Honeywell

Experion PKS
Safety Manager Integration Guide

Release 431

Honeywell

Document	Release	Issue	Date
EPDOC-X119-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.

Copyright 2015 - Honeywell International Sàrl

Contents

About this guide

This guide describes the options and procedures for integrating Safety Manager with Experion.

Revision history

Revision	Date	Description
A	February 2015	Initial release of document.

Intended audience

This guide is intended for engineers and technical staff who need to plan and configure the integration of Safety Manager with an Experion system. It assumes a high degree of technical knowledge about Safety Manager, Experion, and Microsoft Windows, especially time synchronization procedures.

How to use this guide

For information about	Go to
The ways in which you can integrate Safety Manager with Experion, as well as planning considerations and prerequisites.	"Planning considerations for integrating Safety Manager with Experion" on page 7
Configuring data exchange between Safety Manager and an Experion server.	"Integrating Safety Manager with an Experion server" on page 19
Configuring peer-to-peer data exchange between Safety Manager and CEE controllers.	"Integrating Safety Manager with CEE controllers" on page 53
Troubleshooting tips.	"Troubleshooting Safety Manager integration problems" on page 59

Related topics

"Related documents for Safety Manager integration" on page 6

Related documents for Safety Manager integration

The following documents complement this guide.

Safety Manager documents

Document	Description
Safety Manager Planning and Design Guide	Contains planning and design topics applicable to Safety Manager.
Safety Manager Installation and Upgrade Guide	Describes how to install, replace and upgrade the hardware and software for Safety Manager.
Safety Manager On-line Modification Guide	Describes how to modify an application online (that is, 'on-process') in a redundant Safety Manager.
Safety Manager Troubleshooting and Maintenance Guide	Describes troubleshooting and maintenance procedures for Safety Manager.
Safety Manager Software Reference	Describes how to configure the network, hardware, Functional Logic Diagrams (FLDs) and points in Safety Manager.

Experion documents

Document	Description
Peer Control Data Interface Implementation Guide	Describes how you create and configure function blocks in Control Builder for the peer-to-peer data exchange between CEE controllers and devices like Safety Manager that support the Modbus TCP protocol.
Control Hardware Planning Guide	Contains planning and design topics applicable to C300 controllers.
Fault Tolerant Ethernet Overview and Implementation Guide	Gives an overview of FTE and provides planning and implementation details for FTE networks.
Supplementary Installation Tasks Guide	Describes the post-installation tasks for an Experion system including time synchronization procedures.
Server and Client Planning Guide	Contains high-level planning information about Experion server and client functionality. It also includes high-level information about time synchronization.
Server and Client Configuration Guide	Contains detailed configuration procedures for an Experion server and client system.

Planning considerations for integrating Safety Manager with Experion

Before integrating Safety Manager with Experion it is recommended that you consider the following aspects of the integration.

Related topics

"About integrating Safety Manager with Experion" on page 8
"Supported network configurations for Safety Manager integration" on page 10
"Hardware and software requirements for Safety Manager integration" on page 15
"About point configuration in an integrated Safety Manager system" on page 16
"About time synchronization and Safety Manager integration" on page 17

About integrating Safety Manager with Experion

By combining Safety Manager with Experion you can make Safety Manager information available to Experion servers and Stations (the Experion HMI).

You can also integrate your Safety Manager and Experion system by establishing peer-to-peer communication between C300 controllers and Safety Manager controllers.

Note that these two different ways of integrating Safety Manager with Experion are complementary, not mutually exclusive.

Integration approaches	Go to
Direct communication between Safety Manager and an Experion server.	"Direct communication between Safety Manager and an Experion server " on page 8
Peer-to-peer communication between Safety Manager and Experion CEE controllers.	"Peer-to-peer communication between Safety Manager and CEE controllers" on page 8

Related topics

"Direct communication between Safety Manager and an Experion server " on page 8
"Peer-to-peer communication between Safety Manager and CEE controllers" on page 8
"About time synchronization and Safety Manager integration" on page 17
"Hardware and software requirements for Safety Manager integration" on page 15

Direct communication between Safety Manager and an Experion server

The advantages of integrating Safety Manager with Experion are:

- You can monitor Safety Manager diagnostics, system information, sequence of events (SOEs), and point data via Experion HMI (Station).
- You can use existing network infrastructure.

You configure the Safety Manager-to-Experion server communication option as follows.

- Use Safety Builder to configure:
  - The physical and logical connection between Safety Manager and the Experion server.
  - The points whose data you want to exchange with the Experion server.
- Use Configuration Studio to define:
  - A Safety Manager channel
  - The Safety Manager controllers
  - The points you want to integrate

  Note that depending on your requirements, you may need to define several 'logical' controllers to represent the one physical Safety Manager.

Related topics

"Integrating Safety Manager with an Experion server" on page 19
"Supported network configurations for Safety Manager integration" on page 10
"Isolating Safety Manager-to-Experion server communication problems" on page 60

Peer-to-peer communication between Safety Manager and CEE controllers

When you implement peer-to-peer communication between Safety Manager and C300 controllers, Safety Manager data is instantly available to C300 controllers.

The Safety Manager-to-CEE controller peer-to-peer communication uses the Experion Peer Control Data Interface (PCDI). This is a licensable option that enables you to build function blocks in Control Builder to configure the direct data exchange between Safety Manager and CEE controllers. This option supports peer-to-peer communication with analyzers and Programmable Logic Controllers (PLCs) that support the Modbus TCP protocol.

In the PCDI communication relationship, the C300 acts as the master and the Safety Manager acts as the slave. The C300 initiates both reads from Safety Manager and writes to Safety Manager, and the Safety Manager responds as required. Experion PCDI supports C300 redundancy.

Attention

Honeywell recommends that you only use PCDI blocks to configure peer-to-peer points, and that you access normal SCADA data via the Experion server.

Note that Experion PCDI does not support peer-to-peer communication between Safety Manager and C200 controllers or between Safety Manager and ACE. If you want to establish peer-to-peer communication between Safety Manager and ACE, you need to use a C300 controller 'in the middle.'

For practical reasons, Honeywell does not recommend using serial communications. However, if you want to integrate an existing serial Safety Manager with C300 or C200 controllers, see *Application Note, PM.MAN.6528, Peer-to-Peer Communication Safety Manager/FSC - C300/C200*.

For more information about the Experion PCDI, see the *Peer Control Data Interface Implementation Guide*.

Advantages

Because a C300 controller can read 'raw' sensor values directly from the Safety Manager controller, engineering costs are reduced and cost savings are available as a result of sharing sensors between process safety and process control. With peer-to-peer communication C300 controllers can also use calculated (2oo3) data.

Direct data exchange between Safety Manager and a C300 controller can also minimize the impact of a (partial) process shutdown initiated by Safety Manager. In the event of such an emergency shutdown, C300 controllers (both upstream and downstream) can automatically divert the process flow to a parallel train or provide for a 'soft landing' that allows you to manage the downstream shutdown process. It also facilitates a faster process restart.

Other advantages of implementing peer-to-peer communication between Safety Manager and CEE controllers include:

- The ability to use existing (redundant) network infrastructure.
- Communications do not have to pass through the server or any other device.
- Increased speed and reliability of data exchange.

Peer-to-peer communication between Safety Manager and CEE controllers also enables:

- Automatic process interlock from shutdown valve to control valves. This prevents the PID from winding up and the control valve from ramping wide open, thus avoiding a surge when the shutdown valve is subsequently opened.
- The automatic bypass of a low flow or pressure trip on a pump discharge based on the running status of the pump.
- The automatic suppression of alarms in either the C300 or Safety Manager controller when some bypass units are out of service or a trip is in bypass. For example, when Safety Manager trips a pump, you can suppress any alarms relating to an 'uncommanded change.'
- The automatic opening and closing of shutdown valves during a compressor purge sequence.

Related topics

Supported network configurations for Safety Manager integration

The following types of network configurations can be used to integrate Safety Manager with Experion.

Network connection type	Go to:
FTE	"Safety Manager in FTE networks" on page 10
Ethernet	"Safety Manager in Ethernet networks" on page 11

Process data connections to the Safety Manager are made on TCP port 51000. Information scan connections to the Safety Manager are made on TCP port 51001.

> **Attention**
>
> For practical reasons, Honeywell does not recommend using serial communications. However, if you want to integrate an existing serial Safety Manager, see *Application Note, PM.MAN.6528, Peer-to-Peer Communication Safety Manager/FSC - C300/C200*.

Related topics

"Safety Manager in FTE networks" on page 10
"Safety Manager in Ethernet networks" on page 11
"About time synchronization and Safety Manager integration" on page 17
"Hardware and software requirements for Safety Manager integration" on page 15
"Direct communication between Safety Manager and an Experion server " on page 8
"Integrating Safety Manager with an Experion server" on page 19
"About time synchronization and Safety Manager integration" on page 17

Safety Manager in FTE networks

You can have either a redundant or non-redundant Safety Manager connected to CEE controllers in an FTE network.

Redundant Safety Manager in an FTE network

In a redundant Safety Manager FTE network configuration, the USI-0001 communication module in CP1 of the redundant Safety Manager is connected to the FTE network through the yellow switch, and the USI-0001 communication module in CP2 is connected to the network through the green switch, as shown in the following figure.

> **Attention**
>
> When setting up peer-to-peer communication between Safety Manager and a C300 controller, it is recommended that Safety Manager be attached either directly to Level 1 switches (or to the Level 1 side of a split switch). Note that the TCP port must be set to 502 for peer-to-peer communication through a Level 1 switch.
>
> For SCADA access through the Experion server, it is recommended that you connect Safety Manager to Level 2 switches.
>
> For more information about network levels, see the *Network and Security Planning Guide*. For more information on best practices in implementing FTE, see the *Fault Tolerant Ethernet Overview and Implementation Guide*.

When using SCADA access, the switch from CP1 to CP2 will only occur when the fail alarm limit (if configured) on the active link has been reached, or when the active link has been disabled.

Figure 1: A redundant Safety Manager in an FTE network

Non-redundant Safety Manager in an FTE network

In a non-redundant Safety Manager FTE network configuration, the USI-0001 communication module in CP1 of the non-redundant Safety Manager is connected to the FTE network through the yellow switch, as shown in the following figure.
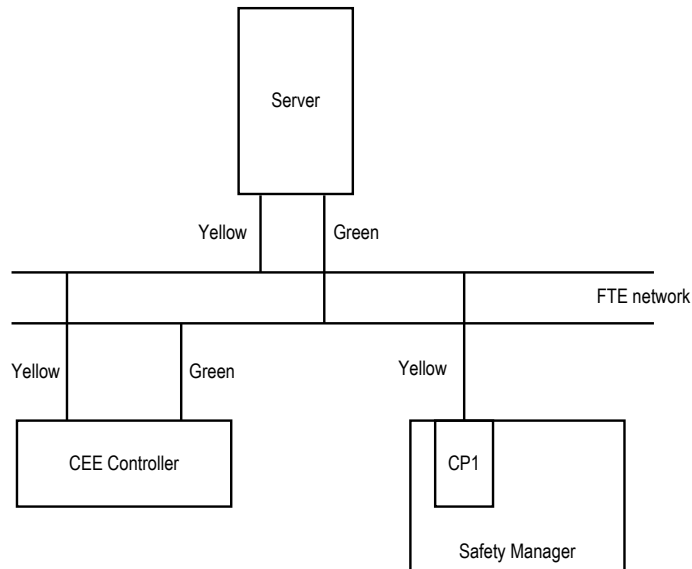
Figure 2: A non-redundant Safety Manager in an FTE network

Related topics

"Safety Manager in Ethernet networks" on page 11

Safety Manager in Ethernet networks

You can have either a redundant or non-redundant Safety Manager in an Ethernet network. For detailed information about supported network topologies, see the controller documentation.

Redundant Safety Manager in a redundant Ethernet network

Note that CEE controllers are not supported on redundant Ethernet (non-FTE) networks.

Where a redundant Safety Manager is in a redundant Ethernet (non-FTE) network, the USI-0001 communication module in CP1 of the redundant Safety Manager is connected to subnet A, and the USI-0001 communication module in CP2 is connected to subnet B, as shown in the following figure.

When using SCADA access, the switch from CP1 to CP2 will only occur when the fail alarm limit (if configured) on the active link has been reached, or when the active link has been disabled.
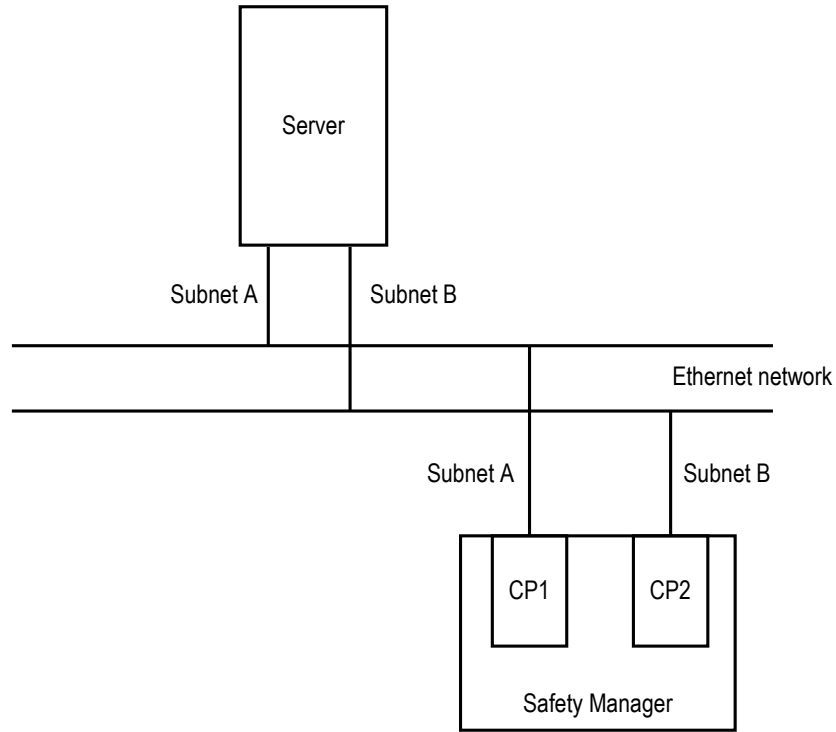
Figure 3: A redundant Safety Manager in a redundant Ethernet network

Redundant Safety Manager in a non-redundant Ethernet network

Note that C300 controllers are not supported on non-redundant Ethernet (non-FTE) networks.

Where a redundant Safety Manager is in a non-redundant Ethernet (non-FTE) network, both CP1 and CP2 are connected to the single Ethernet network as shown in the following figure.

When using SCADA access, the switch from CP1 to CP2 will only occur when the fail alarm limit (if configured) on the active link has been reached, or when the active link has been disabled.
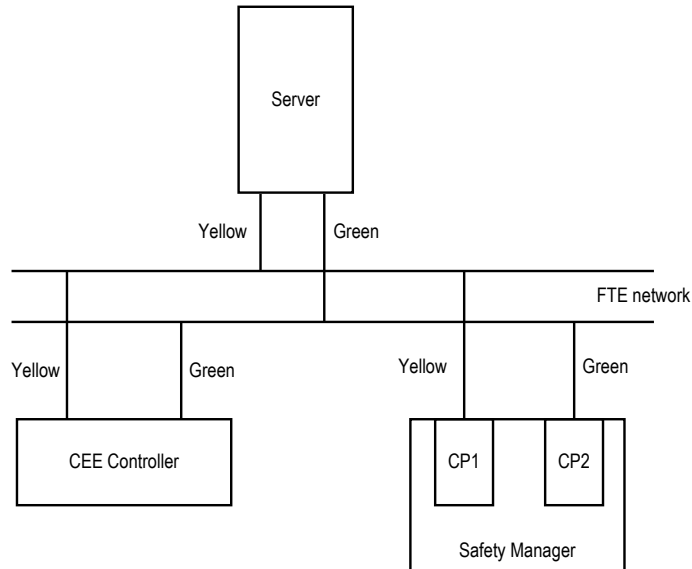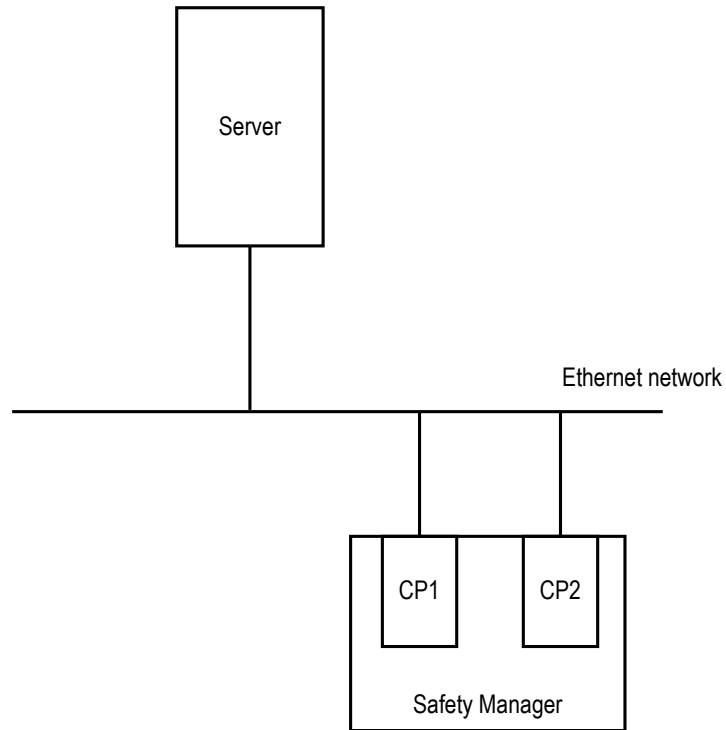
Figure 4: A redundant Safety Manager in a non-redundant Ethernet network

Non-redundant Safety Manager in a non-redundant Ethernet network

Note that C300 controllers are not supported on non-redundant Ethernet (non-FTE) networks.

Where a non-redundant Safety Manager is in a non-redundant Ethernet (non-FTE) network, the USI-0001 communication module in CP1 of the Safety Manager is connected to the network, as shown in the following figure.

Server

Ethernet network

CP1
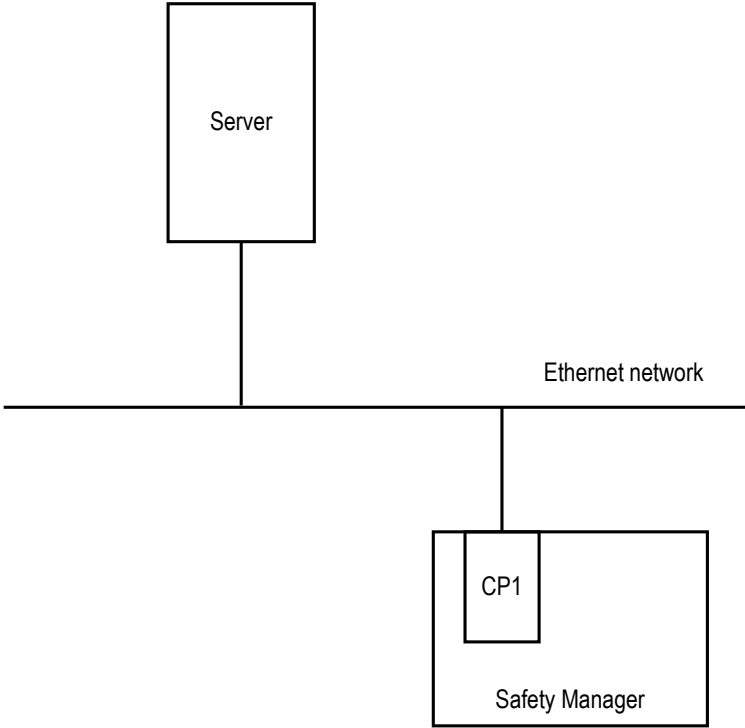
Safety Manager

Figure 5: A non-redundant Safety Manager in a non-redundant Ethernet network

Related topics

"Safety Manager in FTE networks" on page 10

Hardware and software requirements for Safety Manager integration

The hardware and software requirements for integrating Safety Manager with Experion are as follows.

Safety Manager-to-Experion server integration

- Safety Manager with USI-0001 communication module(s).
- Safety Builder.
- An Experion server running Configuration Studio.

Safety Manager-to-CEE controller integration

- Safety Manager with USI-0001 communication module(s) running R130 (or later) firmware.
- Safety Builder R130 (or later) software.
- An Experion server running Configuration Studio.
- Redundant or non-redundant C300 controllers with compatible firmware.
- A license for peer control data interface (PCDI) components.
- SIM-C300 controller for simulation support (optional).

> **Attention**
>
> - The Experion server and CEE controller use the same physical communication port on a USI. Honeywell recommends that you reserve communication port A for the FTE and/or Ethernet connection.
> - There is a limit of eight physical CEE connections per Safety Manager communication channel.
> - Safety Manager cannot be connected to CEE controllers through a CF9 device.

Related topics
"About time synchronization and Safety Manager integration" on page 17
"About integrating Safety Manager with Experion" on page 8
"Supported network configurations for Safety Manager integration" on page 10
"Integrating Safety Manager with an Experion server" on page 19
"Integrating Safety Manager with CEE controllers" on page 53

About point configuration in an integrated Safety Manager system

You can configure points in Safety Manager to be communicated to an Experion server or a CEE controller (or both). You can configure multiple recipients per point.

All of the points in Safety Manager can be configured for communication including system state indicators, diagnostic indicators, time and date indicators, alarms, field I/O states (analog and digital) and communication points.

About configuring fast changing points

When configuring fast-changing points for communication, you need to take into consideration the cycle time differences between sender and receiver.

> **Tip**
> A typical cycle time value in Safety Manager is less than 300 ms. Its exact value depends on the application and system configuration of Safety Manager and can best be indicated with the cycle time calculation tool (offline) or with the Safety Builder online tool (choose **Controller Management > System Info**).

Ideally, the receiver updates faster than the sender, so it never misses a change in state. If a receiver does not update faster than the sender, pulses on field I/O devices and alarms initiated by the sender may go unnoticed. In such situations, latching logic should be used in the sender to capture and extend the duration of a pulse, allowing the receiver to notice its occurrence.

Options for automating point configuration

If you have a large number of points that need to be configured, you can speed up the configuration process by using the automatic allocation tool or by bulk importing points.

For more information on using the automatic allocation tool, see the *Safety Manager Software Reference*. For more information on bulk importing, see the "Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe" topic.

Related topics

"Using Safety Builder to configure points for Safety Manager integration" on page 31
"Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe" on page 38

About communication inputs in an integrated Safety Manager system

In addition to communicating the states of Safety Manager points to an Experion server or CEE controller, you can also create or configure inputs to the safety application to be updated by an Experion server or CEE controller. This input can be a marker or a register type input, and is referred to as a communication input in Safety Manager.

By using peer-to-peer communication between a CEE controller and Safety Manager, communication inputs allow for increased automation and sequencing of supervised interlock and/or start-up procedures that require close interaction between the CEE controller application and the emergency shutdown (ESD) application.

> **Attention**
> Because a safety application's first priority is to safeguard the process, the conditions under which a state or value change of communication inputs can be accepted by Safety Manager must follow applicable safety guidelines such as defined in IEC 61511. These guidelines are partly executed and enforced by the application run by Safety Manager, and partly by the safety integrity of Safety Manager. However, it is the user's responsibility to implement and validate the relevant safety application in line with those guidelines.

Related topics

"Configuring communication inputs for Safety Manager integration" on page 32

About time synchronization and Safety Manager integration

Safety Manager and CEE controllers generate SOE data and timestamp it independently. They then send this data to the Experion server, which collects and catalogs all SOE messages. To ensure that all SOE messages are sorted and displayed in a true chronological manner, Safety Manager and CEE controllers must use the same time source.

Related topics

"Hardware and software requirements for Safety Manager integration" on page 15
"About integrating Safety Manager with Experion" on page 8
"Supported network configurations for Safety Manager integration" on page 10
"Integrating Safety Manager with an Experion server" on page 19
"Supported network configurations for Safety Manager integration" on page 10
"Configuring time synchronization between Safety Manager and Experion" on page 28

Choosing a time source for your integrated system

When integrating Safety Manager with an Experion system, the technical accuracy of the time is not as critical as the consistency of time source. Therefore while a UTC-based time server is the most technically accurate time source, it is neither essential nor the most important consideration.

The recommended approach to time synchronization in an integrated system is to use a single NTP server as the time server for your Experion system (including your CEE controllers, if applicable) and each Safety Manager.
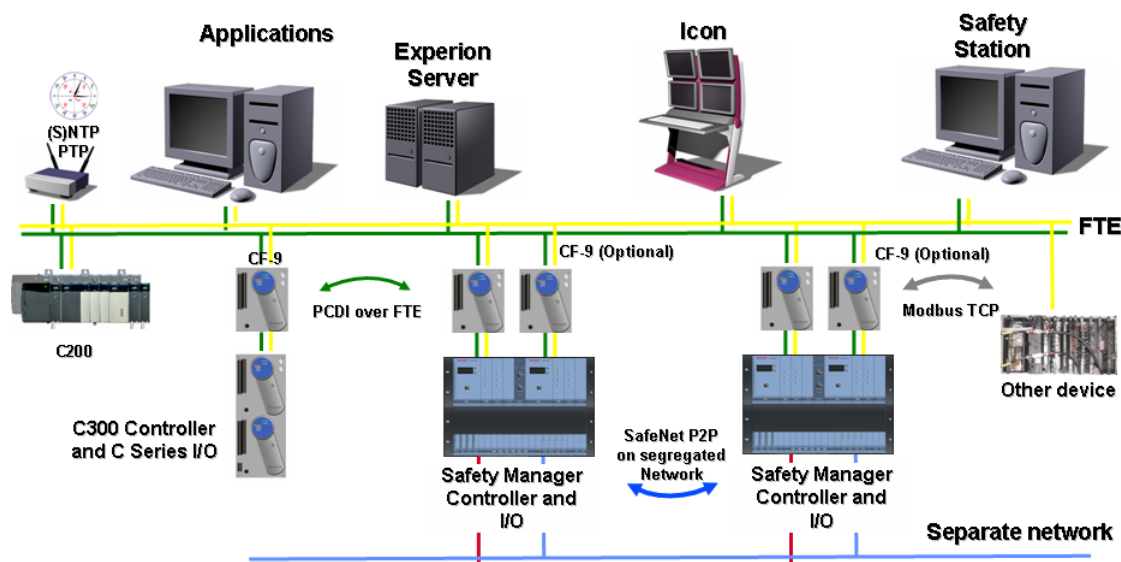
Figure 6: NTP protocol time server in an Experion system

Recommendations and guidelines relating to time synchronization

- As illustrated in the above figure, use an external NTP protocol time server for your Experion system and use the same time server for each Safety Manager linked to the Experion system.
- Alternatively (or as a backup), use the Experion server itself as the time source for each Safety Manager. For more information, see the *Safety Manager Software Reference*.
- Ensure that all systems are configured for the same time zone and have the same daylight savings time settings.

Tip
Time synchronization is a complex topic involving site-specific considerations and customization. If you are not technically proficient in time synchronization procedures, it is strongly recommended that you contact Honeywell Automation College about the training courses available on the use of NTP and time technology in an Experion system.

For more information about time synchronization in an Experion system, see the section titled "Time synchronization" in the Server and Client Planning Guide.

Related topics

"Configuring time synchronization between Safety Manager and Experion" on page 28

Integrating Safety Manager with an Experion server

Use the following checklist to configure the communication between Safety Manager and the Experion server.

Prerequisites

- You have met the hardware and software requirements for integrating Safety Manager and an Experion server (as described in the topic titled "Hardware and software requirements for Safety Manager integration").
- Your Safety Manager system has been configured using Safety Builder as described in the Safety Manager documentation.
- Your Experion system has been installed and configured as described in the Experion documentation.
- You have engineering level (or higher) access to Safety Builder and Experion Configuration Studio.

Tasks

Task	Go to:	Done?
Configure the physical connection between the Experion server and Safety Manager.	"Using Safety Builder to configure the physical connection between Safety Manager and the Experion server" on page 21	
Configure the logical connection between the Experion server and Safety Manager.	"Using Safety Builder to configure the logical connection between Safety Manager and an Experion server node" on page 22	
Configure time synchronization.	"Configuring time synchronization between Safety Manager and Experion" on page 28	
Configure the communication points for Experion server in Safety Manager.	"Using Safety Builder to configure points for Safety Manager integration" on page 31	
(Optional) If you want Safety Manager Sequence of Events (SOE) data included in the SOE log on the Experion server, configure SOE.	"Configuring Safety Manager SOE to be logged on an Experion server" on page 35	
Compile your application.	*Safety Manager Software Reference*	
Load the application in Safety Manager:		
• For on-process loading	*Safety Manager On-line Modification Guide*	
• For off-process loading	*Safety Manager Installation and Upgrade Guide*	
(Optional) If you want to perform a bulk import of Safety Manager channels, controllers, or points into Configuration Studio, use `SM2XperionConverter.exe`. Note that if you use this tool to import all of your Safety Manager details into Configuration Studio, you do not need to carry out the individual steps listed below for defining the Safety Manager channels, controllers, and points.	"Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe" on page 38	

Task	Go to:	Done?
Define a Safety Manager channel in Configuration Studio.	"Using Configuration Studio to define a Safety Manager channel" on page 41	
Define the Safety Manager controllers in Configuration Studio.	"Using Configuration Studio to define Safety Manager controllers" on page 44	
Download the channel and controller definitions to the Experion server.	**Quick Builder User's Guide** > **Getting started with Quick Builder** > **Basic Quick Builder Tasks** > **Downloading items**.	
Check that the server can communicate with the Safety Manager controller.	"Testing Safety Manager communications with the server" on page 61	
Define Safety Manager addresses as points in Configuration Studio. Note that SOE numbers should be assigned to points that match the Safety Manager configuration.	"Using Configuration Studio to define points for Safety Manager integration " on page 47	
Download the points to the Experion server.	**Quick Builder User's Guide** > **Getting started with Quick Builder** > **Basic Quick Builder Tasks** > **Downloading items**.	

Related topics

"Using Safety Builder to configure the physical connection between Safety Manager and the Experion server" on page 21

"Using Safety Builder to configure the logical connection between Safety Manager and an Experion server node" on page 22

"Configuring time synchronization between Safety Manager and Experion" on page 28

"Using Safety Builder to configure points for Safety Manager integration" on page 31

"Configuring Safety Manager SOE to be logged on an Experion server" on page 35

"Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe" on page 38

"Using Configuration Studio to define a Safety Manager channel" on page 41

"Using Configuration Studio to define Safety Manager controllers" on page 44

"Using Configuration Studio to define points for Safety Manager integration " on page 47

"Direct communication between Safety Manager and an Experion server " on page 8

"About time synchronization and Safety Manager integration" on page 17

"Supported network configurations for Safety Manager integration" on page 10

"Isolating Safety Manager-to-Experion server communication problems" on page 60

"Hardware and software requirements for Safety Manager integration" on page 15

"Integrating Safety Manager with CEE controllers" on page 53

"Configuring time synchronization between Safety Manager and Experion" on page 28

"Using Safety Builder to configure the physical connection between Safety Manager and a CEE controller" on page 55

Using Safety Builder to configure the physical connection between Safety Manager and the Experion server

To configure the Safety Manager side of the physical connection to Experion you use the Network Configurator in Safety Builder to define:

- The device with which Safety Manager is communicating.
- The physical communication address.
- The communication channels and protocols.

To configure the physical connection

1   Start Safety Builder and open **Network Configurator - Physical View**.

2   Drag the **Experion server** icon from the button bar in the **Work** area and connect it to the **Plant** icon.

3   In the **Experion server** dialog box type a unique name for the Experion server and click **OK**.

4   If you have already created a Physical Connection to the FTE or Ethernet network, proceed to step .
     If you have not yet created a Physical Connection to the FTE or Ethernet network:

   a   Drag a **Physical Connection** icon from the button bar and connect it to the Experion server.

   b   Type a unique name for that network connection to the Experion server in the **Physical Network Properties** dialog box.

   c   If you have a switch between Safety Manager and the FTE/Ethernet, set the **Baud** according to the switch settings.

   d   Click **OK**.

   e   Proceed to step .

5   Drag a suitable (existing) Physical Network Connection from the Explorer bar, connect it to the Experion server.

> **Attention**
>
> By connecting an existing Physical Network Connection to the Experion server you automatically connect the Safety Manager controller that has been configured at the other end of the network connection to that Experion server.

6   If a Safety Manager controller is already configured at the other end of the selected network connection, you have finished configuring the physical connection.

     If you have not yet configured a Safety Manager controller at the other end of the selected network connection, drag an existing Safety Manager controller from the Explorer bar and connect it to the physical network. (If you have not yet configured a Safety Manager controller, refer to the procedures in the *Safety Manager Software Reference*.)

> **Tip**
>
> If you cannot connect the Safety Manager controller from the Explorer bar, this means that the Safety Manager controller has no suitable (or free) communications channel available.
>
> In that case, free a suitable communication channel (channel A on a USI-0001 communication module) or add another USI-0001. For details, see the *Safety Manager Software Reference*.

Related topics

Using Safety Builder to configure the logical connection between Safety Manager and an Experion server node

Use the following procedure to configure the logical connection between Safety Manager and an Experion server node, that is, between:

- Safety Manager and an Experion server.
- Safety Manager and a CEE controller.

Prerequisites

- You have already configured the physical connection of the Experion PKS via Safety Builder (see the topics titled "Using Safety Builder to configure the physical connection between Safety Manager and the Experion PKS server" and "Using Safety Builder to configure the physical connection between Safety Manager and a CEE controller").

To configure the logical connection between Safety Manager and an Experion server node

1 Start Safety Builder and open **Network Configurator - Logical View**.

2 To add all the necessary logical connections, click the **Add Logical Connections** button to insert a new empty row in the grid.
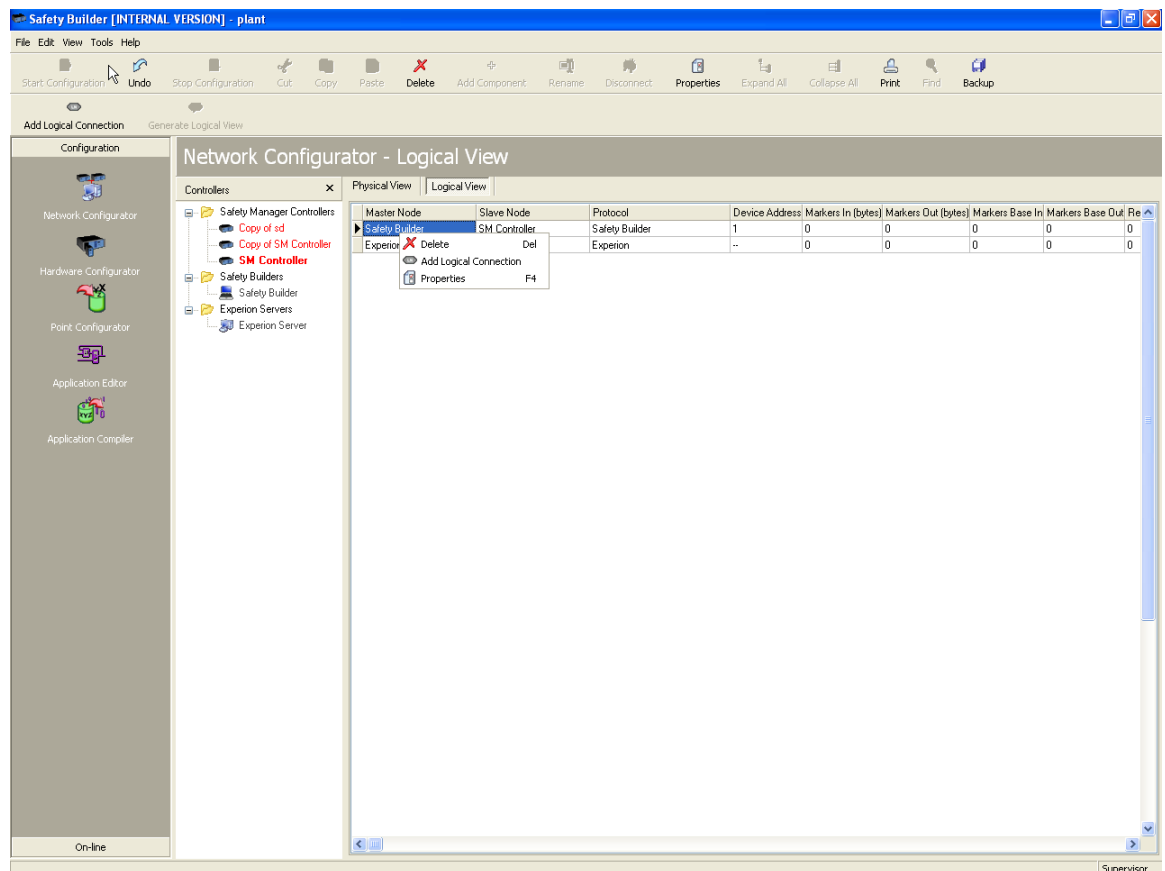

Figure 7: Network Configurator - Logical View

3 Right-click the new row inserted in the grid to display the popup menu and choose **Properties**. The **Logical Network Properties** dialog box appears.

4 Use the **Logical Network Properties** dialog box to configure the communication range for Safety Manager-to-Experion server (or Safety Manager-to-CEE controller communications).

Related topics

Logical Network Properties settings

You use the Logical Network Properties dialog box to define the logical network properties for each logical communication link (that is, for each Safety Manager-to-CEE controller communication link and each Safety Manager-to-Experion server communication link) by defining the following data exchange properties:

- The logical link.
- The response to link failure.
- The communication capacity that Safety Manager has to reserve for each point type.
- The communication base addresses per point type. (The communication base address is the lowest PLC address, that is, the PLC address of the first marker/register in.)

📝 **Tip**
The properties Marker In, Marker Out, Register In, Register Out, PLC Base In, and PLC Base Out for both Markers and Registers, and Network Delay, Enable Slave Timeout, Timeout, and Device Address can be configured by using the grid itself or the **Logical Network** properties dialog box.

Complete the Logical Network Properties dialog box as suggested in the following table. Note that the following settings and recommendations apply whether you are connecting Safety Manager to an Experion server or to a CEE controller.

Property	Description
Master Node	Select an Experion node as a master node for the logical link.
	If it is read-only, the logical link has already been defined.
Slave Node	Select a Safety Manager controller as a slave node to the Experion node.
	If the box is read-only, the logical link has already been defined.
Protocol	This box automatically displays the protocol used by the master and slave node selected by the user. However, for clock sources, users can choose between NTP and PTP.
Route	Lists the available communication paths between master and slave. If only one path is available, it is selected automatically and the box is read-only.
Device Address	Specify the (logical) connection to Safety Manager. Safety Manager ensures that this address is unique for each configured logical connection. For more information, see the section below titled "Device Address values."
Marker: In size	Defines the allocation pool of the marker-in buffer (that is, the number of bytes reserved in memory for coil data received from the Experion server or CEE controller).
	The Marker In size must be a multiple of 4.
Markers: Out size	Defines the allocation pool of the marker-out buffer (that is, the number of bytes reserved in memory for coil data sent to the Experion server or CEE controller).
	The Marker Out size must be a multiple of 4.
Markers: PLC base in Markers: PLC base out	These boxes display the base address for the Marker In/Marker Out. The following address ranges apply: • CEE controller: the PLC address can be from 1 to 65,535 • For an Experion server, digital input and digital output point types (coils) can be assigned in the range 1 to 8,192. Note that the first 32 addresses are reserved for system markers.
Registers: In size	Defines the allocation pool of the register-in buffer (that is, the number of bytes reserved in memory for binary input point data received from the Experion server or CEE controller). The Register In size must be a multiple of 4.
Registers: Out size	Defines the allocation pool of the register-out buffer (that is, the number of bytes reserved in memory binary output point data sent to the Experion server or CEE controller). The Register Out size must be a multiple of 4.

Property	Description
Registers: PLC base in Registers: PLC base out	These boxes display the base addresses for the Register In and Register Out. Valid address ranges for a CEE controller are as follows: • The PLC address can be from 1 to 65,535. • Long words and floats have 2 PLC addresses assigned. • The address ranges (4)9996–(4)9999 are reserved for clock synchronization. For PCDI, this only applies if the clock source option has been selected. Even with the clock source option selected, this address range can still be used. • For an Experion server, digital input and digital output point types (coils) can be assigned in the range 1 to 8,192. Valid address ranges for an Experion server are as follows: • The PLC address can be from 10,001 to 18,192. • Long words and floats have 2 PLC addresses assigned. Note that the first four addresses are reserved for system registers.
Enable timeout	Use this check box to specify whether or not you want to define a timeout value. If timeout is enabled, and no communication takes place during the defined timeout period, Safety Manager sets a diagnostic marker and generates a diagnostic message. For more information, see the *Safety Manager Software Reference*.
Timeout	If you have enabled timeout, use this box to specify the maximum time-out value (in ms) in this box. **Attention** • Note that for an Experion server, the timeout value must be greater than 25000 ms to ensure that the controller does not disconnect the Experion server from the non-active link between the diagnostic scans that occur every 20 seconds. • For a Safety Manager to CEE controller link, it is recommended that you set the timeout value as follows: Take the configured time-out in the CEE controller, multiply this value by 3, and add one second. The resulting value is the time-out to be filled in the SM Controller Communication timeout (ms) box.
Network delay	This is the network delay for the logical connection, specified in milliseconds. The maximum value permitted is 32,767.

Device Address values

The following table describes the settings for Device Address values in the **Logical Network Properties** dialog box.

Application protocol	Device type	Device address
Modbus	DCS	Modbus slave device ID = 1–247
PCDI[1]	CEE controller	The device address can increment by 1.
CDA		FTE node number of the CEE controller or Experion server (range 1–509)
	Experion server	The device address can increment by 2. As it starts from 1, the next valid value should be 3, 5, and so on.

---

[1] PCDI is a licensed option for Experion and initially only available for C300 controllers, and not C200 or ACE nodes.

Application protocol	Device type	Device address
PlantScape		N.A.
SafeNet	Safety Manager Controller	N.A.
FSC-DC	Safety Builder	Safety Builder ID 1–63.
NTP	External Clocksource	N.A.
PTP		

Related topics

"Using Safety Builder to configure the logical connection between Safety Manager and an Experion server node" on page 22

"Using Safety Builder to configure points for Safety Manager integration" on page 31

"Determining the allocation size for markers" on page 26

"Determining the allocation size for registers" on page 26

"Using Control Builder to configure the PCDI components for Safety Manager" on page 56

Determining the allocation size for markers

Determining the allocation size for markers involves calculating the number of bytes required for coils received by Safety Manager ('markers in') and coils transmitted by Safety Manager ('markers out'). Each byte can contain up to 8 markers (or coils). The allocation size for markers must be a multiple of 4 bytes.

To determine the allocation size for markers in and out

1   Determine the number of coils (markers) that need to be communicated.

2   Add a percentage of spare coils (markers).

> **Attention**
> Make sure that you allocate sufficient spare capacity for future expansion as changing buffer sizes while systems are on-process can result in a temporary loss of communication.

3   Divide the total number of bytes by 8 and round up the result to a multiple of 4.

Example

1. You need to communicate 110 coil states to Safety Manager and you need 30% spare capacity. That makes a minimum buffer space for 143 coils.

2. 143 divided by 8 equals 18 bytes (rounded up).

3. Rounding up to a multiple of 4 gives a buffer size of 20 bytes (capable of containing 160 coils). You therefore specify the size of the 'marker in' buffer to be *20*.

Related topics

"Determining the allocation size for registers" on page 26

"Logical Network Properties settings" on page 23

Determining the allocation size for registers

Word format registers consume 2 bytes. Long word or float formatted registers consume 4 bytes. The allocation size for a register must be a multiple of 4.

Determining the allocation size for registers involves calculating the number of bytes required for words, long words or floats received by Safety Manager ('register in') or transmitted by Safety Manager ('register out').

To determine the allocation size for registers in and out

1 Determine the number of words that need to be communicated and multiply by 2.

2 Add the number of long words and floats that need to be communicated, and multiply that number by 4.

3 Total these numbers and add a percentage for spare registers.

> ! **Attention**
> Make sure that you allocate sufficient spare capacity for future expansion as changing buffer sizes while systems are on-process can result in a temporary loss of communication.

4 Round up the result to a multiple of 4.

Example

You need to forward 42 analog signals from Safety Manager and 5 register values. You have a requirement for 30% spare capacity.

The format of register values is determined by the safety application and can be anything from byte to float. (Bytes are sent as a word.)

Analog signals are 12-bit RAW values sent in a word format (655 representing 4 mA, 3,276 representing 20 mA). The receiving end should convert these values to engineering units before processing.

Words are used for all analog signals. After investigating the background and usage, you find that the 5 register values are floats.

You now calculate as follows:

1. 42 words times 2 equals 84.
2. 5 floats times 4 equals 20.
3. Adding both numbers gives a total of 104 bytes that must be reserved to forward register values.
4. Add 30% spare capacity to get a total of 136 bytes (rounded up).
5. As this is an exact multiple of 4, you can enter *136* as the size for the 'register out' buffer.

Related topics

Configuring time synchronization between Safety Manager and Experion

This topic lists the tasks for configuring time synchronization between Safety Manager and Experion.

> **Tip**
> Time synchronization is a complex topic involving site-specific considerations and customization. If you are not technically proficient in time synchronization procedures, it is strongly recommended that you contact Honeywell Automation College about the training courses available on the use of NTP and time technology in an Experion system.

Prerequisites

- You have read the information in the topic titled "About time synchronization and Safety Manager integration."
- You have read the information in the 'Time synchronization' topic in the *Server and Client Planning Guide*.
- You have decided on the time source for your system, as recommended in topic titled "Choosing a time source for your integrated system."

Tasks

Task	Go to:	Done?
Configure the time synchronization for your Experion system (including your CEE controllers, if applicable)	"Setting up time synchronization" in the *Supplementary Installation Tasks Guide*	
Synchronize each Safety Manager to the same master time source used by the Experion system. Alternatively, use the Experion system itself as the master time source. Note that each Safety Manager (whether standalone or whether network-connected via SafeNet) needs to be synchronized with Experion.	"Configuring Safety Manager clock synchronization" on page 28	

Related topics

Configuring Safety Manager clock synchronization

Use one of the following recommended methods for synchronizing Safety Manager clocks:

- Set up a link to the primary (S)NTP-based plant clock that synchronizes Experion PKS server.
- Alternatively (or as backup) set up a link to either:
  - The Experion PKS server using the Experion PKS (or PlantScape) clock synchronization mechanism.
  - The SafeNet time master (note that this is only possible when this Safety Manager is a slave in a SafeNet network).

> **Attention**
> If you choose to use the last of these methods, you must ensure that Safety Manager is connected to SafeNet and is not the SafeNet time master. Time masters feed the clock synchronization signal onto SafeNet. To configure a time master, choose one of the other synchronization methods above.

To set up a clock sync link to an (S)NTP-based plant clock

1   Start Safety Builder, open **Network Configurator** and click the **Physical View** tab.

2   Drag an **External Clocksource** from the button bar and connect it to the Plant.
    The **External Clocksource** properties window opens.

3   Type a unique clock name and click **OK**.

4   Drag a suitable FTE connection from the Explorer bar and connect it to the clock. This automatically connects the underlying Safety Manager.

5   Go to the Logical View (click the **Logical View** tab), and click **Add Logical Connection** button.

6   Right-click the connection to display the popup menu and choose **Properties**.
    The **Logical Network Properties** dialog box appears.

7   In the **Logical Network Properties** dialog box, select the (S)NTP-based clock as the master node and the Safety Manager controller as the slave node. Then select **NTP** as the communication protocol (that is, the default value) and click **OK**.

8   Return to the Physical View (click the **Physical View** tab).

9   Open **External Clocksource Properties**, complete the IP address of the primary (S)NTP-based clock server, and then click **OK**.

10 Now that you have built a link to an external clock source, you need to rank its priority to '1', as the NTP clock server is the preferred synchronization source. You do this as follows:

    a   In Network Configurator, click the **Physical View** tab, open the **SM Controller Properties** window and click the **Clock Sources** tab.

    b   There are three clock source priority drop-down boxes. Set the NTP-based clock source in the **Clock source priority 1** drop-down box and click **OK**. (Relocate lower ranked clock sources to box 2 and 3 if necessary.)

11 As you have now included a link to an NTP clock source, you must also set the local time zone, as an NTP server sends 'global' UTC synchronization signals. To set the correct time zone:

    a   In **Network Configurator**, click the **Physical View** tab and open **Plant Properties**.

    b   Set the time zone and date format appropriate for your region and click **OK**.

To set up a clock sync link to Experion PKS server via the Experion PKS/PlantScape protocol

1   Ensure that clock synchronization via the Experion PKS/PlantScape protocol is enabled in the Experion PKS server.

2   Start Safety Builder, open **Network Configurator** and click the **Physical View** tab.

3   Open **Experion PKS Server Properties** and select the **Clock source allowed** check box.

4   The default clock source timeout is set to 26 hours. Change this if necessary, but make sure it remains higher than the actual synchronization frequency and click **OK**.

5   You now need to rank the Experion PKS clock source priority:

    a   In **Network Configurator**, click the **Physical View** tab, open the **Safety Manager Controller Properties** window and click the **Clock Sources** tab.

    b   You have three clock source priority boxes. The NTP-based clock source is set as clock source priority 1. Set the Experion PKS clock as the second priority clock source and click **OK**.

To set up a clock sync link to the SafeNet time master

1   Start Safety Builder and open **Network Configurator - Physical View**.

2   Open the **Safety Manager Controller Properties** and click the **Clock Sources** tab.

3   You have three clock source priority boxes. The NTP-based clock source is set as clock source priority 1.

4   Set the SafeNet time master (another SM Controller) as lowest priority clock source and click **OK**.

Using Safety Builder to configure points for Safety Manager integration

To configure a point in Safety Manager for integration with an Experion server or a CEE controller based on PCDI, you need to assign a logical connection and a PLC address.

The following procedures are specific to configuring points for the Safety Manager integration options. They do not cover the general configuration options and settings for configuring a point in Safety Manager, which are described in the *Safety Manager Software Reference*.

> **Tip**
>
> Instead of configuring individual points as described in the following procedure, you can use the bulk configuration option of the automatic configuration wizard or Safety Builder's import/export functions. For details, see the Safety Manager Software Reference.

Prerequisites

- You have configured a communication link.
- You have used the **Logical Network Properties** dialog box to allocate space to store point data for communication details.

To configure a point in Safety Manager

1   Open **Point Configurator** in Safety Builder.

2   Select the point that you want to configure for communication.

3   In the **Point Properties** window, select the first empty **Output** row in the **Communication allocation** box.

4   Use the **Logical connection** list to choose the external device (CEE controller or Experion server) to which you want this point to communicate.

5   In the **PLC address** box, choose the PLC address that you want to allocate this point to. This address must correspond to the index or address used in the CEE controller or Experion server for that point.

> ❗ **Attention**
> When configuring points for the Safety Manager integration options, you must ensure that the point type, format (word, float, digital etc.) and index or address of the points are identical in both the source and destination.

6   If the point needs to communicate to another external device, repeat steps to for the additional device.

Related topics

"About point configuration in an integrated Safety Manager system" on page 16

"Using Safety Builder to configure the logical connection between Safety Manager and an Experion server node" on page 22

"Logical Network Properties settings" on page 23

"About PLC addresses" on page 33

Configuring communication inputs for Safety Manager integration

You can use communication inputs to configure inputs to the safety application that can be updated by CEE controllers or the Experion server.

To configure communication inputs

1   Open **Point Configurator** in Safety Builder.

2   Select or create an input point that you want to configure for communication.

The location for this input point must be *COM*. If the location is not shown as *COM*, you will not see an input row in the **Communication allocation** box.

3   In the **Point Properties** window, select the input row in the **Communication allocation** box and use the **Logical connection** list to choose the communication path that you want to use for updating the input state.

4   In the **PLC address** box, choose the PLC address that you want to allocate this point to. This address must correspond to the Modbus or DCS address used in the CEE controller or Experion server for that point.

> ❗ **Attention**
> When configuring points for the Safety Manager integration options, you must ensure that the point type, format (word, float, digital etc.) and PLC address of the points are identical in both the source and destination.

5   From the **Fault Reaction** list, choose the required type of response to the safety application, in the unlikely event that the communication link fails:

   •   If the input is digital you can choose between *Low*, *High*, and *Freeze*.

   •   If the input is numeric or float you can choose between *Fixed value* and *Freeze*. If you choose *Fixed value*, you must also enter the fixed value in **Value** box.

> **Tip**
> Choose the value that steers your process away from a dangerous state.

Related topics

"About communication inputs in an integrated Safety Manager system " on page 16
"About PLC addresses" on page 33

About PLC addresses

The PLC address is a unique, predetermined range and address allocation that is used for communicating to both systems.
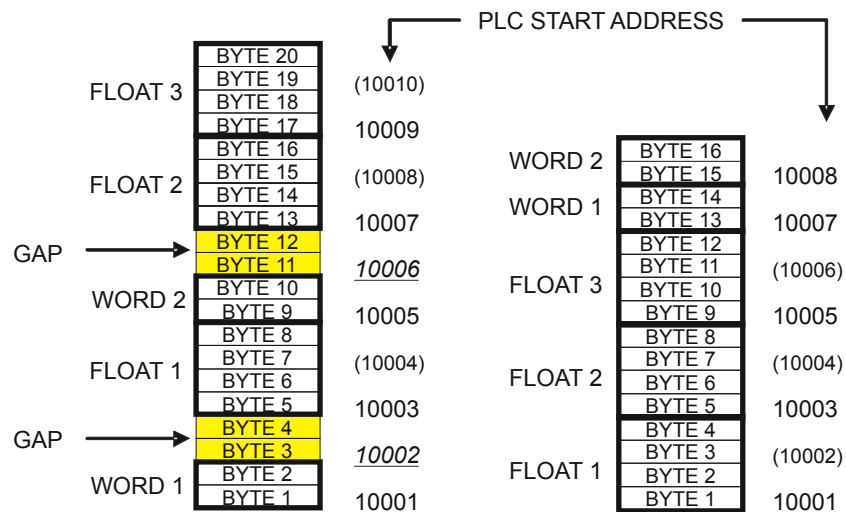
> **Attention**
> Changing or expanding an address range (buffer size) while systems are online results in a temporary loss of communication.

The following rules and guidelines apply to determining the PLC address range.

For	Rules and guidelines
Digital points (markers)	The base PLC address is the start address for allocating digital communication inputs.
	Each digital communication input (marker in) consumes one PLC address.
	The start address for allocating digital signals to other devices (marker out) starts at: base address + 8 x marker in size. This address minus one is the last address for allocating digital communication inputs.
	The last address for allocating digital signals to other devices (marker out) is: base address -1 + 8 x (marker in + marker out size).
Registers	The base PLC address is the start address for allocating register communication inputs.
	Each word of a register communication input (register in) consumes one PLC address.
	Note that long words and floats therefore consume two PLC addresses: to address a long word or a float you must use the lowest PLC address.
	The start address for allocating registers to other devices (register out) starts at: base address + register in size / 2. This address minus one is the last address for allocating register communication inputs.
	The last address for allocating registers to other devices (register out) is: base address -1 + (register in + register out size) / 2.

It is regarded as good practice to:

* Consume PLC addresses in blocks and not leave gaps.
* Avoid mixing allocation of words, long words and floats in a register buffer. The difference between configuring a mixed allocation and a per register type of allocation is shown in the figure below, which demonstrates how mixing allocations consumes more buffer space.

PLC START ADDRESS

FLOAT 3	BYTE 20	
	BYTE 19	
	BYTE 18	(10010)
	BYTE 17	10009
FLOAT 2	BYTE 16	
	BYTE 15	(10008)
	BYTE 14	
	BYTE 13	10007
GAP →	BYTE 12	
	BYTE 11	*10006*
WORD 2	BYTE 10	
	BYTE 9	10005
FLOAT 1	BYTE 8	
	BYTE 7	(10004)
	BYTE 6	
	BYTE 5	10003
GAP →	BYTE 4	
	BYTE 3	*10002*
WORD 1	BYTE 2	
	BYTE 1	10001

WORD 2	BYTE 16	
	BYTE 15	10008
WORD 1	BYTE 14	
	BYTE 13	10007
FLOAT 3	BYTE 12	
	BYTE 11	(10006)
	BYTE 10	
	BYTE 9	10005
FLOAT 2	BYTE 8	
	BYTE 7	(10004)
	BYTE 6	
	BYTE 5	10003
FLOAT 1	BYTE 4	
	BYTE 3	(10002)
	BYTE 2	
	BYTE 1	10001

Related topics

"Configuring communication inputs for Safety Manager integration" on page 32
"Using Safety Builder to configure points for Safety Manager integration" on page 31

Configuring Safety Manager SOE to be logged on an Experion server

If you want an Experion server to record the Safety Manager's sequence of event (SOE) data in the Experion PKS SOE log, you need to incorporate the following procedures into the main integration tasks.

Prerequisites

• You have set up time synchronization on your Safety Manager and Experion systems (see the topic titled "Configuring time synchronization between Safety Manager and Experion").

Tasks

Task	Go to:	Done?
Enable SOE collection in Safety Manager and set a unique SOE ID range. If you want the Experion server to record and log SOE messages from various Safety Managers, you need to make sure that these Safety Managers do not have overlapping SOE ranges.	"Enabling SOE collection in Safety Manager and setting a unique SOE ID range" on page 35	
Assign a unique SOE ID to each SOE-enabled point in Safety Manager.	"Enabling SOE collection in Safety Manager and setting a unique SOE ID range" on page 35	

Related topics

"Enabling SOE collection in Safety Manager and setting a unique SOE ID range" on page 35
"Assigning a unique SOE ID to each SOE-enabled point in Safety Manager" on page 36
"SOE log entries reference" on page 36
"SOE log entries reference" on page 36
"Configuring time synchronization between Safety Manager and Experion" on page 28
"Safety Manager controller Main properties" on page 44
"Ethernet data tables" on page 49
"About data format scaling" on page 50
"Scanning guidelines for Safety Manager controllers" on page 51
"Address syntax for coils and registers" on page 48
"Floating point data formats for a Safety Manager" on page 49
"Address syntax for SOE-only points" on page 49

Enabling SOE collection in Safety Manager and setting a unique SOE ID range

To enable SOE collection in Safety Manager and set a unique SOE ID range

1 Start Safety Builder and open **Network Configurator - Physical View**.

2 Right-click the Safety Manager controller to display its pop-up menu and choose **Properties**.

3 Click the **SOE** tab and check **SOE enable**.
   The **SOE ID Range** settings are displayed on the **SOE** tab.

4 Use the **SOE ID Range** to set the minimum and maximum SOE ID boundaries for this Safety Manager. (Note that IDs 0–15 are reserved.)

   • The SOE ID range determines the maximum number of Safety Manager points that can be SOE-enabled. Note that force-enabled Safety Manager points are also SOE-enabled and that the first five SOE IDs are reserved for system events.

- If the Experion PKS server collects and logs SOEs from multiple Safety Managers, the SOE ID ranges of these Safety Managers may not overlap.

> **Tip**
> Set an SOE ID range that includes the unique Safety Manager ID number (between 1 and 63).

```
Set SM Controller_10 to use SOE range 10.000–10.999
Set SM Controller_12 to use SOE range 12.000–12.999
Set SM Controller_63 to use SOE range 63.000–63.999
```

5 Click **OK**.

You are now ready to enable SOE on each Safety Manager point that requires event recording.

Assigning a unique SOE ID to each SOE-enabled point in Safety Manager

Prerequisites

- You have enabled SOE and set the SOE ID range in Safety Manager.
- You have prepared a list of points that should be SOE enabled.

  Note that it is not wise to set all points to be SOE-enabled. To create a useful SOE log you should carefully consider which points should be logged. It is recommended, for example, that you do not log continuously changing points.

To assign a unique SOE ID to each SOE-enabled point in Safety Manager

1 Start Safety Builder and open **Point Configurator**.

2 Select the point that you want to SOE-enable.

3 In the Point Properties sheet, select the **SOE enable** check box.

Safety Builder automatically assigns a free SOE ID to this point.

4 Repeat steps and until all the required points are SOE-enabled.

SOE log entries reference

The following table describes the fields that appear in the server's SOE log for each SOE.

Field	Description
Date & Time	The date and time given to the SOE by the Safety Manager.
Source	The server's point ID that corresponds with this SOE.
Condition	The Safety Manager SOE number associated with this SOE.
Action	The contents of this field depend on the types of SOE, as specified in the following table.
Description	The server's point description.
Value	The value returned in the SOE (if applicable). For a status point built against a coil, this displays the appropriate state descriptor for that point. Indeterminate values display either blank or zero.

Table 1: Action descriptors for SOE types

Event type	Safety Manager data type	Safety Manager description	Descriptor in the Action field of SOE log
Event report[2]	Any		--[3]

---

[2] System events.

Event type	Safety Manager data type	Safety Manager description	Descriptor in the Action field of SOE log
Process variable event	Boolean	True to False	F
		False to True	T
	Analog	LowLow	LL
		Low	LO
		Healthy	HLT
		High	HI
		HighHigh	HH
Process variable force event	Boolean	Force Set	SET
		Force Cleared	CLR
	Analog	Force Set	SET
		Force Cleared	CLR
Diagnostic event	Diagnostic Event		--

Related topics

"Configuring Safety Manager SOE to be logged on an Experion server" on page 35

---

[3] Actions that are not applicable or indeterminate appear as '--'.

Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe

For the bulk importation of Safety Manager points and other data into Experion, you can use *SM2XperionConverter.exe*. This tool is available on the System Builder software media.

With this tool there are two ways of creating the *pnt* and *hdw* files for Experion:

- Using the plant and controller file.
- Using a point export file.

  To use this option, you first need to export your point database, converting it to an *.xls* file.

Prerequisites

- You are familiar with the concepts of *pntb1d* and *hdwb1d* files and how you can import them into Experion. For more information about *pntb1d* and *hdwb1d* files, see the *Hardware and Point Build Reference*.

To import Safety Manager points and other data using SM2XperionConverter.exe

1 Run *SM2XperionConverter.exe*
   This displays the **Safety Manager-Experion Database Converter** dialog box.

2 To import the points from a plant and controller file:

   a Click the **Safety Manager database** tab.

   b Click **Select Plant**, browse to the appropriate location and select the appropriate plant database file (the file format is *filename.cac*).

   c Click **Select Controller**, browse to the appropriate controller and select it.

   Alternatively, you can export your Safety Manager point database in *.xls* format, and then export it by clicking the **Safety Manager Export file** tab, and then clicking **Select Export** file and choose the *.xls* file from Point Configurator.

3 Click **Config**.
   The **Configuration** dialog box appears.

4 On the **Safety Manager Controller** tab:

    a Choose the controller number of the Safety Manager.

    b Choose the appropriate redundancy option.

    c Type the names and parameter details of the controller, channels, time synchronization and area.

5 Click the **Safety Manager SM-Experion Interface** tab and type the Safety Manager IP addresses of the channels connected to Experion.

6 In the **Experion Area** tab, define an area that matches an asset.

For more information about Experion PKS assets, see the topic titled "About assignable assets and scope of responsibility" in the "Enterprise models" section of the *Server and Client Planning Guide*).

7 Click **OK** to close the **Configuration** dialog box.

8 Click **Point Definition File** to create the *pnt* file.

By default, this file is stored in the same folder as the controller and has the same name as the controller with the file extension *pnt*.

9 Click **Hardware Definition File** to create the *hdw* file.

By default, this file is stored in the same folder as the controller and has the same name as the controller with the file extension *hdw*.
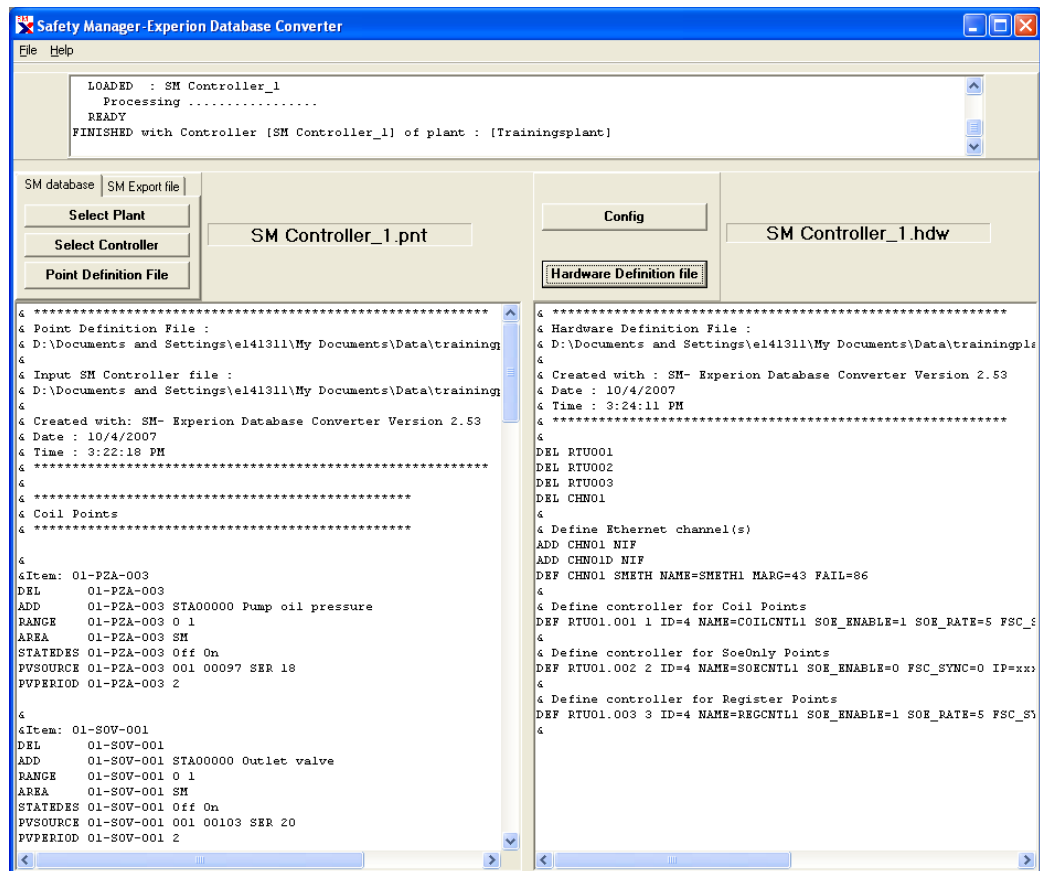
10 Import the *pnt* and *hdw* files into Quick Builder (using Configuration Studio).

> **Attention**
>
> If SOE is enabled in the Safety Manager, only one Experion controller should be SOE-enabled. You need to adjust this setting in Quick Builder after you have imported the *pnt* and *hdw* files as it is not possible to do this via the conversion tool.
>
> If you get an import error, check that your version of SM2Experion converter is the latest version.

Related topics

"About point configuration in an integrated Safety Manager system" on page 16
"Using Configuration Studio to define Safety Manager controllers" on page 44
"Using Configuration Studio to define a Safety Manager channel" on page 41
"Using Configuration Studio to define points for Safety Manager integration " on page 47
"Scanning guidelines for Safety Manager controllers" on page 51
"Address syntax for coils and registers" on page 48
"Address syntax for SOE-only points" on page 49
"Troubleshooting problems when importing hardware and point data" on page 63

Using Configuration Studio to define a Safety Manager channel

You use Configuration Studio to manually define a Safety Manager channel.

Although you only need one channel to integrate Safety Manager with Experion, you might want to configure multiple channels if:

- You need to disable and enable communications on specific controllers.
- There is a high scan load.

Tip

You can also import controllers with the SM2XperionConverter tool. For more information, see the topic titled "Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe."

Prerequisites

- You have started Configuration Studio and you are connected to the Experion server (see topic titled "Starting Configuration Studio" in the "Getting started with Configuration Studio" section of the *Configuration Studio Overview Guide*).

To define a channel

1   Click **Control Strategy** in the Configuration Explorer tree.

    This displays the Control Strategy task list.

2   In the **SCADA Control** group of tasks, click **Build Channels**.

    This launches the Quick Builder tool.

    If the **Enable Components** window appears, make sure that you enable Safety Manager before you click **OK**.

3   On the Quick Builder toolbar, click ⊞.

    The **Add Items** dialog box opens.

4   In the **Add Items** list, click **Channel**.

5   In the **Type** list, click **Safety Manager channel** and click **OK**.

6   Specify appropriate values for the Safety Manager channel properties on each tab (that is, the Main tab, the Port tab, and if appropriate, the Redundant Port tab).

Related topics

Safety Manager channel Main tab properties

The following table lists the properties and recommended settings for the Main tab of a Safety Manager channel in Quick Builder.

Property	Description
Name	The unique name for the channel. A maximum of 10 alphanumeric characters (no spaces or double quotes).
Description	The description of the channel. A maximum of 30 characters, including spaces.

Property	Description
Marginal Alarm Limit	The communications alarm marginal limit at which the channel is declared to be marginal. When this limit is reached, a high priority alarm is generated. A channel barometer monitors the total number of requests and the number of times the controller did not respond or the response was incorrect. The barometer increments by 2 or more, depending on the error and decrements for each good call. To calculate an acceptable limit, multiply the square root of the number of controllers on the channel by the **Marginal Alarm Limit** defined for those controllers. (Normally, you specify the same value for all controllers on a channel). For example, if there are 9 controllers on the channel and their **Marginal Alarm Limit** is set to 10, the value would be [3 is square root] x 10 = 30.
Fail Alarm Limit	The communications alarm fail limit at which the channel is declared to have failed. When this barometer limit is reached, an urgent alarm is generated. If configured, a backup channel will be used when the active channel fails. When the alarm is reached in a redundant configuration, communications will switch to the backup link. A CP fail can sometimes be caused by downloads effectively 'locking up' the server. Set the Fail Alarm Limit to double the value specified for the channel **Marginal Alarm Limit**.
Connect Timeout	The time (in seconds) the server waits to connect to the controller before abandoning the connection. The default is *10* seconds. Use the default value unless the communications line has a high error rate or you are using modems.
Read Timeout	The time (in seconds) that the server waits for a reply from the controller. The default is *2* seconds. Use the default value unless the communications line has a high error rate or you are using modems.
Item Type	Shows the type of channel.
Last Modified	Shows the date when the channel was last modified.
Item Number	The unique item number currently assigned to the channel. You can change the item number if you need to match your current server database configuration. The item number must be between 1 and the maximum number of channels allowed for your system.

Safety Manager channel Port tab properties

The topic describes the properties and recommended settings for the Port tab of a Safety Manager channel in Quick Builder.

Use the Port tab to define the communication-related properties for the Safety Manager channel.

Select **LANVendor** as the **Port Type**. (The **Serial** and **TerminalServer** options are not applicable.)

> **Attention**
> If you have a redundant link, you must define the second link on the Redundant Port tab.

Property	Description
Port Name	Leave blank.

Safety Manager channel Redundant Port tab properties

The topic describes the properties and recommended settings for the Port tab of a Safety Manager channel in Quick Builder.

If you are configuring a redundant link, use the Redundant Port tab to define the communication-related properties of a redundant port for the Safety Manager channel.

Select **Redundant LANVendor** as the **Port Type**. (The **Redundant Serial** and **Redundant TerminalServer** options are not applicable.)

Property	Description
Port Name	Leave blank.

Using Configuration Studio to define Safety Manager controllers

After defining a channel with the Quick Builder tool in Configuration Studio, you need to define Safety Manager controllers. Depending on your requirements, you may need to define several 'logical' controllers to represent a single physical Safety Manager.

You must define a separate logical controller for each Ethernet data table you want the server to access. For example, you must define three logical controllers if you want the server to access a Safety Manager's Coils, Registers and SOE Only tables.

> **Tip**
> You can also import controllers with the SM2XperionConverter tool. For more information, see the topic titled "Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe."

Prerequisites

- You still have Configuration Studio open and are still connected to the Experion server (see topic titled "Starting Configuration Studio" in the "Getting started with Configuration Studio" section of the *Configuration Studio Overview Guide*).
- You have defined the Safety Manager channel as described in the topic titled "Using Configuration Studio to define a Safety Manager channel."

> **Attention**
> If you are defining several logical controllers on the same channel, ensure that you enable SOE on only one controller.

To define the controller

1 On the Quick Builder toolbar, click ⬚.
   The **Add Items** dialog box opens.

2 In the **Add Items** list, click **Controller**.

3 In the **Type** list, click **Safety Manager controller** and click **OK**.

4 Specify appropriate values for the properties on the **Main** tab. Make sure that you define the correct channel name and set the appropriate database table.

5 Repeat the above procedures for each controller.

Related topics

"Safety Manager controller Main properties" on page 44
"Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe" on page 38
"Using Configuration Studio to define a Safety Manager channel" on page 41

Safety Manager controller Main properties

The following table lists the properties and recommended settings for the Main tab of a Safety Manager controller in Quick Builder.

Property	Description
Name	The unique name of the controller. A maximum of *10* alphanumeric characters (no spaces or double quotes). Note: In Station displays, underscore characters (_) appear as spaces. For LAN–connected controllers, the name is used to look up the IP address in the TCP/IP database if you do not specify an **IP Address** property.
Description	(Optional) A description of the controller. A maximum of *132* alphanumeric characters, including spaces.

Property	Description
Channel Name	The channel on which the controller communicates with the server.
Marginal Alarm Limit	The communications alarm marginal limit at which the controller is declared to be marginal. When this value is reached, a high priority alarm is generated. This limit applies to the controller barometer which monitors the total number of requests to the controller and the number of times the controller did not respond or the response was incorrect. The barometer increments by 2 or more, depending on the error and decrements for each good call. The default is *25*.
Fail Alarm Limit	The communications alarm fail limit at which the controller is declared to have failed. When this value is reached, an urgent alarm is generated. Set this to double the value specified for the controller **Marginal Alarm Limit**.
Dynamic Scanning Fastest Scan Period	Select the **Dynamic Scanning** check box to enable dynamic scanning of all point parameters on this controller. The default setting for this check box is selected. Define the fastest possible scan period (in seconds) that dynamic scanning will scan point parameters on this controller. The default is *15* seconds. The dynamic scanning period does not affect the static scanning rate for a parameter. For example, if the scanning rate for a parameter is 10 seconds, and the dynamic scanning rate for the controller is 15 seconds, the parameter will still be scanned at a period of 10 seconds.
Communication Address	Set this to four times the Safety Manager System number. You define the System number using Safety Builder.
Data Table	The Ethernet data table that this controller addresses.
IP Address 1 IP Address 2	The controller's Ethernet addresses.
SOE Enable SOE Rate	Select **SOE Enable** if you want the server to record the controller's sequence of events (SOEs) in its SOE log. **❗ Attention** To prevent communication problems, ensure that you only enable SOE if SOE has been configured for the safety system. Specify the time, in seconds, between polls for SOE data in **SOE Rate**. (The default is 30 seconds, and the minimum value is 1 second.) **❗ Attention** If you define several logical controllers for the same physical Safety Manager, only select **SOE Enable** for one of those logical controllers.
Sync Enable Sync Time	Select **Synch Enable** if you want to synchronize the controller time with the server time. **Synch Time** is the time (in minutes after midnight) at which the server sends a synchronization command. If you define several logical controllers for the same physical Safety Manager, you can specify a different time for each logical controller—this allows the Safety Manager to be synchronized several times each day. The default is *–1* (no synchronization).
Connection Type	The connection type is shown as Ethernet.
Item Type	Shows the type of controller.
Last Modified	Shows the date when the controller was last modified.
Item Number	The unique item number currently assigned to the controller. You can change the item number if you need to match your current server database configuration. The item number must be between 1 and the maximum number of controllers allowed for your system.

Related topics

"Using Configuration Studio to define Safety Manager controllers" on page 44
"Using Configuration Studio to define a Safety Manager channel" on page 41
"Configuring Safety Manager SOE to be logged on an Experion server" on page 35

Using Configuration Studio to define points for Safety Manager integration

You use the Quick Builder tool in Configuration Studio to define the Safety Manager addresses for point parameters, so that the server can read from (or write to) those addresses in Safety Manager.

If you define a logical controller for the SOE Only tables, you can build point parameters on it for:

- Safety Manager points to which you have assigned an SOE number.
- Safety Manager system events, which have reserved SOE numbers.

Point source parameters built on an SOE-only controller should have a scan period of zero.

> **Tip**
> You can also import controllers with the SM2XperionConverter tool. For more information, see the topic titled "Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe."

When a control operation is performed on a status point that has four OP states, the two coil values are written individually, one after the other. Control operations for such points are therefore *not* atomic. If either of the two write requests fail, there will be a maximum of two retries before failing the control request. If you write such points to Safety Manager, this possible delay or failure must be allowed for when configuring Safety Manager communication inputs (see the topic titled "About communication inputs in an integrated Safety Manager system"). In the event of a control failure, the two coils may be left in incorrect immediate states.

The following example summarizes how to add a point and define the Safety Manager address for the **PV source address**.

When defining points with source addresses, make sure that you optimize scanning.

Prerequisites

- You still have Configuration Studio open and are still connected to the Experion server (see topic titled "Starting Configuration Studio" in the "Getting started with Configuration Studio" section of the *Configuration Studio Overview Guide*).
- You have defined the Safety Manager channel as described in the topic titled "Using Configuration Studio to define a Safety Manager channel."
- You have successfully downloaded the channel and controller definitions to the Experion server.

To add a point and define its PV source address

1 Click 🔳 .
   The **Add Items** dialog box opens.

2 In the **Add Items** list, click **Point**.

3 In the **Type** list, click the point type.

4 Define the point's name and then click **OK**. The point is added to the list of points.

5 In the **PV Source Address** property (on the **Main** tab) type the Safety Manager address using the appropriate address syntax. For help with address syntax, see the topic titled "Calling up help for the Safety Manager address syntax."

6 Repeat the above procedures for each point.

Related topics

"Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe" on page 38
"Scanning guidelines for Safety Manager controllers" on page 51
"Address syntax for coils and registers" on page 48
"Address syntax for SOE-only points" on page 49
"Calling up help for the Safety Manager address syntax" on page 48

Calling up help for the Safety Manager address syntax

When defining an address in Quick Builder, you can call up the help for the address syntax.

To call up help for the address syntax

1   Click ... to the right of the address box you are filling in.

The **Address Builder** dialog box opens.

2   In the **Address Type** list, click **Controller**.

3   In the **Controller** list, click the Safety Manager controller you want to address.

4   Press **F1**.

The help for the Safety Manager address syntax appears.

5   You can now define the address by typing it (excluding the name of the controller) in the **Address** box and clicking **OK**.

Related topics

"Address syntax for coils and registers" on page 48
"Address syntax for SOE-only points" on page 49
"Using Configuration Studio to define points for Safety Manager integration " on page 47

Address syntax for coils and registers

`ControllerName PLCAddress [Format|BitNumber] [SOE SOENumber]`

Part	Description
ControllerName	The name of the Safety Manager controller.
PLCAddress	The relevant PLC address.
Format	(Optional) The format used to read raw values: • **To scale**. Uses data format scaling. • **To read without scaling**. Select a format of *C16*, or type *0*, to read all 16 bits in the register without scaling. To read less than 16 bits without scaling, type the starting bit number (1 to 15). If you are not using scaling, the point range is still used for PV indicator bar height only (the PV indicator bar is on the Point Detail display on Station). • **To read floating point values**. The supported floating point formats are specific to the controller type.
BitNumber	(Optional) The first bit that is read. The valid range is 0 (default) to 15, where 0 is the right-most bit in the 16-bit register. Analog and accumulator point parameters can read up to 16 bits. Status point parameters can read 1, 2 or 3 consecutive bits.
SOENumber	The SOE number.

Related topics

"Using Configuration Studio to define points for Safety Manager integration " on page 47
"Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe" on page 38
"Scanning guidelines for Safety Manager controllers" on page 51
"Address syntax for SOE-only points" on page 49
"Calling up help for the Safety Manager address syntax" on page 48

Address syntax for SOE-only points

POS: *Index* SOE *SOENumber*

Part	Description
Index	The server's internal position allocated to this point. It must be unique. Range = 1–8192
SOENumber	The SOE number, either one you have assigned or a reserved number.

Related topics

Ethernet data tables

Safety Manager uses the following Ethernet data tables.

Data table	Server addressable range (DCS address)
Coils (Safety Manager types: DI, DO)	1–8192
SOE Only	N/A
Registers (Safety Manager types: AI, AO, BI, and BO)	10001–18192

Related topics

Floating point data formats for a Safety Manager

Table 2: Data formats for binary-in and binary-out

Format	Description
S8B	Short signed integer.
S16B	Signed word.
S32B	Signed long integer.
IEEEFP	IEEE Floating point.

Table 3: Data formats for analog-in and analog-out

Format	Description
SM020MA	0 - 20 mA
SM420MA	4 - 20 mA
SM05V	0 - 5 V
SM15V	1 - 5 V
SM010V	0 - 10 V
SM210V	2 - 10 V

Related topics

"Address syntax for coils and registers" on page 48

"Ethernet data tables" on page 49

"About data format scaling" on page 50

"Scanning guidelines for Safety Manager controllers" on page 51

"Configuring Safety Manager SOE to be logged on an Experion server" on page 35
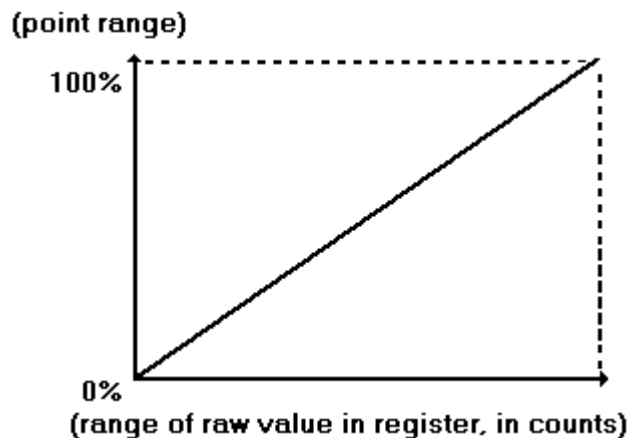
About data format scaling

You can scale parameter values with addresses in the Input register and Holding register data tables with a data format. Select the format that corresponds to the counts that have been set in the controller register.

> **Attention**
> If auxiliary parameters have a data format type that requires scaling (U4095, U999, and so on), they will take the same range as the PV.

The data format tells the server how to interpret the register value. Raw values in the controller register tables can be scaled by the 0% and 100% point range values in order to convert them into engineering units (EU).

To select a format for scaling, you select the format that corresponds to the counts that have been set in the register where the point parameter value is sourced.

Figure 8: Scaling raw data

Related topics

"Scanning guidelines for Safety Manager controllers" on page 51

"Address syntax for coils and registers" on page 48

"Ethernet data tables" on page 49

Scanning guidelines for Safety Manager controllers

An understanding of Safety Manager scan packets will help you configure points that optimize the performance of data acquisition.

Safety Manager addresses that are read from the controller should be grouped together consecutively in blocks and scanned at the same scan rate. Doing this maximizes the amount of data acquired with each request and reduces the load on the server, the network and the physical controller.

If there are gaps in scanned addresses that prevent the formation of continuous consecutive blocks of addresses then you should build 'dummy' points to scan the unused addresses.

The maximum number of registers that can be requested in one scan packet is 62. This limit applies regardless of the size of the registers. Each register in a scan packet adds 4 bytes to the size of the response from the controller regardless of the size of the registers.

The maximum number of coils that can be requested in one scan packet is 2,000. Each span of 8 bits, or part thereof, adds 1 byte to the size of the response from the controller. For example, the data portion of the response for a request for 8 consecutive coils is 1 byte in size, for 9 consecutive coils it is 2 bytes in size.

Note that the diagnostic scan rate is not configurable.

You can use the **lisscn** utility to analyze your scanning configuration. For more information about the lisscn utility, see "Diagnostic commands" in the "Command Reference" topic in the *Server and Client Configuration Guide*.

Configuring OP/SP source addresses

If you configure an OP or SP source address, every write operation to the corresponding OP or SP destination address will result in a demand scan of that single OP or SP address. This can result in an increased load on the server, network and controller—particularly if there are a large number of such parameters being written automatically by automated methods such as OPC Integrator or Experion algorithms.

Therefore, you should only configure OP and SP source addresses if absolutely necessary.

Related topics

Integrating Safety Manager with CEE controllers

Use the following checklist for implementing the Safety Manager-to-CEE controller peer-to-peer communication option.

Prerequisites

- You have met the hardware and software requirements for peer-to-peer communication between Safety Manager and CEE controllers (as described in the topic titled "Hardware and software requirements for Safety Manager integration").
- Your Safety Manager system has been configured using Safety Builder as described in the Safety Manager documentation.
- Your Experion system and CEE controllers have been configured as described in the Experion documentation.
- You have configured the communication between Safety Manager and the Experion server (including time synchronization) as described in the topic titled "Integrating Safety Manager with an Experion server."
- You have engineering level (or higher) access to Safety Builder and Experion Configuration Studio.

Tasks

Task	Go to:	Done?
Configure the physical connection between the CEE controller and Safety Manager.	"Using Safety Builder to configure the physical connection between Safety Manager and a CEE controller" on page 55	
Configure the logical connection between the CEE controller and Safety Manager.	"Using Safety Builder to configure the logical connection between Safety Manager and an Experion server node" on page 22	
Configure points for communicating with the CEE controller.	"Using Safety Builder to configure points for Safety Manager integration" on page 31	
Compile your application.	See the *Safety Manager Software Reference*	
Load the application in Safety Manager:		
• For on-process loading	See the *Safety Manager On-line Modification Guide.*	
• For off-process loading	See the *Safety Manager Installation and Upgrade Guide.*	
Configure the PCDI components.	"Using Control Builder to configure the PCDI components for Safety Manager" on page 56	

Results

For detailed instructions on Safety Manager procedures, consult the Network Configuration section of the *Safety Manager Software Reference*.

Related topics

"Using Safety Builder to configure the physical connection between Safety Manager and a CEE controller" on page 55

"Using Control Builder to configure the PCDI components for Safety Manager" on page 56

"Configuring time synchronization between Safety Manager and Experion" on page 28

"Dealing with Safety Manager-to-CEE controller peer-to-peer problems" on page 61

"Peer-to-peer communication between Safety Manager and CEE controllers" on page 8

"Integrating Safety Manager with an Experion server" on page 19

"Hardware and software requirements for Safety Manager integration" on page 15

Using Safety Builder to configure the physical connection between Safety Manager and a CEE controller

To configure the physical connection between Safety Manager and a CEE controller you use the Network Configurator in Safety Builder to define:

- The device that Safety Manager is communicating with.
- The physical communication address.
- The communication channels and protocols.

Prerequisites

- You have already configured the connection to the Experion server as described in the topic titled "Integrating Safety Manager with an Experion server."
- You have synchronized your Experion system (including CEE controllers, if applicable) and each Safety Manager to a single time source as described in the topic titled "Configuring time synchronization between Safety Manager and Experion."

To configure the physical connection

1   Start Safety Builder and open **Network Configurator - Physical View**.
2   Drag the **CEE Controller** icon from the button bar in the **Plant** area and connect it to the **Plant** icon.
3   In the **CEE Controller Properties** dialog box type a unique name for the CEE controller and click **OK**.
4   Drag a suitable (existing) Physical Network Connection from the Explorer bar, connect it to the CEE controller.

> **❗ Attention**
>
> By connecting an existing Physical Network Connection to the CEE controller you also connect the Safety Manager controller that has been configured at the other end of the network connection to that CEE controller.

If you cannot connect the Safety Manager controller from the Explorer bar, this means that the Safety Manager Controller has no suitable communications channel available, or that you have reached the limit of 8 CEE controllers per communication channel.

In that case, free a suitable communication channel (channel A on a USI-0001 communication module) or add another USI-0001. For details see the *Safety Manager Software Reference*.

Related topics

"Using Safety Builder to configure the logical connection between Safety Manager and an Experion server node" on page 22
"Using Safety Builder to configure the physical connection between Safety Manager and the Experion server" on page 21
"Integrating Safety Manager with an Experion server" on page 19
"Configuring time synchronization between Safety Manager and Experion" on page 28

Using Control Builder to configure the PCDI components for Safety Manager

You use Control Builder to create function blocks for configuring the peer-to-peer communication between Safety Manager and CEE controllers.

The high-level steps are listed below. For detailed procedures, refer to the *Peer Control Data Interface Implementation Guide*.

> **Attention**
>
> PCDI is a licensed option that is only supported in C300 controllers, not C200 or ACE nodes.
>
> When setting up peer-to-peer communication between Safety Manager and a C300 controller, it is recommended that Safety Manager be attached either directly to Level 1 switches (or to the Level 1 side of a split switch).
>
> Note also that the TCP port must be set to 502 for peer-to-peer communication through a Level 1 switch.

To configure the PCDI components for Safety Manager

1   Add a peer control data interface device (PCDI_MASTER) block to the project.

    a   On the **Module Configuration** tab, add the IP addresses for Control Processor 1 and Control Processor 2 (CP1 and CP2).

    b   On the **Slave Configuration** tab, set the timeout (in ms) to 2000, and set the Unit ID to the same value as the **Device Address** in Safety Builder (see the topic titled "Logical Network Properties settings").

2   Add a PCDI Array Request Channel Block to the relevant Control Module and assign the channel to PCDI_MASTER block.

3   Assign the PCDI-Master Block and the Control Module(s) to the Execution Environment.

4   Create or configure flag arrays and numeric arrays with PCDI_MASTER block Unit ID settings that match the Device Address in Safety Manager (see step above).

Related topics

"Logical Network Properties settings" on page 23

Settings for CEE controller-to-Safety Manager points

Observe the following recommendations and settings when configuring CEE controller-to-Safety Manager points.

> **Attention**
>
> Do not allow a NaN (Not a Number) or Inf (Infinity) to be sent to a floating point input of Safety Manager. Sending a Nan or and Inf will result in an "Illegal data" error. For more information, see the topic titled "Checking for Illegal Value errors on the CEE controller."

Point type	Read/write	Recommended option	PLC address prefix	Comments
Digital input	Write	WriteOnDiff	0	
Digital input	Read	ReadOnly	1	
Word	Write	WriteOnDiff	4	
Word	Read	ReadOnly	3	
Float	Write	WriteOnDiff	7	
Float	Read	ReadOnly	7	

Point type	Read/write	Recommended option	PLC address prefix	Comments
Analog point	Read	ReadOnly	3	For a 0-20mA analog point, set the RAW bottom and top values to 0-3276 respectively. For a 4-20mA analog point, set the RAW bottom and top values to 655-3276 respectively. If the analog point is scaled in Safety Manager then scale the point in the CEE controller too.

Related topics

"Checking for Illegal Value errors on the CEE controller" on page 62

Troubleshooting Safety Manager integration problems

The recommended procedures for isolating and dealing with common problems related to integrating Safety Manager with CEE controllers and Experion depend on the type of integration option(s) you have implemented at your site.

Related topics

"Isolating Safety Manager-to-Experion server communication problems" on page 60
"Dealing with Safety Manager-to-CEE controller peer-to-peer problems" on page 61
"Troubleshooting problems when importing hardware and point data" on page 63
"Accessing diagnostics for a Safety Manager controller" on page 64

Isolating Safety Manager-to-Experion server communication problems

You can often gain a better understanding of a problem by performing the following basic checks.

Check	Go to:	Done?
Check the server log for error messages.		
Test communications with the server.	"Testing Safety Manager communications with the server" on page 61	
Check that you have optimized scanning.	"Scanning guidelines for Safety Manager controllers" on page 51	
If you have defined several logical controllers on the same channel, check that you have enabled SOE on only one controller.	"Safety Manager controller Main properties" on page 44	
In Safety Builder, check that SOE numbers are not assigned to addresses unnecessarily. Reporting unnecessary SOEs to Experion generates unnecessary network traffic and delays the logging of useful SOEs.	"Configuring Safety Manager SOE to be logged on an Experion server" on page 35	
If you are getting communication errors, check that there is no mismatch between the SOE configuration on the safety system and Experion. If no SOE is configured in the safety system, ensure that **SOE enable** is not selected for the Experion controller, and remove the **SOE only** controller in Experion.	"Using Configuration Studio to define Safety Manager controllers" on page 44	
When downloading from Safety Builder to a Safety Manager Control Processor, temporarily disable the Experion channel link to that Control Processor to prevent unnecessary communications errors. Ensure that the backup Control Processor is active and healthy before doing this.		
In Safety Builder, check that timeouts in the Experion Logical Network Properties are either enabled with a value greater than 25000 ms or else disabled.	"Logical Network Properties settings" on page 23	
If *Illegal data address* errors appear in the server log, check that all Safety Manager addresses that are being written to by Experion are configured correctly in the controller.		
If illogical diagnostic or system messages appear on the console, check that the correct diagnostic message files have been loaded on the Experion server.	"Testing Safety Manager communications with the server" on page 61	

Related topics

"Integrating Safety Manager with an Experion server" on page 19
"Direct communication between Safety Manager and an Experion server " on page 8

Dealing with Safety Manager-to-CEE controller peer-to-peer problems

For additional information, see the troubleshooting section in the *Peer Control Data Interface Implementation Guide*.

Check	Go to:	Done?
Test communications between Safety Manager and the server.	"Testing Safety Manager communications with the server" on page 61	
Check for Illegal Value errors on the C300 controller.	"Checking for Illegal Value errors on the CEE controller" on page 62	

Related topics

"Testing Safety Manager communications with the server" on page 61
"Checking for Illegal Value errors on the CEE controller" on page 62
"Integrating Safety Manager with CEE controllers" on page 53
"Configuring time synchronization between Safety Manager and Experion" on page 28
"Peer-to-peer communication between Safety Manager and CEE controllers" on page 8

Testing Safety Manager communications with the server

Experion includes a diagnostic utility, **smetst**, that you can use to test communications with Safety Managers.

> **Attention**
> This procedure should only be used for off-process testing.

Prerequisites

- You have set up Safety Manager in accordance with the Safety Manager documentation, and you have connected it to the network.
- You have downloaded the Safety Manager channel and controller(s) from Quick Builder without errors.
- The server database service is running.
- To get a correct Safety Manager diagnostic representation on Experion, copy the following files from the Safety Builder CD and replace the files in the Experion server folder `\Experion PKS\Server\Data`:

  `fsc_module.txt`

  `fsc_fault.txt`

To test Safety Manager communications with the server

1 On the server, open a Command Prompt window.
2 If the server is running, stop it by typing the following command at the command prompt:

   `hscserver /load`

   Answer **y** in response to the prompt.

   You need to stop the server to prevent it from communicating with the controllers. If you don't do this, the test utility might interfere with communications.
3 In the Command Prompt window, type **smetst** and press ENTER.
   The test utility is launched. It is menu-driven, and self-explanatory. If there are any communications errors, error messages will describe what is wrong.

4 Restart the server by typing the following command at the command prompt:

```
hscserver /start
```

Answer **y** in response to the prompt.

Checking for Illegal Value errors on the CEE controller

Care must be taken with C300 writes to Safety Manager as Safety Manager treats NaN (not a number) or Inf (Infinity) values as bad values that indicate a communication problem or error. Safety Manager therefore returns an *illegal value* error message to the C300 controller.

Note also that if any value in a list write is NaN, none of the individual writes in the list are accepted by Safety Manager.

There are no issues with C300 from Safety Manager because Safety Manager does not return NaN or Inf values. Furthermore, C300 controllers treat NaNs and Infs as 'normal' floating point values that are freely propagated between function blocks. Function blocks are designed to take specific actions when NaNs or Infs are encountered.

Related topics

"Settings for CEE controller-to-Safety Manager points" on page 56

Troubleshooting problems when importing hardware and point data

Some older versions of *SM2XperionConverter.exe* can produce incorrect output that needs to be corrected manually.

Diagnostic check

Check that you are using the most recent version of *SM2XperionConverter.exe*.

Solution

- Obtain a more recent version of the tool and run it again.
- If you are using the latest version of the tool, and you still get errors, you will need to correct the data manually.

Related topics

"Importing Safety Manager details into Configuration Studio with SM2XperionConverter.exe" on page 38

Accessing diagnostics for a Safety Manager controller

System information and extended diagnostic data are accessible from Station for Safety Managers.

To access system information

• Double-click the PV of a Safety Manager point. Alternatively, click **Details** in the controller status, which shows the **Ext Diagnostics** tab, then click the **System Info** tab for the required link.

The system information and extended diagnostic information is updated automatically every 50 seconds. You can manually refresh the information by clicking **Refresh**.

If the diagnostic data cannot be retrieved from the controller, the most recent diagnostic data from the controller will continue to be displayed until the new data is obtained. If successive attempts to obtain diagnostic data from the controller fail, then an alarm message will be generated in the Alarm Summary.

To access extended diagnostics

• Click **Details** in the controller status.

This shows up to 32 extended diagnostics messages for each controller. Each message represents a hardware or software fault associated with that particular controller.

If there is an extended diagnostic message for a controller, a `Message(s) Available` alarm will appear in the Alarm Summary. To view extended diagnostic information for an alarm, double-click the alarm to call up the controller status, then click **Details**.

Notices

Trademarks

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

OneWireless™ is a trademark of Honeywell International, Inc.

Other trademarks

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

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

Third-party licenses

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

Documentation feedback

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

http://www.honeywellprocess.com/support

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

hpsdocs@honeywell.com

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

How to report a security vulnerability

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

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

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

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

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

- Send an email to security@honeywell.com.

  or

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

Support

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

Training classes

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

NOTICES

Index