that can exchange data between Experion and another application, which is either on the server or another computer. (Network API is part of the Open Data Access (ODA) option.)

Microsoft Excel Data Exchange

Microsoft Excel Data Exchange allows you to capture real-time point parameter and history information, and display the data in a Microsoft Excel spreadsheet.

You can capture server data using either the Microsoft Excel Data Exchange Wizard, or through cell formulas. The captured data can be static or dynamically updating, and can consist of either point parameter or historical data.

After capturing the data, you can create charts to display and analyze data with Microsoft Excel's toolset. You can also link the values into other OLE-enabled applications.

Microsoft Excel Data Exchange provides:

- Read/write access to point parameter values
- Read access to history data
- Read/write access to server database files (user files)

For more information, see 'Using the Microsoft Excel Data Exchange wizard' in the *Server and Client Configuration Guide*.

Related topics

"Integrated Microsoft Excel reports" on page 133

ODBC Data Exchange

ODBC Data Exchange enables two-way exchange of data between the Experion database and an ODBC-compliant database (either local or remote). It is typically used to periodically transfer data such as production totals and values for billing customers. ODBC-compliant databases include Microsoft SQL Server, Oracle 7, Microsoft Access, and Sybase 10.

With ODBC Data Exchange, the Experion server acts as a *client* application. (Contrast this with the ODBC Driver, where the Experion server acts a *server* application.)

For more information, see 'Configuring Experion ODBC' in the *Server and Client Configuration Guide*.

ODBC Driver

The ODBC Driver is part of the Open Data Access (ODA) option. It is primarily intended for reporting, and enables an ODBC-compliant application to access data in the Experion database, such as history, event and point parameter values. ODBC-compliant applications include Microsoft Access and Microsoft Excel.

With the ODBC Driver, the Experion server acts as a *server* application. (Contrast this with ODBC Data Exchange, where the Experion server acts a *client* application.)

For more information, see 'Configuring Experion ODBC' in the *Server and Client Configuration Guide*.

OPC

Experion provides the following OPC interfaces, each of which has been optimized for a particular purpose:

Experion OPC Client Interface

The Experion OPC Client Interface is primarily designed for integrating low-complexity subsystems, such as controllers. Configuration involves individually mapping OPC items to standard Experion points (analog, status and so on).

If you require alarming for an item, you must configure the associated point's alarm properties.

If your system has redundant third-party OPC servers, the OPC Client interface can be used as it natively supports the concept of preferred and secondary servers. However, Honeywell recommends that you use Redirection Manager when communicating with redundant third-party OPC servers, as it can give better performance during OPC server failover, because it builds OPC groups on both OPC servers.

For more information, see the *OPC Client Interface Reference*.

Experion OPC Advanced Client

The Experion OPC Advanced Client includes a data client, and an alarm and event client for connection to third-party OPC servers.

If your system has redundant third-party OPC servers, Experion Redirection Manager (RDM) should also be installed and used. RDM is the only way to provide redundancy with the Experion OPC Advanced Client.

For information about installing and configuring Redirection Manager and the System Management runtime component, see : Experion R431 > Installation and Upgrades > Supplementary Installation Tasks Guide > Installing Redirection Manager.

Attention

It is preferable for the third-party OPC servers to run in a dual active mode rather than an active-passive mode.

Experion OPC Advanced Data Client

The Experion OPC Advanced Data Client is primarily designed for integrating complex subsystems, and is compliant with the OPC Data Access specification. Such systems typically have OPC items with multiple parameters, and are capable of generating their own, often broad range of alarms.

It also performs dynamic communications optimization. Only those parameters (items) that are currently being accessed—in displays, reports and so on—are subscribed from the OPC server. The points are dynamically subscribed and unsubscribed as required to minimize load on the source system.

For more information about the Experion OPC Advanced Data Client, see 'Experion OPC Advanced Client' in the *Server and Client Configuration Guide*.

Experion OPC Advanced Alarm and Event Client

The Experion OPC Advanced Alarm and Event Client enables Experion to receive alarms and events from third-party OPC alarm and event servers.

The Experion OPC Advanced Alarm and Event Client is based on the OPC Foundation Alarm and Events Specification.

Attention

There are different interpretations of the OPC AE standard by third-party OPC AE server vendors. Integration issues have been seen with OPC condition events in areas such as alarm acknowledgement and duplicate alarm identification. If you want to integrate a third-party OPC AE server that utilizes OPC condition events with Experion, you should contact Honeywell.

The risks with OPC simple and tracking events are lower than for OPC condition events. However, due to different interpretations of the OPC AE standard, integration issues may still be found. Thorough testing between the Experion OPC client and third-party server should be performed to ensure correct operation.

Experion OPC Display Data Client

The Experion Display Data Client is designed to be used when you want to add OPC items to custom displays, but have no requirement for advanced features such as alarms, history or reporting.

If your system has redundant third-party OPC servers, Experion Redirection Manager (RDM) should also be installed and used. RDM is the only way to provide redundancy with the Experion OPC Display Data Client.

For information about installing and configuring Redirection Manager and the System Management runtime component, see the following topic: Experion R431 > Installation and Upgrades > Supplementary Installation Tasks Guide > Installing Redirection Manager.

Attention

It is preferable for the third-party OPC servers to run in a dual active mode rather than an active-passive mode.

You can directly add OPC items to custom displays, without having to first define them as points in Quick Builder.

Experion OPC Server

The Experion OPC Server gives an OPC client read/write access to Experion point parameters. It is compliant with the OPC Data Access specification, and can accept connections from OPC clients.

The Experion OPC Server supports all mandatory OPC interfaces, including an automation interface for application development in Visual Basic, as well as the IOPCBrowseServerAddressSpace interface. For more information on the automation interface, see the *OLE for Process Control Standard.*

If your system has redundant third-party OPC servers, Experion Redirection Manager (RDM) should also be installed and used. RDM is the only way to provide redundancy with the Experion OPC Server.

For information about installing and configuring Redirection Manager and the System Management runtime component, see : Experion R431 > Installation and Upgrades > Supplementary Installation Tasks Guide > Installing Redirection Manager.

Attention

It is preferable for the third-party OPC servers to run in a dual active mode rather than an active-passive mode.

Experion OPC Historical Data Access Server

The Experion OPC Historical Data Access Server (HDA) gives an OPC client access to Experion point parameter history. It is compliant with the OPC Historical Data Access Specification.

If your system has redundant third-party OPC servers, Experion Redirection Manager (RDM) should also be installed and used. RDM is the only way to provide redundancy with the Experion OPC Historical Data Access Server.

For information about installing and configuring Redirection Manager and the System Management runtime component, see the following topic: Experion R431 > Installation and Upgrades > Supplementary Installation Tasks Guide > Installing Redirection Manager.

Attention

It is preferable for the third-party OPC servers to run in a dual active mode rather than an active-passive mode.

Experion OPC Alarm and Event Server

The Experion OPC Alarm and Event Server allows an OPC alarm and event client to receive alarm and event information from Experion. It is compliant with the OPC Foundation Alarm and Event Specification.

If your system has redundant third-party OPC servers, Experion Redirection Manager (RDM) should also be installed and used. RDM is the only way to provide redundancy with the Experion OPC Alarm and Event Server.

For information about installing and configuring Redirection Manager and the System Management runtime component, see the following topic: Experion R431 > Installation and Upgrades > Supplementary Installation Tasks Guide > Installing Redirection Manager.

Attention

It is preferable for the third-party OPC servers to run in a dual active mode rather than an active-passive mode.

Experion OPC Integrator

The Experion OPC Integrator (OPCI) is used to transfer data between different parts of the system using data that is accessible through OPC. OPC Integrator can be used in many different architectures that include process controllers, SCADA controllers, distributed control systems, local and remote Experion servers. This section describes OPC Integrator, and three typical system topologies using OPC Integrator.

Attention

OPC Integrator is not designed to transfer safety or process critical data. To transfer critical data, you should use a direct peer to peer method of communication between controllers rather than through a server-based process.

OPCI groups and connectivity

The key functionality with OPCI is that OPC clients have the ability to update server data by making a write request. OPCI allows you to integrate separate OPC servers together in a limited manner which otherwise wouldn't normally be possible, requiring a server/client interaction. OPCI interfaces between the OPC servers as a client to each server, thus integrating the servers to each other.

Experion OPC Integrator integrates source and destination OPC server data points into groups. OPC Integrator does not handle alarms and events.

When you configure an OPCI group, you nominate two OPC servers, a source server and a destination server, and a list of OPC data item pairs to transfer data between them. For example, if you nominate the Experion OPC server as the source server and a 3rd party OPC server as the destination, then OPCI reads the Experion point data and writes it to the 3rd party system.

Each OPCI group, when enabled, establishes a connection to both the source and destination OPC servers that are configured for that group. It then adds, to each OPC server, the list of items that have been configured for that group on that OPC server. The OPCI group then subscribes to receive callbacks from the source OPC server only. This means, that when values change on any of the source points configured, the Experion OPC server will send the new values to OPCI. This is standard OPC server/client interaction. OPCI then writes these values to the corresponding items configured on the destination OPC server.

For best performance, OPCI destination groups should be configured on the server where the writes will occur. Be aware that configuring OPC Integrator with one or more items in a destination group on a different server may place undesirable load on the communications subsystems of target controllers.

For more information about the Experion OPC Integrator, see “Experion OPC Integrator” in the *Server and Client Configuration Guide*.

Transferring data between local controller points

In this topology, OPC Integrator and the Experion OPC server are installed on the same Experion server to achieve communication between controllers. OPC Integrator can read and/or write to each controller. The controllers can be:

- Honeywell Process controllers (C200, C300)
- Experion SCADA Fail Safe Controllers (FSC)
- SCADA controllers connected using the Experion OPC Client Interface

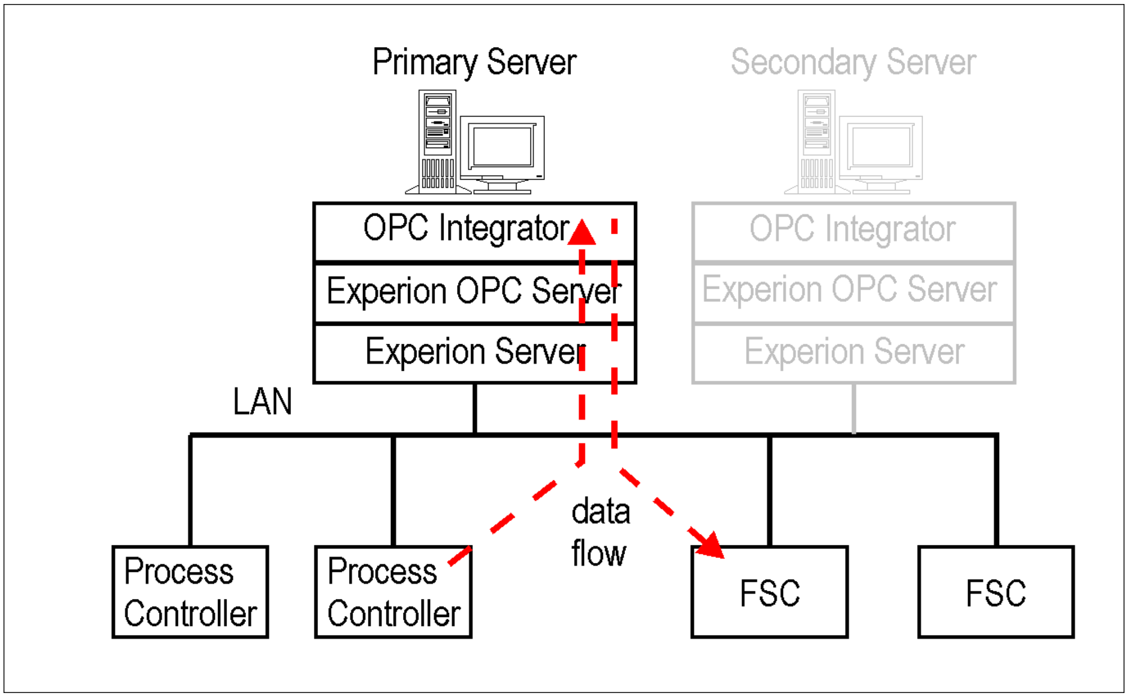


Figure 21: Transferring data between local controller points using OPC Integrator

Previously the value transportation algorithm may have been used to achieve this type of communication, however, now the OPC Integrator provides a more efficient method.

This architecture supports Experion server redundancy.

Transferring data between local and remote points

In this topology, OPC Integrator is installed on the local Experion server. Although the OPC integrator groups are configured with localhost, the source or destination points could be part of a controller that is connected to a different Experion server. In this situation, data transfer is achieved using the DSA subsystem.

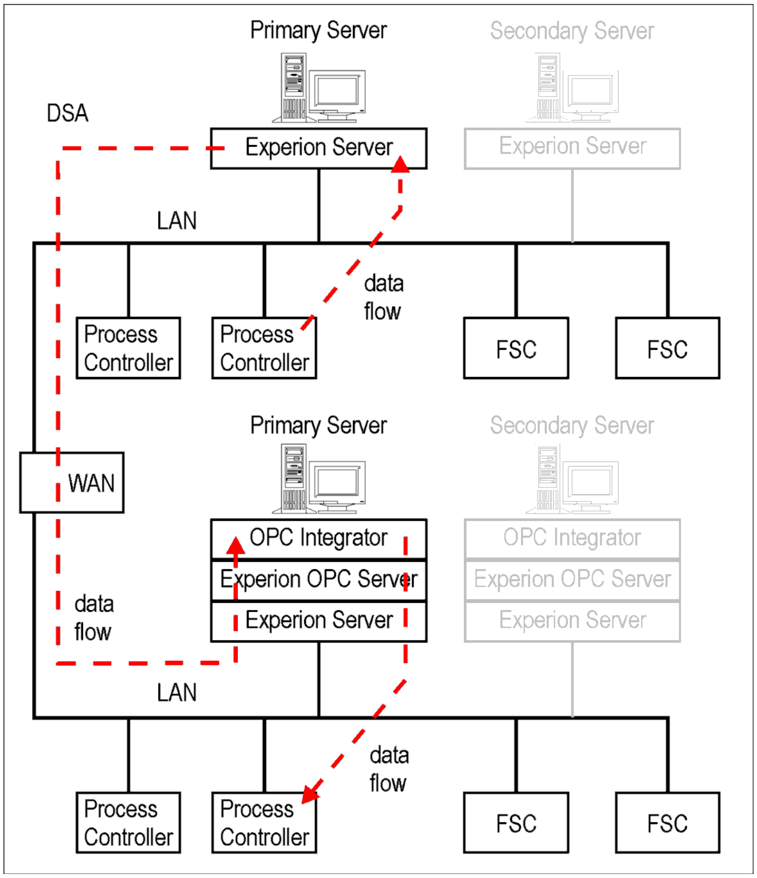


Figure 22: Transferring data between local and remote controller points using OPC Integrator

It is important to note that OPC Integrator groups must be configured so that controller writes are performed on the local server. That is, all destination items must be part of a controller that is connected to the local server.

This architecture supports Experion server redundancy.

Transferring data between Experion and a third-party OPC server

In this topology, OPC Integrator interfaces with the local Experion OPC server and a remote third-party OPC server connected to another system to achieve data transfers between other OPC connected systems and Experion.

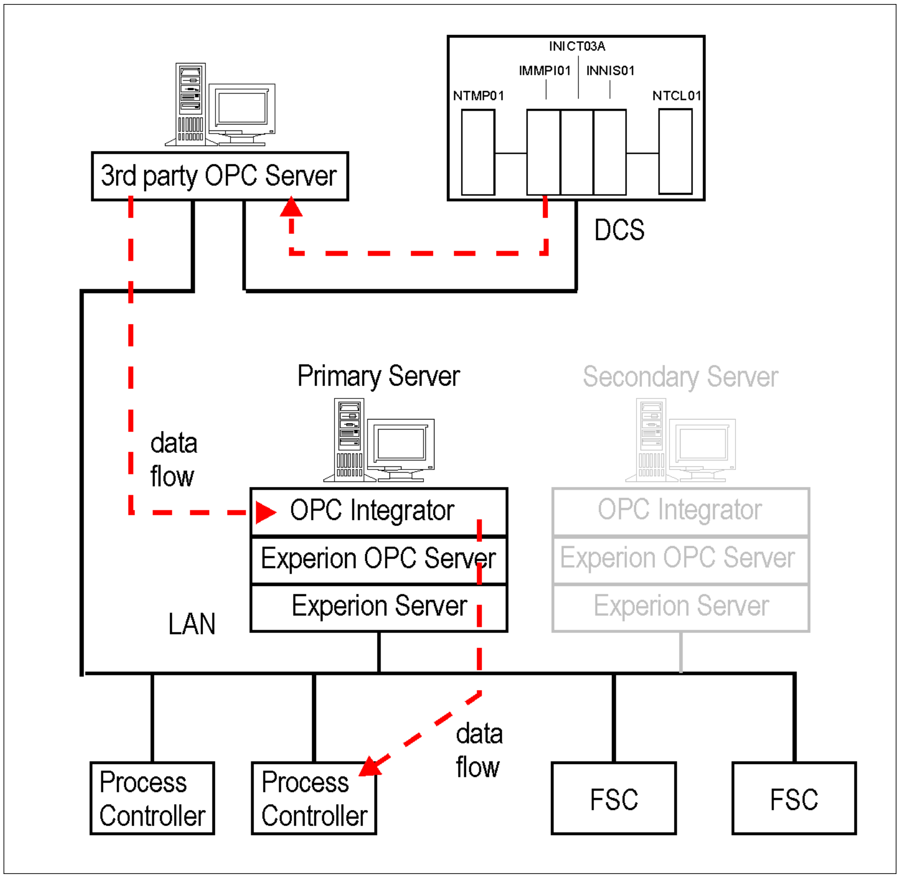


Figure 23: Transferring data between local and third-party OPC points using OPC Integrator

Operator changes and controller initiated changes performed on other systems can be transferred to Experion. Likewise, operator changes and controller initiated changes performed in Experion can be transferred to other systems. OPC Integrator can have bidirectional groups which are designed to transfer data in both directions, regardless of where the change occurred.

In this topology, one of the systems has the role of master to prevent transfers going in to a continuous loop.

This architecture supports Experion server redundancy and also supports redundancy for remote OPC servers.

If your system has redundant third-party OPC servers, OPCI can be used to manage the redundancy. However, Honeywell recommends that you use Redirection Manager when communicating with redundant third-party OPC servers, as it can give better performance during OPC server failover, because it builds OPC groups on both OPC servers.

OPC Integrator licensing

For information about OPC Integrator licensing, contact your Honeywell representative.

Network API

Network API is part of the Open Data Access (ODA) option. It allows you to create applications—in Visual C/C++ or Visual Basic—that exchange data with the Experion database. These applications can run on another computer or the Experion server.

Applications that use Network API can have:

- Read/write access to point parameter values
- Read access to history data
- Read/write access to server database files (user files)

ODA incudes libraries of functions, header files, and sample source programs to help programmers create network applications.

For more information, see 'Network API reference' in the *Application Development Guide*.

Integrating TPS systems

If you have a license for the TPS integration option, you can use an Experion Server-TPS (ESVT) to connect an Experion cluster with a TPS cluster via DSA.

The following figure shows a typical integrated system. The ESVT node is a specialized Experion server that includes some TPS components, and is fitted with an LCNP card so that it can communicate over the TPS network.

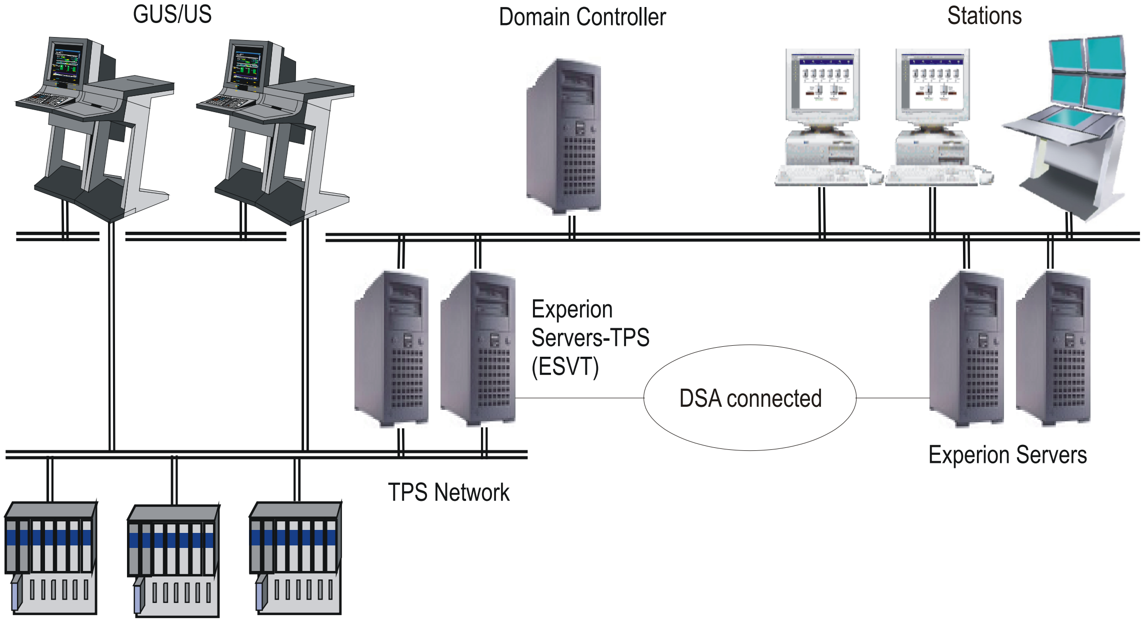


Figure 24: Typical integrated system

TPS data and notifications in Experion

When you integrate your TPS systems with Experion, TPS data is treated the same way as native Experion data. For example, you can include TPS data in displays and reports, and can access it through Experion's interfaces such as ODBC and Microsoft Excel Data Exchange.

TPS notifications (alarms and events) are also treated in the same way as native Experion alarms and events. For example, they are automatically included in the Alarm, Event, and Message Summary displays.

For more information about using an ESVT node to connect Experion and TPS clusters via DSA, see the *Integrated Experion-TPS User's Guide*.

Experion Stations-TPS

- Alternatively, you can replace Global User Station (GUS) and Universal Station (US) functionality through the use of integrated Experion-TPS nodes, as shown in the following example scenario. For more information, see the *Integrated Experion-TPS User's Guide*.

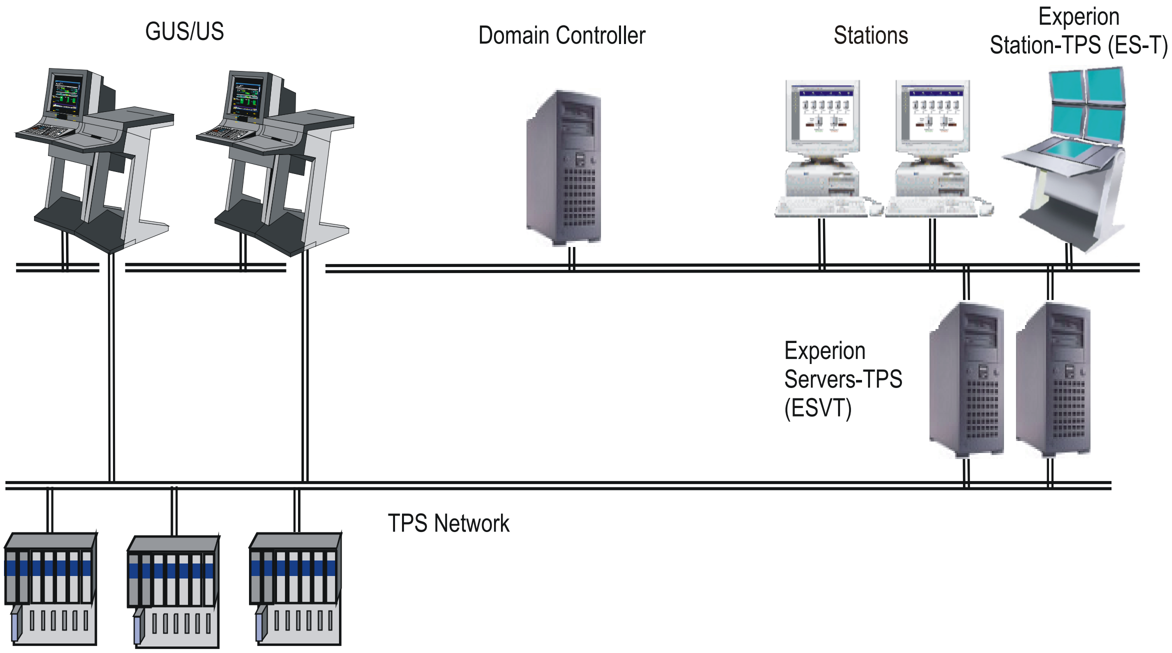


Figure 25: Small integrated system which uses an ESVT for both the Experion and TPS systems

Related topics

"Networks" on page 39

Creating custom applications

The Experion Server API allows you to create two types of custom applications that run on the server: *tasks* and *utilities*.

Tasks are usually dormant, waiting for a request. For example, tasks can be activated:

- On a regular basis
- When a status point changes state
- While a standard point is on scan
- When an operator presses a function key
- When an operator selects a Station menu item
- When an operator clicks a button on a display

Utilities run interactively from the command line, and typically perform administrative functions. A utility can prompt the user for more information and can display information directly to the user through a Command Prompt window.

Custom applications can be written in Visual C/C++ or Visual Basic. The Server API Library incudes libraries of functions, header files, and sample source programs to help programmers create applications.

For more information about the Server API, see the *Application Development Guide*.

Installation and commissioning tasks

Issue	Comments
Installation and configuration	Perform installation and configuration tasks in a logical order, and assign appropriate resources.
Testing	Develop a comprehensive test plan that thoroughly tests each subsystem.
Training	Determine the training needs of operators, and maintenance engineers and production controllers.

Related topics

"Installation and configuration tasks" on page 158

Installation and configuration tasks

The following table lists typical installation and configuration tasks.

The table lists the tasks in approximate order. However, you can perform some tasks in parallel—for example, you can create custom displays and configure controllers at the same time.

For a more complete and detailed list of:

- Installation tasks, see the *Getting Started with Experion Software Guide* and the *Supplementary Installation Tasks Guide*.
- Configuration tasks, see the *Server and Client Configuration Guide*.

Task	For details, see
Purchase required hardware and software for the server and client computers.	*Server and Client Planning Guide*.
Prepare the server and client computers, and install the Experion components.	*Software Installation User's Guide*.
Configure your controllers.	For Process Controllers, see the *Control Hardware Planning Guide* and the *Control Hardware Installation Guide*. For controllers other than Process Controllers, see: • The manufacturer's documentation. • The Experion interface reference for the controller type or communication protocol.
Build your system model and asset model.	• “Enterprise models” section of the *Server and Client Planning Guide* • *Server and Client Configuration Guide*.
Define Flex Stations and printers in Configuration Studio.	*Quick Builder User’s Guide* or Quick Builder's help.
Build your control strategy with Configuration Studio’s Control Builder (for Process Controllers) or Quick Builder (for SCADA controllers).	For Process Controllers, see Control Builder's help. For SCADA controllers, see: • *Quick Builder User’s Guide* or Quick Builder's help. • The Experion interface reference for the controller type or communication protocol.
Create custom displays.	*HMIWeb Display Building Guide* or the associated help.
If applicable, create custom applications.	*Application Development Guide*.
If applicable, write server scripts.	*Server Scripting Reference*.
If applicable, integrate your TPS system(s).	*Integrated Experion-TPS User's Guide*.
Fine-tune your configuration.	*Server and Client Configuration Guide*

Related topics

“Configuration tools” on page 159

“Enterprise models” on page 11

Configuration tools

Experion provides a number of configuration tools and utilities:

Related topics

“Configuration Studio” on page 160
“Experion server utilities” on page 163
“Station” on page 164
“Special-purpose utilities” on page 165
“Installation and configuration tasks” on page 158

Configuration Studio

Configuration Studio provides a central location from which you can configure your Experion system. The individual tools required to configure various parts of your system are integrated with, and launched from, Configuration Studio.

In Configuration Studio, you are provided with a customized list of tasks that you are required to complete to configure your system. When you click a task, the appropriate tool is launched so that you can complete the task.

From Configuration Studio, you can launch a range of configuration tools that include:

- Enterprise Model Builder
- The Alarm Suppression display
- Quick Builder
- Control Builder
- System displays
- HMIWeb Display Builder

Attention

HMIWeb Display Builder creates web-based displays—called HMIWeb displays. If you want to create displays that use the proprietary DSP format, see the separate *Display Building Guide*.

Enterprise Model Builder

Enterprise Model Builder is a graphical tool that you use to define:

- The servers that constitute your system.
- The assets that constitute your asset model.
- Alarm groups for your system.

These definitions constitute the Enterprise Model Database (EMDB).

Related topics

“Enterprise models” on page 11

Alarm Suppression display

The **Configure Alarm Suppression** task in Configuration Studio calls up the **Alarm Suppression** display.

You use this display to configure Dynamic Alarm Suppression (DAS) by creating, modifying and then loading alarm suppression groups to your system’s servers.

Dynamic Alarm Suppression (DAS) is an Experion license option that provides an automated way of temporarily removing alarms from the default (unfiltered) view of the Alarm Summary. Alarms are removed in accordance with a set of rules that you configure. By temporarily removing specific alarms from the Alarm Summary when pre-configured conditions are met, DAS helps operators to focus on the issue at hand or on other more critical conditions in the plant.

For more information, see the *Server and Client Planning Guide* and the *Server and Client Configuration Guide*.

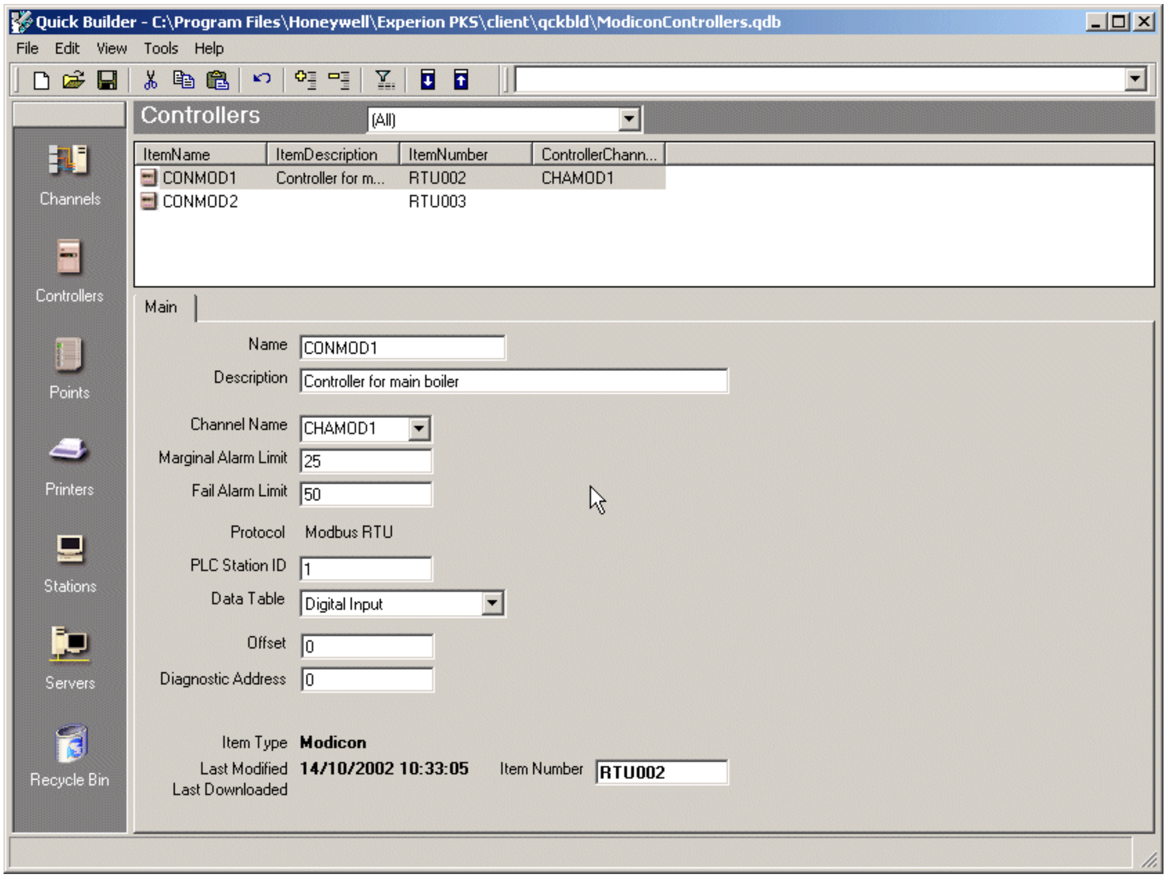
Quick Builder

Quick Builder is a graphical tool for configuring Flex Stations, printers, controllers (other than Process Controllers) and standard points. (If you have Process Controllers, you configure them with Control Builder. For details, see the *Control Building User's Guide*.)

After building hardware and points with Quick Builder, you download these items to the server database.

When you download the data in Quick Builder—or part of it—to the server, it becomes part of the *configuration database*. (The configuration database defines how each component in your system is configured.) If necessary, you can update the data and repeat the download process. Alternatively, you can upload data from the configuration database into Quick Builder, edit it and then download it back to the server.

The procedures you use to build items with Quick Builder are documented in the *Quick Builder User's Guide*.



ItemName	ItemDescription	ItemNumber	ControllerChann...
CONMOD1	Controller for m...	RTU002	CHAMOD1
CONMOD2		RTU003	

Name: CONMOD1
Description: Controller for main boiler
Channel Name: CHAMOD1
Marginal Alarm Limit: 25
Fail Alarm Limit: 50
Protocol: Modbus RTU
PLC Station ID: 1
Data Table: Digital Input
Offset: 0
Diagnostic Address: 0
Item Type: **Modicon**
Last Modified: **14/10/2002 10:33:05**
Item Number: RTU002
Last Downloaded

Figure 26: Quick Builder

Related topics

"Container points" on page 78

Control Builder

Control Builder is a graphical tool for building your control strategy for Process Controllers.

The procedures you use to build your control strategy are documented in the *Control Building User's Guide*.

System displays

The system displays that you can call up in Configuration Studio are used to configure items such as reports, group displays, trends, alarm trackers, Station settings, Console Stations, and so on.

The procedures for configuring these items are documented in the *Server and Client Configuration Guide*.

HMIWeb Display Builder

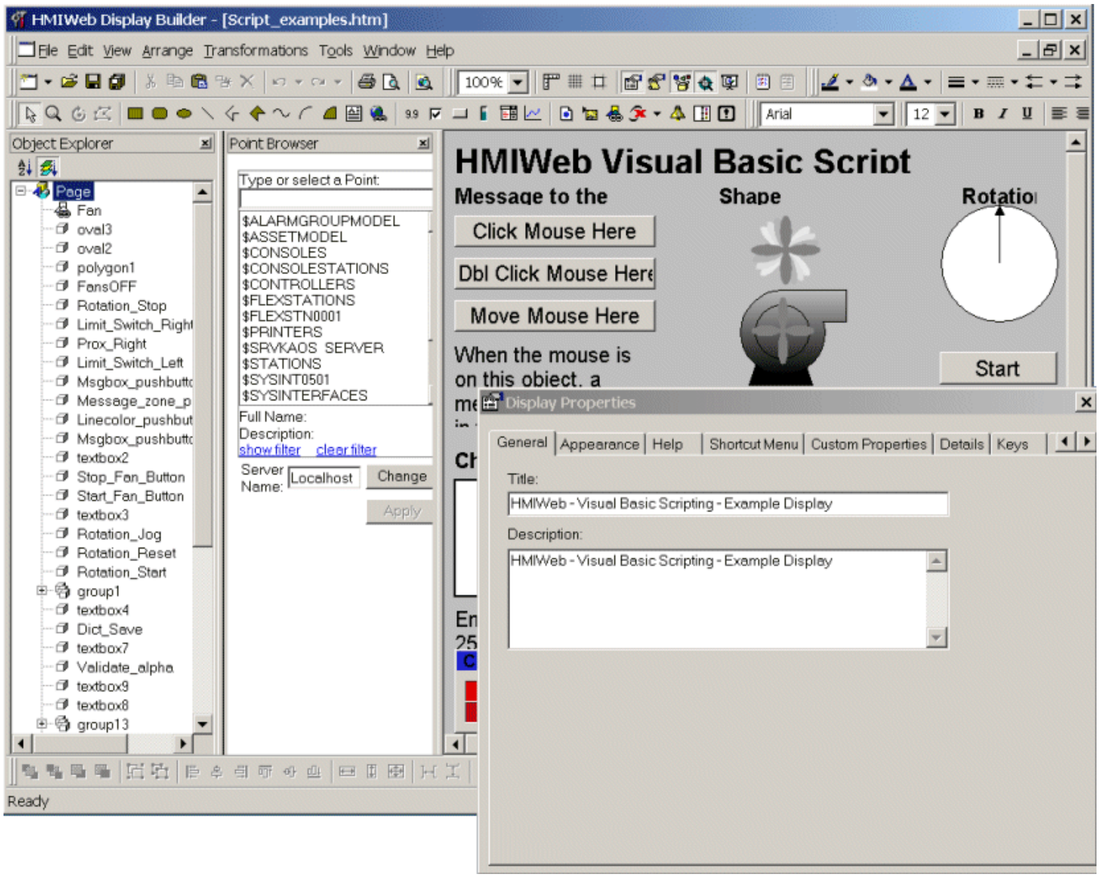
HMIWeb Display Builder is the specialized drawing tool you use to create your own (custom) displays.

Experion also includes Display Builder, which creates displays with a proprietary 'DSP' format. This format was used exclusively in earlier versions of Experion and is still used for some system displays.

Each version is supplied with clip art libraries that cover a range of industries. You can also insert your own graphics, such as photographs and layout diagrams. Each version supports a number of graphic formats, including:

- GIF (*.gif)
- Windows Bitmap (*.bmp)
- JPEG (*.jpg)
- Metafile (*.wmf)
- Portable Network Graphic (*.png)

For more information, see the *HMIWeb Display Building Guide*, or the *Display Building Guide*, or the help.



Title:
HMIWeb - Visual Basic Scripting - Example Display

Description:
HMIWeb - Visual Basic Scripting - Example Display

Figure 27: Typical layout of HMIWeb Display Builder

Experion server utilities

Utilities that run on the server are available to assist you in configuration and administration tasks. Utilities that apply to specific controllers, such as communications testing utilities, are described in the controller references. General utilities are described in “Command reference” section of the *Server and Client Configuration Guide*.

Station

Apart from being the operator interface, Station is also used to 'fine tune' the configuration database after you have downloaded your Quick Builder projects to the server.

Attention

If you use Station to modify the configuration database, it will no longer be synchronized with your Quick Builder projects.

Honeywell strongly advises that you keep your Quick Builder projects synchronized with the configuration database by uploading configuration data from the server at regular intervals.

Special-purpose utilities

Experion includes a comprehensive set of utilities to help you perform specialized tasks, such as diagnosis, communications testing and database initialization. For example, there is a communications test utility for each of the supported controllers.

For details about the controller-related utilities, see the individual *interface references*. For details about the other utilities, see the “Command reference” section of the *Server and Client Configuration Guide*.

Index