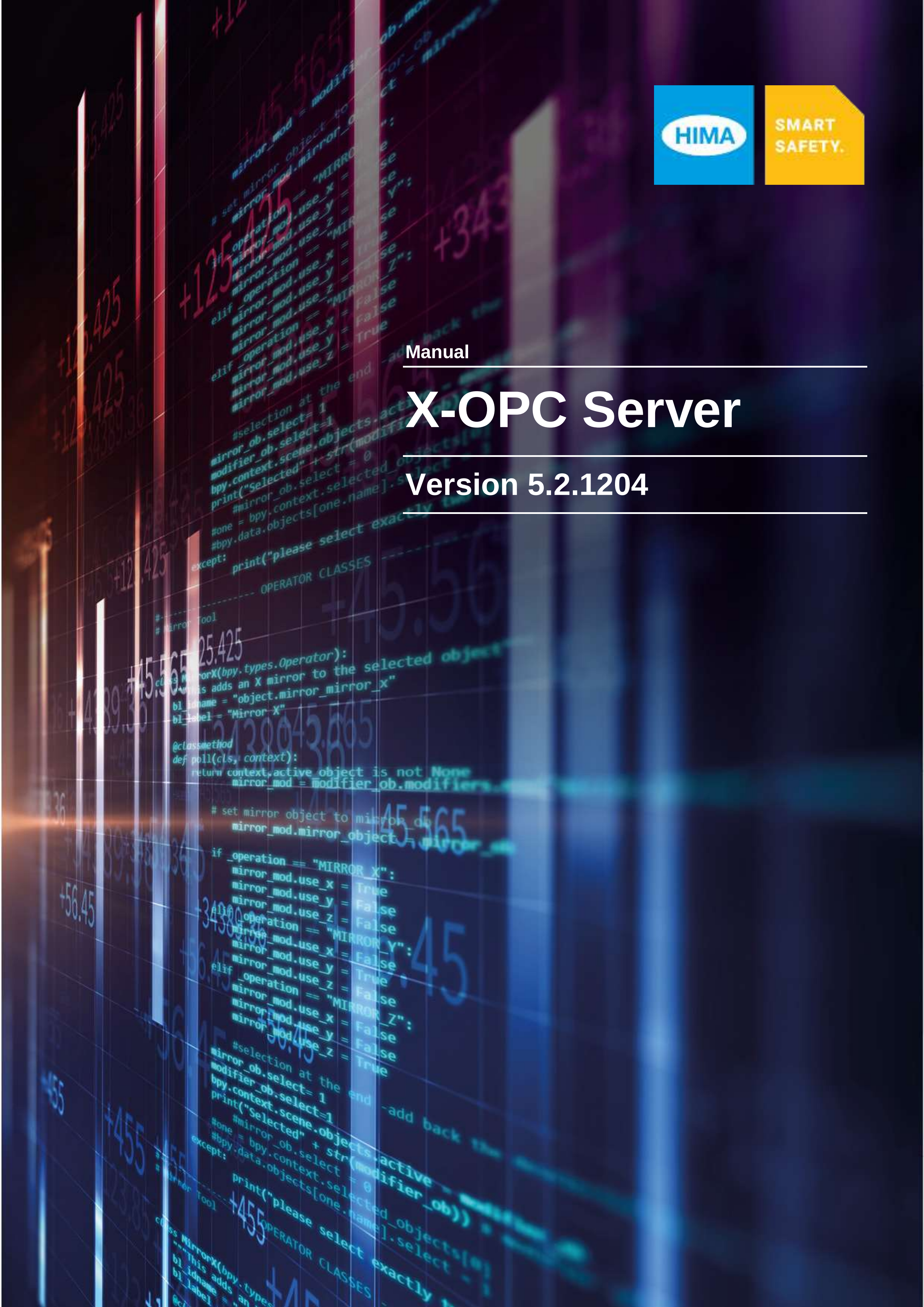


Manual

X-OPC Server

Version 5.2.1204

All technical specifications and notes in this manual have been written with great care and effective quality assurance measures have been implemented to ensure their validity. For questions, please contact HIMA directly. HIMA appreciates any suggestion on which information should be included in the manual.

Equipment subject to change without notice. HIMA also reserves the right to modify the written material without prior notice.

All the current manuals can be obtained upon request by sending an e-mail to: documentation@hima.com.

Contact

HIMA contact details:

HIMA Paul Hildebrandt GmbH

P.O. Box 1261

68777 Brühl, Germany

Phone: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Document designation	Description
HI 801 479 D, Rev. 1.00 (1734)	German original document
HI 801 480 E, Rev. 1.00.00 (1745)	English translation of the German original document

Table of Contents

1 Introduction

The X-OPC manual describes the properties, installation and configuration of X-OPC using SILworX.

Knowledge of regulations and the proper technical implementation of the instructions detailed in this manual performed by qualified personnel are prerequisites for planning, engineering, programming, installing, starting up, operating and maintaining the HIMA controllers.

HIMA shall not be held liable for severe personal injuries, damage to property or the environment caused by any of the following: unqualified personnel working on or with the devices, de-activation or bypassing of safety functions, or failure to comply with the instructions detailed in this manual (resulting in faults or impaired safety functionality).

HIMA automation devices have been developed, manufactured and tested in compliance with the pertinent safety standards and regulations. They may only be used for the intended applications under the specified environmental conditions.

1.1 Structure and Use of This Manual

The manual contains the following chapters:

- Introduction
- Safety
- Product description
- Configuring the X-OPC protocol in SILworX

Additionally, the following documents must be taken into account:

Name	Content	Document no.
HIMax system manual	Hardware description of the HIMax system	HI 801 001 E
HIMax safety manual	Safety functions of the HIMax system	HI 801 003 E
HIMatrix safety manual	Safety functions of the HIMatrix system	HI 800 023 E
HIMatrix compact system manual	Hardware description HIMatrix compact system	HI 800 141 E
HIMatrix modular system manual	Hardware description HIMatrix modular system	HI 800 023 E
SILworX first steps manual	Introduction to SILworX.	HI 801 103 E

Table 1: Additional Applicable Manuals

The current manuals can be downloaded from the HIMA website at www.hima.com. The revision index in the footer can be used to compare the manuals in use with the Internet edition and determine if they are up to date.

1.2 Target Audience

This document is aimed at the planners, design engineers and programmers of automation systems as well as the persons authorized to start up, operate and maintain the devices and systems concerned. Specialized knowledge of safety-related automation systems is required.

1.3 Writing Conventions

To ensure improved readability and comprehensibility, the following writing conventions are used in this document:

Bold	To highlight important parts. Names of buttons, menu functions and tabs that can be clicked and used in the programming tool.
Italics	Parameters and system variables, references.
`Courier`	Literal user inputs.
RUN	Operating states are designated by capitals.
Chapter 1.2.3	Cross-references are hyperlinks even if they are not particularly marked. When the cursor hovers over a hyperlink, it changes its shape. Click the hyperlink to jump to the corresponding position.

Safety notices and operating tips are particularly marked.

1.3.1 Safety Notices

Safety notices must be strictly observed to ensure the lowest possible risk.

The safety notices are represented as described below.

- Signal word: warning, caution, notice.
- Type and source of risk.
- Consequences arising from non-observance.
- Risk prevention.

The signal words have the following meanings:

- Warning indicates hazardous situations which, if not avoided, could result in death or serious injury.
- Caution indicates hazardous situations which, if not avoided, could result in minor or modest injury.
- Notice indicates a hazardous situation which, if not avoided, could result in property damage.

⚠ SIGNAL WORD

Type and source of risk!

Consequences arising from non-observance.

Risk prevention.

NOTICE

Type and source of damage!

Damage prevention.

1.3.2 Operating Tips

Additional information is structured as presented in the following example:

i The text giving additional information is located here.

Useful tips and tricks appear as follows:

TIP The tip text is located here.

2 Safety

All safety information, notes and instructions specified in this document must be strictly observed. The HIMA controllers may only be used if all guidelines and safety instructions are adhered to.

The HIMA controllers are operated with SELV or PELV. No imminent risk results from the controllers themselves. Use in the Ex zone is only permitted if additional measures are taken.

2.1 Intended Use

To use the HIMA controllers, all pertinent requirements must be met, see relevant manuals in Table 1.

2.2 Residual Risk

No imminent risk results from a HIMA system itself.

Residual risk may result from:

- Faults related to engineering.
- Faults in the user program.
- Faults related to the wiring.

2.3 Safety Precautions

Observe all local safety requirements and use the protective equipment required on site.

2.4 Emergency Information

A HIMA system is a part of the safety equipment of a plant. If the controller fails, the system enters the safe state.

In case of emergency, no action that may prevent the HIMA system from operating safely is permitted.

2.5 Cyber Security for HIMA Systems

Industrial controllers must be protected against IT-specific problem sources. Those problem sources are:

- Attackers inside and outside of the customer's plant
- Operating failures
- Software failures

All requirements for protection against manipulation specified in the safety and application standards must be met. The operator is responsible for authorizing employees and implementing the required protective actions.

⚠ WARNING

Physical injury possible due to unauthorized manipulation of the controller!

The controller must be protected against unauthorized access!

For example:

- **Changing the default settings for login and password!**
- **Controlling physical access to the controller, X-OPC Server and PADT!**

Careful planning should identify the measures to implement. The required measures are to be implemented after the risk analysis is completed. Such measures are, for example:

- Meaningful allocation of user groups.
- Maintained network maps help to ensure that secure networks are permanently separated from public networks and, if required, only a well-defined connection exists (e.g., via a firewall or a DMZ).
- Use of appropriate passwords.

A periodical review of the security measures is recommended, e.g., every year.

The user is responsible for implementing the necessary measures in a way suitable for the plant!

For more details, refer to the HIMA cyber security manual (HI 801 373 E).

3 Product Description

The HIMA X-OPC Server V5.2.1204 serves as transfer interface between HIMax/HIMatrix controllers and third-party systems that are equipped with an OPC interface.

OPC means *Open Platform Communications* and is based on Microsoft's DCOM technology (*Distributed Component Object Model)* which is used for communications between DCOM objects (OPC Client and X-OPC Server).

After installation, the HIMA X-OPC Server is run on a PC as Windows service. For further information, refer to www.opcfoundation.org.

i SILworX is used to configure and operate the entire X-OPC Server. The X-OPC Server can be loaded, started and stopped in the SILworX Control Panel like a controller.

The X-OPC Server supports the following specifications:

- **Data Access (DA) versions 1.0, 2.05a and 3.0**
  DA ensures that real-time data is transmitted and global variables are read from a HIMax/HIMatrix controller and written to the OPC Client or vice versa. The DA specifications do not include interfaces for providing historical values to the DA clients.
- **Alarms&Events (A&E) version 1.10**
  A&E is used to transfer alarms and events from the HIMax/HIMatrix controller to the OPC Client. Each global variable of the HIMax/HIMatrix controller can be monitored using sequence of events recording.
  Events are changes in a variable's state, which are performed by the system or controller and are provided with a timestamp.
  Alarms are events that signalize increased risk potential.

3.1 Equipment and System Requirements

The new X-OPC Server V5.2.1204 features are only available with SILworX V9. For redundant operation, identical X-OPC Server versions should be used.

Element	Description
Activation	Software activation code to be generated from the HIMA website `Product Registration->X-OPC Server`. The following licenses can be activated on an individual basis: ▪ Data Access (DA) Server ▪ Alarms&Events (A&E) server
Requirements for the host PC	The computer used for the X-OPC Server must meet the same minimum requirements as those applying for SILworX. The minimum requirements are specified on the corresponding installation DVD. In particular with very large projects, old PCs may require long processing times and thus be inappropriate for this task. Therefore, state-of-the-art computers should be used whenever possible. Enhanced hardware features, such as computing power and memory space, result in improved performance. i The minimum requirements only apply for operating an X-OPC Server if no additional applications, such as SILworX or Word, are running on the host PC.

Table 2: Equipment and System Requirements for the X-OPC Server

3.2 Compatibilities with Previous Versions

HIMA X-OPC Server version 5.2.1204 is compatible with all previous versions. The upgrade to the newest version can be performed from all previous versions.

3.2.1 Synchronization Mode, A&E ID and Cookies

These features are available as of version 5.2.1204:

- Synchronization mode:
  The synchronization mode is used to define how redundant X-OPC Servers should behave when synchronizing alarms and events at start-up, see Chapter 5.1.1.
- A&E ID and Cookies:
  The *A&E ID* parameter is used to specify a unique value (1…511) in the A&E Editor of the controller. This is included in the cookies calculation and serves to unambiguously identify the event source, see Chapter 6.1.3. When the A&E ID is entered, the redundant X-OPC Servers within a set receive identical cookies irrespective of the synchronization mode.

3.2.2 Forcing Global Variables on I/O Modules

i

If an I/O module forces global variables that are connected to a process value, the forced global variables have no effect on the global variables connected to the following parameters:
->State LL, ->State L, ->State N, ->State H, ->State HH.
This also applies if these alarms are used in the A&E Editor.
While testing, these variables must be forced individually.

3.3 Properties of X-OPC Server V5.2.1204

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>OPC Server</td><td>The X-OPC Server V5.2.1204 supports the following functions:
▪ OPC Data Access Custom Interface, versions 1.0, 2.05a and 3.0.
▪ OPC A&E, interfaces 1.10</td></tr>
<tr><td>Safety-related</td><td>The X-OPC Server runs on a PC and is not safety-related.</td></tr>
<tr><td>Interface</td><td>Recommended: Ethernet 1GBit/s(D10_0032_OPC: 714)</td></tr>
<tr><td>Data exchange</td><td>Data exchange via safe<b>ethernet</b>.</td></tr>
<tr><td>Ethernet Network</td><td>The underlying Ethernet network speed must be designed in accordance with the data traffic (min. 100 Mbit/s, recommended 1GBit/s).</td></tr>
<tr><td>Global Variables</td><td>Only global variables from the configuration context may be used!</td></tr>
<tr><td>Permissible
Variable Types</td><td>All data types that can be created in SILworX are permitted.
The structure or array elements are implemented as individual variables and are not available as structures or arrays.</td></tr>
<tr><td>Impermissible ASCII characters</td><td>The following characters are reserved and must not be used (e.g., for global variables): ! " # ' , . / \` : |</td></tr>
<tr><td>HIMax/HIMatrix Controllers</td><td>An X-OPC Server can support a maximum of 254 HIMax/HIMatrix controllers.
Vice versa, a controller can communicate with 254 OPC DA Servers including a maximum of 4 X-OPC Servers with active A&E.</td></tr>
<tr><td>Prozessdatenmenge</td><td>Maximale Prozessdatenmenge zu einer Steuerung
HIMax: 128 kB
HIMatrix up to F*03 16 kB
HIMatrix F*03: 64 kB</td></tr>
<tr><td>X-OPC Server</td><td>10 X-OPC Servers can be operated on a host PC.</td></tr>
<tr><td>X-OPC Clients</td><td>An X-OPC Server supports 10 X-OPC Clients.</td></tr>
<tr><td>Data Access Tags</td><td>A data access server supports a maximum of 100 000 DA tags.
Definition:
Tags: Data provided by the X-OPC Server The structure or array elements are used as individual variables.
Items: Data required by the OPC Client.</td></tr>
<tr><td>Alarms&Events
Event definitions</td><td>An X-OPC A&E Server supports a maximum of 100 000 event definitions.</td></tr>
</table>

Table 3: X-OPC Server Properties

i When the data type of a tag is changed into an array or structure, or vice versa, the variable in the OPC Client must be deleted before loading the X-OPC Server and a new variable must be created after the X-OPC Server has been loaded again.

3.4 HIMax Controller Properties for X-OPC Connection

Element	HIMax	HIMatrix F*03	HIMatrix prior to F*03	Description
Process data volume	128 kB	128 kB	16 kB	Maximum process data volume that a HIMA controller can exchange for each safe**ethernet** connection to one X-OPC Server.
Fragment size	1100 bytes	1100 bytes	900 bytes	In each HIMaxcycle, only a fragment is sent to an X-OPC Server.
Ethernet interfaces	10/100/ 1000BaseT	10/ 100BaseT	10/ 100BaseT	Ethernet interfaces in use, can simultaneously be employed for other protocols.
Max. number of system events (CPU event)	20 000	4000	n.a.	Events defined as CPU events are created on the processor module. The processor module creates all events in each of its cycles. This allows the value of each global variable to be recorded and evaluated as an event.
Max. number of I/O events (I/O event)	6000	n.a.	n.a.	Events defined as I/O events can only be created on I/O modules supporting SOE (e.g., X-AI 32 02 or X-DI 32 04).
Event memory size	5000	1000 (with enabled license only)	n.a.	Non-volatile event buffer of the HIMax processor module. If the event buffer is full, new events can only be stored after an event entry has been read by the X-OPC A&E server and marked for overwriting.
Max. number of X-OPC Servers with A&E	4	4	4	Maximum number of X-OPC Servers that can access a HIMA controller and simultaneously read events from the event buffer of the processor module.
Max. number of X-OPC Servers without A&E	254	254	254	Maximum number of X-OPC Servers that can exchange global variables with the HIMA controller. Less the number of X-OPC Servers with active A&E.
n.a.: not applicable				

Table 4: HIMax Controller Properties for X-OPC Connection

Range of values for the UTC timestamp (Universal Time Coordinated):

- s fraction since 1970 in [UDWORD]
- ms fraction of the seconds as [UDWORD] from 0-999

Default value: 2000-01-01 / 00:00:00 An automatic change to/out of daylight-saving time is not supported.

3.5 Actions Required as a Result of Changes

The user must ensure that configuration changes are implemented both on the controller and the X-OPC Server.

When a change is performed through a reload, ensure that the new configuration is first loaded into the X-OPC Server and then into the controller.

The use of reload for changing the resource configuration must be agreed upon with the competent test authority! For further details on reload, refer to the safety manual of the corresponding system family.

The following table shows the actions that must be performed after a change in the individual systems. For further details on safe**ethernet** reload, refer to the communication manual (HI 801 101 E).

Type of change	Changes to		
	HIMax	HIMatrix	X-OPC
DA			
Add tags	C+R	C+R	C+R
Tag name (change of GV name)	C+R	C+R	C+R
Delete tags	C+R	C+R	C+R
Change fragments (parameters and Add/Delete)	C+R	C+R	C+R
A&E			
Add event definition	C+R	C+R[1]	C+R
Delete event definition	C+R	C+R[1]	C+R
Change event source	C+R	C+R[1]	C+R
Change alarm text	-	-	C+R
Change alarm severity	-	-.	C+R
Change the value of *Ack Required*	-	-	C+R
Change the value of *Alarm Values* for scalar events	C+R	C+R[1]	C+R
Change the value of *Alarm at False* for Boolean events	C+R	C+R[1]	C+R
Change name	C+R	C+R[1]	C+R
Connect I/O channel to global variable	C+R	C+R[1]	-
Connect state variable to global variable	C+R	C+R[1]	-
In general			
Change safe**ethernet** parameters	C+D	C+D	C+D
C: Code generation required R: Reload required D: Download required	n.a.: not applicable -: No action required [1] Applicable as of F*03 with SMR license		

Table 5: Actions Required as a Result of Changes

4 Installing Redundant X-OPC Servers

4.1 Configuring an X-OPC Server Connection

This example shows how to configure a redundant X-OPC Server connection to a HIMax controller.

The X-OPC Servers provide the process variables and event values of the HIMax controller to the OPC Clients. The OPC Clients access these process variables and event values and represent them on their user interface.

4.1.1 Software Requirements

- SILworX
- X-OPC Server
- OPC Client

i SILworX is used to configure and operate the entire X-OPC Server. The X-OPC Server can be loaded, started and stopped in the SILworX Control Panel like a controller.

4.1.2 Requirements for Operating the X-OPC Server

- The Ethernet network should have a bandwidth of at least 100 Mbit/s (better 1GBit/s).
- The IP addresses on the PCs must be located in different subnets.
- HIMA recommends synchronizing the system time of computers and servers, e.g., using SNTP.
- Make sure that the data records for data access and A&E on the controller, X-OPC Servers and OPC Clients match one another.
- If the OPC Client and X-OPC Server are not running on the same PC, the DCOM interface must be adjusted. For further information, refer to www.opcfoundation.org.

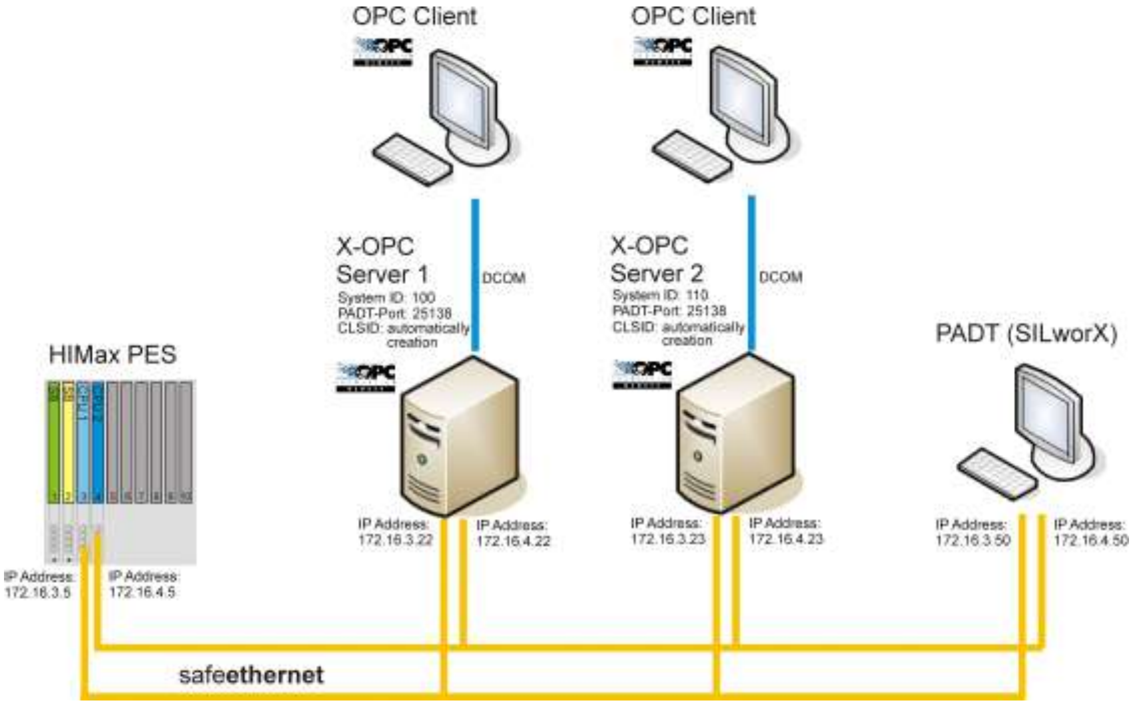
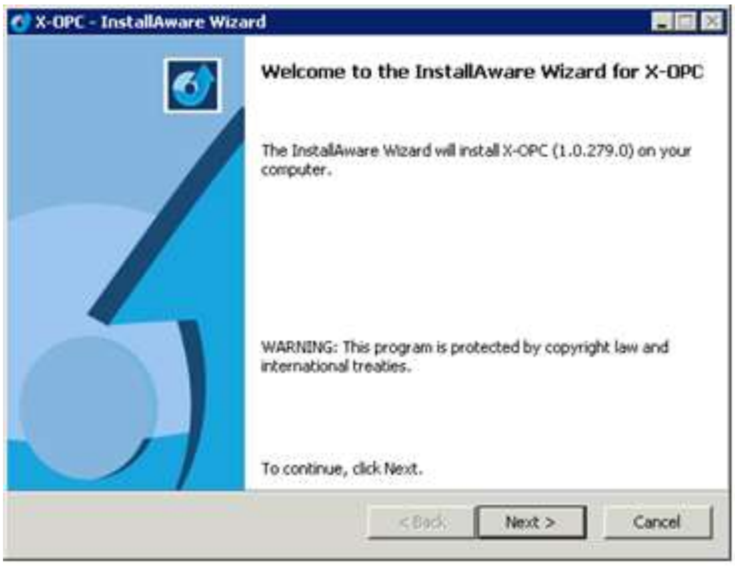


Figure 1: Redundant X-OPC Operation

4.2 Installation on Host PC

The X-OPC Server must be installed on the respective host PC.

i Note down the system ID and the number of the PADT port. This data is required for generating the license key!



X-OPC - InstallAware Wizard

Welcome to the InstallAware Wizard for X-OPC

The InstallAware Wizard will install X-OPC (1.0.279.0) on your computer.

WARNING: This program is protected by copyright law and international treaties.

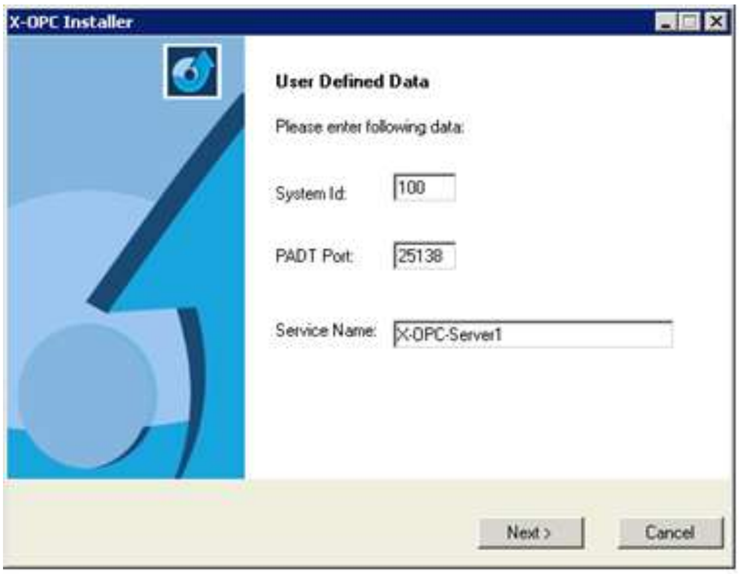
To continue, click Next.

Figure 2: Wizard for Installing the X-OPC Server

To install the X-OPC Server on the first host PC

Start the *X-OPC.exe* file on each host PC and follow the instructions of the install wizard.

1. Enter the following data for the X-OPC Server:
   - System ID: 100
   - PADT port: 25138
   - An arbitrary name for the X-OPC Server (displayed in the OPC Client).
2. To install the X-OPC Server, click **Next>**.



X-OPC Installer

User Defined Data

Please enter following data:

System Id: 100

PADT Port: 25138

Service Name: X-OPC-Server1

Figure 3: Wizard for Installing the X-OPC Server

To automatically generate the CLSID on the first host PC

1. Select the CLSID setting **automatic** for DA and AE.
2. To install the X-OPC Server, click **Next>**.

To determine the class ID of the first X-OPC Server

If one OPC Client is redundantly connected to two X-OPC Servers, some OPC Client systems expect that the CLSIDs of the two X-OPC Servers are identical. First determine the CLSID of the first X-OPC Server and note it down.

The CLSID can be determined with one of the following methods:

- Read it in the OPC Client.
- Read the CLSID of the first X-OPC Server from the computer or server registry, under `HKEY_CLASSES_ROOT\CLSID`.

To install the X-OPC Server on the second host PC

Start the *X-OPC.exe* file on the second host PC and follow the instructions of the install wizard.

1. Enter the following data for the X-OPC Server:
   - System ID: 110
   - PADT port: 25138
   - An arbitrary name for the X-OPC Server (displayed in the OPC Client).

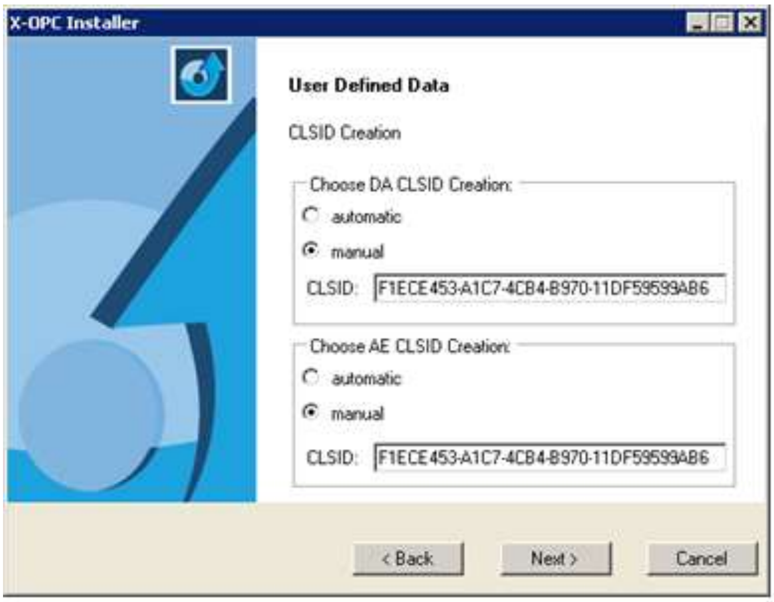
i PADT port and HH port of the second X-OPC Server may be identical with the first one, if the X-OPC Servers are run on different PCs.

2. Click **Continue>** to confirm.

To set the same CLSID on the second host PC

i The CLSIDs of both X-OPC Servers may only be identical if the X-OPC Servers are operated on different PCs.

1. Select the CLSID setting **manual** for DA and AE.
2. Enter the class ID of the first X-OPC Server in the **CLSID** fields.
3. To install the X-OPC Server, click **Next>**.



X-OPC Installer

User Defined Data

CLSID Creation

Choose DA CLSID Creation:

○ automatic

● manual

CLSID: F1ECE453-A1C7-4CB4-B970-11DF59599AB6

Choose AE CLSID Creation:

○ automatic

● manual

CLSID: F1ECE453-A1C7-4CB4-B970-11DF59599AB6

Figure 4: Setting the CLSID of the Second X-OPC Server Manually

i CLSIDs (class identifiers) are used to unambiguously identify DCOM objects. A class ID always includes 5 groups of hexadecimal digits 8-4-4-4-12.
A possible CLSID would be `2CA0AB0D-2BD1-48ED-8215-E06B203D44E6`

The X-OPC Server (service) must be restarted to allow the change to be effective.

To automatically start the X-OPC Servers after restarting the PCs

1. In Windows, go to **Start**, **Settings**, **Control Panel**, **Administration**, **Services** and select **X-OPC Server** from the list.
2. Select **Properties** from the context menu for the OPC Server.
3. In the **General** tab, select the **Automatic** start type.

To ensure that the X-OPC Servers operates properly on the PC

1. Open the *Windows Task Manager* and select the **Processes** tab.
2. Start *X-OPC.exe* if X-OPC has not yet been started on the PC.

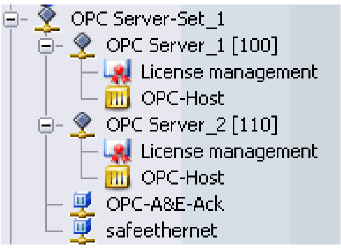
4.3 Configuring the OPC Server Set in SILworX

The OPC Server Set is used as common platform for configuring up to two OPC Servers.

The OPC Server Set properties for the two redundant X-OPC Servers are automatically identical.

To create a new OPC Server Set in SILworX

1. In the structure tree, open **Configuration**.
2. Right-click **Configuration**, and then select **New, OPC-Server Set** from the context menu.
   ☑ A new OPC Server Set with an OPC Server is added. This includes the tabs **OPC Server Set Objects** and **Properties**, see Chapter 5.1.



```
OPC Server-Set_1
  OPC Server_1 [100]
    License management
    OPC-Host
  OPC Server_2 [110]
    License management
    OPC-Host
  OPC-A&E-Ack
  safeethernet
```

Figure 5: Redundant X-OPC Operation

3. Right-click **OPC Server Set** and select **Properties** from the context menu.
   ☑ Select the *Full* synchronization mode.

To configure the first OPC Server in SILworX

1. In the structure tree, select **Configuration, OPC Server Set, OPC Server**.
   ☑ This includes the **OPC Server Object**, see Chapter 5.1.2.
2. Right-click **OPC Server** and select **Properties** from the context menu.
   - Enter the system ID [SRS] (e.g., 100).
3. Right-click **OPC Host** and select **Edit**.
   ☑ The OPC host editor for configuring the IP interfaces appears.
4. Right-click anywhere in the OPC host editor and select **New IP Connection**.
   - Set the PADT port (e.g., 25138).
   - Set the first IP address of the PC on which the X-OPC Server is installed (e.g., 172.16.3.22). Mark it as standard interface.
   - Set the second IP address of the PC on which the X-OPC Server is installed (e.g., 172.16.4.22).
   - Set the HH port (e.g., 15138)

i

If several X-OPC Servers are installed on a PC, both the PADT port and the HH port must be unique for each server!

If a firewall is installed on the PC, the TCP/UDP PADT and HH ports of the X-OPC Servers must be configured as exception in the firewall configuration.

To configure the second OPC Server

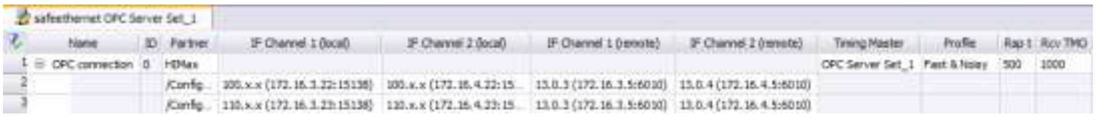
1. In the structure tree, open **Configuration, OPC Server Set.**
2. Right-click **OPC Server Set** and select **New**, **OPC Server**.
   ☑ A second OPC Server is created. This includes the **OPC Server Object**, see Chapter 5.1.2.
3. Right-click this **OPC Server** and select **Properties** from the context menu.
   - Enter the system ID [SRS] (e.g., 110).
4. Right-click **OPC Host** and select **Edit**.
   ☑ The OPC host dialog box for configuring the IP interfaces appears.
5. Right-click anywhere in the OPC host dialog and select **New IP Connection**.
   - Set the PADT port (e.g., 25138).
   - Set the first IP address of the PC on which the X-OPC Server is installed (e.g., 172.16.3.23). Mark it as standard interface.
   - Set the IP address of the PC on which the X-OPC Server is installed (e.g., 172.16.4.23).
   - Set the HH port (e.g., 15138)

i If a firewall is installed on the PC, the UDP PADT and HH ports of the X-OPC Servers must be configured as exception in the firewall configuration.

4.3.1 Settings in the safe**ethernet** Editor for the OPC Server Set

To create a safeethernet connection between the OPC Server Set and a resource

1. In the OPC Server Set, open the safeethernet Editor.
   ☑ This includes the safe**ethernet Editor Object**, see Chapter 5.2.
2. In the Object Panel, click the **Resource** and drag it onto a free space within the workspace of the safe**ethernet** Editor.



safeethernet OPC Server Set_1

	Name	ID	Partner	IF Channel 1 (local)	IF Channel 2 (local)	IF Channel 1 (remote)	IF Channel 2 (remote)	Timing Master	Profile	Rsp t	Rcv TMO
1	⊟ OPC connection	0	HIMax					OPC Server Set_1	Fast & Noisy	500	1000
2			/Config...	100.x.x (172.16.3.22:15138)	100.x.x (172.16.4.22:15...	13.0.3 (172.16.3.5:6010)	13.0.4 (172.16.4.5:6010)				
3			/Config...	110.x.x (172.16.3.23:15138)	110.x.x (172.16.4.23:15...	13.0.3 (172.16.3.5:6010)	13.0.4 (172.16.4.5:6010)				

Figure 6: safe**ethernet** Editor of OPC Server Set

i The used Ethernet interfaces of the PCs are represented in the **IF Channel 1 (Local)** column. The Ethernet interfaces of the Ressource (controller) must be selected in the **IF Channel (remote)** column.

The safe**ethernet** parameters for X-OPC Server communication are set by default for ensuring the maximum availability.

Receive Timeout = 1000 ms, Response Time = 500 ms etc.

For further details on the safe**ethernet** parameters, refer to the communication manual (HI 801 101 E).

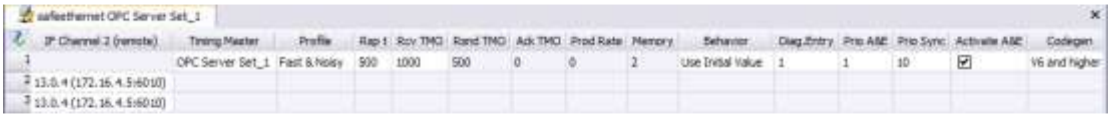
To set the fragment priorities for alarms and events

The events created in the A&E Editor are automatically transferred via safe**ethernet**.

The event priorities are entered in the **Priority of Events** and **Priority of State Values** columns of the safeethernet Editor for the OPC Server Set. These priorities apply to all the A&E fragments of the current safe**ethernet** connection.

1. Scroll the safe**ethernet** Editor to the right.

   ☑ The *Activate A&E* parameter is active by default.



safeethernet OPC Server Set_1

	IP Channel 2 (remote)	Timing Master	Profile	Rsp t	Rcv TMO	Resnd TMO	Ack TMO	Prod Rate	Memory	Behavior	Diag Entry	Prio A&E	Prio Sync	Activate A&E	Codegen
1		OPC Server Set_1	Fast & Noisy	500	1000	500	0	0	2	Use Initial Value	1	1	10	☑	V6 and higher
2	13.0.4 (172.16.4.5:6010)														
3	13.0.4 (172.16.4.5:6010)														

Figure 7: safe**ethernet** Editor of OPC Server Set

2. Double-click **Prio A&E** to modify the priority of the events. All events of this resource receive the priority entered in the **Prio A&E** column (e.g., 1). This defines the priority for events requested by the X-OPC Server from the controller. If no events exist in the controller at a given point in time, none are transferred.
3. Double-click **Prio Sync** to synchronize the priority of the event state values. All event state values of this resource receive the priority entered in the **Sync** column (e.g., 10).

i The state values of the events are only required for synchronization reasons (e.g., when the connection is being established); they can thus be transferred in larger intervals than the events.

4.3.2 Creating the A&E Acknowledge Connection between Redundant X-OPC Servers

The acknowledgements of alarms can be synchronized on the redundant X-OPC Servers. To do this, an acknowledge connection is created in the OPC Server Set.

NOTICE

The A&E Acknowledge Connection is essential for the Full synchronization mode.

1. In the structure tree, select **Configuration, OPC Server Set, New**.
2. Right-click **OPC Server Set** and select **New**, **OPC A&E Ack** from the context menu.

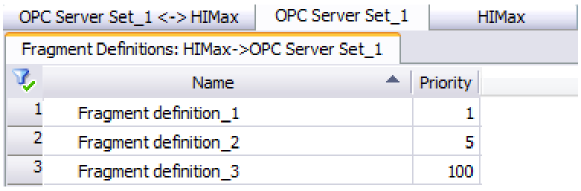
   ☑ This includes the **OPC Server Set Object**, see Chapter 5.1.3.
3. Select the following IP connections in the *OPC A&E Ack* dialog box.
   - IF Channel 1 (OPC Server 1, e.g., 172.16.3.22).
   - IF Channel 2 (OPC Server 1, e.g., 172.16.4.22).
   - IF Channel 1 (OPC Server 2, e.g., 172.16.3.23).
   - IF Channel 2 (OPC Server 2, e.g., 172.16.4.23).

4.4 Configuring the Data Access in the Detail View of the safeethernet Editor

Data Access is configured in the detail view of the X-OPC safe**ethernet** Editor.

4.4.1 Creating the Fragment Definitions for OPC Receive Variables

1. In the OPC Server Set, open the safe**ethernet** Editor.
2. Right-click the resource to open the corresponding context menu.
3. Select **Edit** from the context menu to open the detail view of the safe**ethernet** connection.
   ☑ This includes the detail view of the safe**ethernet** connection, see Chapter 5.3.
4. Select the **OPC Server Set: Fragment Definitions** tab.
5. Right-click a free space in the workspace and select **New Fragment Definition**.
   The *Priority* column is used to define how often this fragment should be sent compared to the other fragments (a fragment's size is 1100 bytes).
   The fragment priority can be set for each fragment definition. The priority is used to determine how often these variables must be refreshed.
   - Use a high priority (e.g., 1) for fragment definitions with global variables that are often updated.
   - Use a low priority (e.g., 10) for fragment definitions with global variables that are rarely updated.


OPC Server Set_1 <-> HIMax
OPC Server Set_1
HIMax
Fragment Definitions: HIMax->OPC Server Set_1

	Name	Priority
1	Fragment definition_1	1
2	Fragment definition_2	5
3	Fragment definition_3	100

Figure 8: safe**ethernet** Connection Detail View

4.4.2 Configuring the OPC Transport Variables

The OPC send and receive variables must be created in the OPC Server Set one time only. The variables are automatically used by both X-OPC Servers in the OPC Server Set.

To add OPC receive variables

The OPC receive variables are sent from the resource to the OPC Server.

1. Open the detail view of the X-OPC safe**ethernet** Editor and select the **OPC Server Set<->Resource** tab.
   ☑ This includes the **OPC Server Set <- Resource** and **OPC Server Set -> Resource** tabs, see Chapter 5.3.1.
2. In the Object Panel, drag a **Global Variable** onto the **OPC Server Set<-Resource** area.
3. Double-click the **Fragment Name** column and select the **Fragment Definition** element created beforehand.
4. Repeat these steps for every further OPC receive variable.

To add OPC send variables

OPC send variables are sent from the OPC Server to the resource.

1. Open the detail view of the X-OPC safe**ethernet** Editor and select the **OPC Server Set<->Resource** tab.
   ☑ This includes the **OPC Server Set <- Resource** and **OPC Server Set -> Resource** tabs, see Chapter 5.3.1.
2. In the Object Panel, drag a **Global Variable** onto the **OPC Server Set->Resource** area.
3. Repeat these steps for every further OPC send variable.

4.5 Configuring Alarms and Events in the the A&E Editor

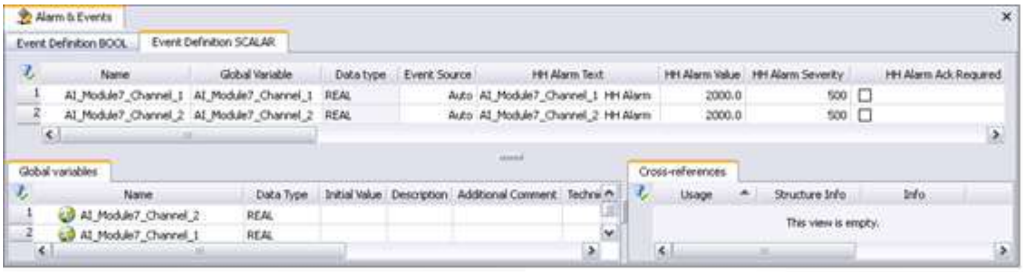
Alarms and events are configured in the A&E Editor of the resource. The events created in the A&E Editor are automatically transferred via the configured safe**ethernet** connection, see Chapter 4.3.1.

To create the A&E Editor for a resource

1. In the structure tree, select **Configuration**, **Resource.**
2. Right-click **Resource** and select **New, Alarms&Events** from the context menu.
   ☑ A new A&E Editor is created. This includes the event definitions and properties, see Chapter 6.

To create alarms and events

1. Right-click **Alarms&Events** and select **Edit**.
2. Select the **Event Definition BOOL** tab for Boolean events, see Chapter 6.1.1.
3. Select the **Event Definition Scalar** tab for scalar events, see Chapter 6.1.2.
4. In the Object Panel, drag the **Global Variable** onto a free space within the workspace of the A&E Editor.



	Name	Global Variable	Data type	Event Source	HH Alarm Text	HH Alarm Value	HH Alarm Severity	HH Alarm Ack Required
1	AI_Module7_Channel_1	AI_Module7_Channel_1	REAL	Auto	AI_Module7_Channel_1 HH Alarm	2000.0	500	□
2	AI_Module7_Channel_2	AI_Module7_Channel_2	REAL	Auto	AI_Module7_Channel_2 HH Alarm	2000.0	500	□

	Name	Data Type	Initial Value	Description	Additional Comment	Techni
1	AI_Module7_Channel_2	REAL				
2	AI_Module7_Channel_1	REAL				

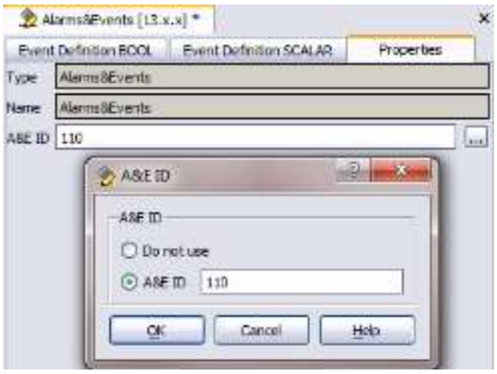
Usage	Structure Info	Info

This view is empty.

Figure 9: A&E Editor

To create A&E IDs for generating unique resource cookies

1. Point to the **Properties** table of the A&E Editor and click the **…** button located next to the *A&E ID* field.
   ☑ The *A&E ID* dialog box appears.
2. Select **A&E ID** and enter a unique *A&E ID*, see Chapter 6.1.3.



Type: Alarms&Events
Name: Alarms&Events
A&E ID: 110

A&E ID

A&E ID
○ Do not use
● A&E ID 110

Figure 10: A&E ID

4.5.1 Code Generation and Verification

To generate the code and load a resource

1. In the structure tree, select **Configuration**, **Resource.**
2. Right-click and select **Code Generation** from the context menu.
3. Thoroughly verify the messages displayed in the logbook and correct potential errors.
4. Load the generated code into the resource.

To generate the code and verify the OPC Server Set

1. In the structure tree, select **Configuration, OPC Server Set.**
2. Right-click and select **Code Generation** from the context menu.
3. Thoroughly verify the messages displayed in the logbook and correct potential errors.

To load the generated code into the X-OPC Server

1. Right-click the **OPC Server** and select **Online** from the context menu to log in to the system.
2. Enter the access data:
   - IP address of the PC on which the X-OPC Server is installed (e.g., 172.16.3.23).
   - User name: Administrator
   - Password: Leave the field empty
3. Click **Login** to open the Control Panel.
4. In the SILworX menu bar, click the **Resource Download** symbol.
   ☑ The code is loaded into the X-OPC Server.
5. In the SILworX menu bar, click the **Resource Cold Start** symbol.
   ☑ The X-OPC Server is running.

4.5.2 Indication in the OPC Client

The name of the X-OPC Server displayed in the OPC Client is composed of:
HIMA (manufacturer)**.Service name** (see Figure 3) **DA** (Data Access).

Connect to the X-OPC Server. At this point, the configured DA data should be transferred to the OPC Client.

Connect to the X-OPC Server. At this point, the configured alarms and events should be transferred to the OPC Client.

i If the *Acknowledge Only or Full* synchronization mode is set, the X-OPC Server is synchronized as soon as a controller is connected to an X-OPC Server. To do so, the X-OPC A&E Server reads the current state of all the variables defined as events and transfers the upcoming alarms to the OPC Client. An updated image of the current controller state can thus be created in the OPC Client. The events are only read at this moment. For further details on the synchronization mode, see Chapter 5.1.1.

5 Description of the X-OPC Server Editors and Objects

This chapter describes the X-OPC Server characteristics, menu functions and dialog boxes required to configure the X-OPC Server in SILworX.

i SILworX is used to configure and operate the entire X-OPC Server. The X-OPC Server can be loaded, started and stopped in the SILworX Control Panel like a controller.

5.1 OPC Server Set

The OPC Server Set is used as a common platform for configuring up to two OPC Servers.

The OPC Server Set properties for the two redundant X-OPC Servers are automatically identical.

The OPC Server Set includes the following objects:

- OPC Server
- OPC A&E Ack
- safe**ethernet** Editor

To create a new OPC Server Set

1. In the structure tree, select **Configuration**.
2. Select **New, OPC Server Set** from the context menu for the configuration to create a new OPC Server Set.
3. Select **Properties** from the context menu for the OPC Server Set and accept the default values.

5.1.1 OPC Server Set Properties

The *Properties* dialog box for the OPC Server Set contains the following parameters:

Name	Description
Name	Name for the OPC Server Set. Max. 31 characters.
Safety time [ms]	The safety time is the time in milliseconds within which the X-OPC Server must react to an error. Condition: safety time ≥ 2 x Watchdog time Range of values: 2000...400 000 ms Default setting: 20 000 ms
Watchdog Time [ms]	The watchdog time is the maximum time that the X-OPC Server may need to complete a program cycle. If the defined watchdog time is exceeded, the X-OPC Server is stopped. Condition: Watchdog time ≥ 1000 ms and ≤ 0.5 * safety time Range of values: 1000...200 000 ms Default setting: 10 000 ms
Target Cycle Time [ms]	Target cycle time for the X-OPC Server Default setting: 50 ms
Target Cycle Time Mode	This parameter can be used to maintain the cycle time constant to a value that is as close as possible to the *Target Cycle Time [ms]*. Tasks such as reload and synchronization of redundant X-OPC Servers are limited to ensure that the target cycle time is maintained.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>Fixed</td><td>If an X-OPC cycle is shorter than the defined target cycle time, the X-OPC cycle is extended to the target cycle time.
If the X-OPC cycle takes longer than the target cycle time, the X-OPC resumes the cycle without delay.</td></tr>
<tr><td>Fixed-tolerant</td><td>Similar to <i>Fixed</i>, but with the following difference:
If necessary, the target cycle time may be violated during synchronization for an X-OPC cycle to allow synchronization to be performed successfully.</td></tr>
<tr><td>Dynamic</td><td>The X-OPC executes each X-OPC cycle as fast as possible. This corresponds to a target cycle time of 0 ms.</td></tr>
<tr><td>Dynamic-tolerant</td><td>Similar to <i>Dynamic</i>, but with the following difference:
If necessary, the target cycle time is automatically increased for an X-OPC cycle to ensure that the synchronization process can be performed successfully.</td></tr>
</table>
Default setting: Fixed-tolerant</td></tr>
<tr><td>Max. Com.Time Slice [ms]</td><td>The Max. Com. Time Slice ASYNC [ms] is the time in milliseconds that is reserved in each X-OPC Server cycle for processing all the tasks scheduled for peer-to-peer communication.
Default setting: 500 ms</td></tr>
<tr><td>Optimized Use of Com. Time Slice</td><td>If activated, shorter response times can be achieved for communication via the process module.
Caution: This mode can affect the temporal utilization of Max. Com.Time Slice ASYNC [ms] and thus also the system parameter Max. Duration of Configuration Connections [ms] to the PADT such that these two times can be subject to more demands (e.g., during reload).</td></tr>
<tr><td>Allow Online Settings</td><td>The setting of the <i>Allow Online Settings</i> OPC switch affects the function of the other OPC switches.
If the main enable is deactivated, the parameters set for the other OPC switches cannot be modified while the user program is being processed (the controller is in RUN).
Default setting: Activated.</td></tr>
<tr><td>Autostart</td><td>Autostart defines if the OPC configurations may be automatically started with a cold start or a warm start after powering up or booting the controller or should not be started (Off).
If Autostart is deactivated, the X-OPC Server adopts the STOP/VALID CONFIGURATION state after booting.
Default setting: Deactivated</td></tr>
<tr><td>Start Allowed</td><td>Only if <i>Start Allowed</i> is activated, can an X-OPC Server be started from within the programming tool.
If <i>Start Allowed</i> is deactivated, the X-OPC Server cannot be started from within the programming tool. In this case, the X-OPC Server can only be started if <i>Autostart</i> is activated and the host PC is switched on or rebooted.
If neither Autostart nor <i>Start Allowed</i> is activated, the X-OPC Server cannot be started. This may be necessary during maintenance actions to prevent the system from starting.</td></tr>
</table>

Name	Description
	Default setting: Activated.
Load Allowed	If *Load Allowed* is deactivated, no (new) OPC configuration can be loaded into the controller. Deactivate *Load Allowed* to avoid that the OPC configuration loaded into the X-OPC Server is overwritten. Default setting: Activated.
Reload Allowed	No function yet!
Global Forcing Allowed.	Global forcing can only be started if *Global Forcing Allowed* is activated. Default setting: Deactivated The Force Editor can also be used to display variable contents if *Global Forcing Allowed* is deactivated.
Global Force Timeout Reaction	If *Stop Resource* is selected, the X-OPC Server enters the STOP state after the preset force time has expired. All outputs of the X-OPC Server are set to LOW. If *Stop Forcing Only* is selected, the X-OPC Server continues executing the OPC configuration after the force time has expired. Default setting: *Stop Forcing Only* If *Global Forcing Allowed* is set, carefully check the setting for Stop at Force Timeout. Also observe the notes in the safety manual.
Minimum Configuration Version	-SILworX V2 -SILworX V6 -SILworX V9
System Variables	The **Edit** button is used to open the *System Variables* dialog box. This dialog box is used to assign alias names to the OPC tags automatically created for system information. This allows the OPC tags to be transmitted to the client. Example: The system variable name is *Date/Time [ms portion]*. Since not every client is familiar with such special characters in the name, an alias name can be allocated in this dialog box, e.g., `Date_Time_s_portion`. System variable that should not be transmitted to the OPC Client can be filtered out with *Hide*.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Synchronization Mode</td><td>This parameter defines the synchronization mode for synchronizing the conditions between the redundant X-OPC Servers (synchronization, for instance, when the connection is being established).
<table>
<tr><td>Acknowledge Only</td><td>Synchronization with the controller's event source (global variable). No synchronization with the redundant X-OPC Server. The result is that the redundant X-OPC Server and the Client have differing timestamps at start-up.</td></tr>
<tr><td>Simple</td><td>Synchronization with the controller's event buffer based on the current timestamp.
In contrast to <i>Acknowledge Only</i> and <i>Full,</i> no states or timestamps are aligned with the redundant X-OPC Server, nor are they sent to the OPC Client. Only states and timestamps of newly occurred events are identical and are sent to the OPC Client.</td></tr>
<tr><td>Full</td><td>The X-OPC Server that first starts up triggers synchronization with the controller's event source (global variable). Synchronization with the redundant X-OPC Server occurs afterwards.</td></tr>
</table>
Default setting: Full</td></tr>
<tr><td>Peer Connection Timeout [ms]</td><td>This parameter defines how long the X-OPC should wait until the connection to the redundant X-OPC Server has been established. The connection state is cyclically verified within this time.
Range of values: UDWORD
Default setting: 2000 ms</td></tr>
<tr><td>Peer Synchronization Timeout [ms]</td><td>This parameter defines how long the X-OPC should wait before receiving the synchronization data from the redundant X-OPC Server. The timer is reset to this value when synchronization data is received.
Range of values: UDWORD
Default setting: 5000 ms</td></tr>
<tr><td>Namespace Separator</td><td>Important for OPC Clients that need different separators.
<table>
<tr><td>Dot</td><td>.</td></tr>
<tr><td>Slash</td><td>/</td></tr>
<tr><td>Colon</td><td>:</td></tr>
<tr><td>Backslash</td><td>\</td></tr>
</table>
Example of names displayed in the OPC Client:
<code>ResName.TagName</code>
<code>ResName/TagName</code>
Default setting: Dot</td></tr>
<tr><td>Namespace Type</td><td>Depending on the OPC Client requirements, the following namespace types can be set:
- Hierarchical Namespace
- Flat Namespace
Default value: Hierarchical Namespace</td></tr>
<tr><td>Changeless Update</td><td>Setting according to the OPC Client requirement.</td></tr>
</table>

Name	Description
	Activated: If *Changeless Update* is activated and the OPC Group Update Rate has expired, the X-OPC Server provides all items to the OPC Client. Deactivated: If *Changeless Update* is deactivated, only the modified values are provided to the OPC Client (this behavior is in accordance with the OPC Specification).
Cycle Delay [ms]	The cycle delay limits the CPU load of the PC due to the X-OPC Server to allow other programs to be run. Range of values: 1...100 ms Default value: 5 ms
Short Tag Names for DA	This parameter can only be activated if *Flat Namespace* is selected. This is an option where data and event sources are offered to the OPC Client without any further context (path name). Default setting: Deactivated
Simple Events for CPU I/O Events	Never Only at Start Always Default setting: Only at Start
Short Tag Names for A&E	This parameter can only be activated if *Flat Namespace* is selected. This is an option where data and event are offered to the OPC Client without any further context (path name). Default setting: Deactivated

Table 6: Properties

5.1.2 The OPC Server Object

To create a new OPC Client

1. In the structure tree, select **Configuration, OPC Server Set.**
2. Select **New**, **OPC Server** from the context menu for OPC Server Set to create a new OPC Server.
3. Select **Properties** from the context menu for OPC Server.

The *Properties* dialog box for the OPC Server contains the following parameters:

Element	Description
Name	Name for the OPC Server.
System ID [SRS]	Default value: 60 000
Namespace Prefix	Default value: Empty

Table 7: Properties

5.1.2.1 The OPC Host Object

To open the OPC host

1. In the structure tree, select **Configuration, OPC Server Set, OPC Server.**
2. Select **Edit** from the context menu for the OPC Host to get an overview of the IP interfaces.

The *Edit* dialog box for the OPC host contains the following parameters:

Element	Description
PADT Port	Default value: 25138
Name	Name for the OPC Server Set.
IP Address	IP address of the host PC. Default value: 192.168.0.1
Standard Interface	To be selected if the host PC is equipped with more than one Ethernet port. Default value: Activated
HH Port	Default value: 15138

Table 8: Edit

5.1.3 OPC A&E Ack Object

To create a new OPC A&E Ack

1. In the structure tree, select **Configuration, OPC Server Set.**
2. Select **New**, **OPC A&E Ack** from the context menu for OPC Server Set to create a new OPC A&E Ack.
3. Select **Properties** from the context menu for OPC A&E Ack.

The **Properties** tab of the OPC A&E Ack contains the following parameters:

Element	Description
Type	OPC A&E Ack
Profile	Combination of matching safe**ethernet** parameters. Fast & Cleanroom Fast & Noisy Fixed Default value: Fast & Noisy

Element	Description
Response Time [ms]	Time until the acknowledgment of a message is received by the sender. Default value: 500
Receive Timeout [ms]	Monitoring time of PES1 within which a correct response from PES2 must be received. Default value: 1000
Resend Timeout [ms]	Monitoring time expressed in milliseconds (ms) and set in PES1 within which PES2 must have acknowledged the receipt of a data packet; upon expiration of this period, the data packet is sent again.
Acknowledge Timeout [ms]	Time period within which the CPU must acknowledge the reception of a data packet.
Production Rate	Minimum time interval between two data packets.
Queue	Number of data packets that can be sent without acknowledgment.
Code Generation Compatibility	V6 and higher: Optimized safe**ethernet** signature Prior to V6: Standard safe**ethernet** signature Default value: V6 and higher
safeethernet Connection ID	safe**ethernet** connection ID Range of values: 0...63
Timing Master	The timing master provides the value for *Receive Timeout*, *Resend Timeout* and the *Acknowledge Timeout* for this safe**ethernet** connection. The opposite controller is the timing slave, which adopts these values. If no timing master is selected, the controller with the smaller IP address determines these safe**ethernet** parameters. *Partner A* *Partner B* Default value:: *Partner A*

Table 9: Properties

The **Partner** tab of the OPC A&E Ack contains the following parameters:

Element	Description
Partner	(First) OPC Server selected from the OPC Set
IF Channel 1	First IP address of the host PC.
IF Channel 2	Second IP address of the host PC.
Partner	(Second) OPC Server selected from the OPC Set
IF Channel 1	First IP address of the host PC.
IF Channel 2	Second IP address of the host PC.

Table 10: Partner

5.2 safeethernet Editor Object

The safeethernet Editor is used to configure the safeethernet connections of the resource to the X-OPC Server Set.

Open the safeethernet Editor of the X-OPC Server Set.

1. **In the structure tree, open Configuration, OPC Server Set.**
2. Right-click safe**ethernet** and select **Edit** from the context menu.
   ☑ The safe**ethernet** Editor includes the workspace and the Object Panel.

To do this, drag the resources that should be connected to the X-OPC Server from the Object Panel onto the workspace.

The following safe**ethernet** protocol parameters must be set to configure the safe**ethernet** connection:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Name</td><td>Name of the safe<b>ethernet</b> connection</td></tr>
<tr><td>ID</td><td>safe<b>ethernet</b> connection ID
Range of values: 0...63</td></tr>
<tr><td>Partner</td><td>Resource name of the link partner</td></tr>
<tr><td>IF Channel</td><td>Ethernet interfaces available on the (local) and (remote) resource.</td></tr>
<tr><td>Timing Master</td><td>The timing master provides the value for <i>Receive Timeout</i>, <i>Resend Timeout</i> and the <i>Acknowledge Timeout</i> for this safe<b>ethernet</b> connection. The opposite controller is the timing slave, which adopts these values.
If no timing master is selected, the controller with the smaller IP address determines these safe<b>ethernet</b> parameters.</td></tr>
<tr><td>Profile</td><td>Combination of matching safe<b>ethernet</b> parameters.</td></tr>
<tr><td>Rsp t</td><td>Time until the acknowledgment of a message is received by the sender.
Default value: 500 ms</td></tr>
<tr><td>Rcv TMO</td><td>Monitoring time of PES1 within which a correct response from PES2 must be received.
Default value: 1000 ms</td></tr>
<tr><td>Rsnd TMO</td><td>Monitoring time expressed in milliseconds (ms) and set in PES1 within which PES2 must have acknowledged the receipt of a data packet; upon expiration of this period, the data packet is sent again.</td></tr>
<tr><td>Ack TMO</td><td>Time period within which the CPU must acknowledge the reception of a data packet.</td></tr>
<tr><td>Prod Rate</td><td>Minimum time interval between two data packets.</td></tr>
<tr><td>Queue</td><td>Number of data packets that can be sent without acknowledgment.</td></tr>
<tr><td>Behavior</td><td>Behavior of the input variables for this safeethernet connection if the connection is interrupted.
<table>
<tr><td>Use Initial Value</td><td>The initial data is used for the input variables.</td></tr>
<tr><td>Freeze Process Value Indefinitely</td><td>The input variables are frozen to the current value and used until a new connection is established.</td></tr>
<tr><td>Limited</td><td>Input: Double-click the drop-down field and enter the time value.
The input variables are frozen to the current value and used until the configured timeout. Afterwards, the initial data is used for the input variables.
The timeout can be extended by up to a CPU cycle.</td></tr>
</table></td></tr>
</table>

Parameter	Description
Diag.Entry	The number of warnings that must occur in sequence within the *Warning Period [ms]* before the warnings are recorded in the diagnostics or communication fault statistics.
Prio A&E	The function is only activated for the connection to the X-OPC Server. This defines the priority for events requested by the X-OPC Server from the controller. Fragments with priority **n** and fragments with priority **m** are sent at a ratio of **n** to **m** times.
Prio Sync	The function is only activated for the connection to the X-OPC Server. This defines the priority for state values requested by the X-OPC Server from the controller. Fragments with priority **n** and fragments with priority **m** are sent at a ratio of **n** to **m** times.
Activate A&E	This parameter activates the transmission of the controller's alarms and events to the X-OPC Server via this safe**ethernet** connection. The alarms and events are configured in the A&E Editor of the corresponding controller (resource), see Chapter 6. Activated: The alarms and events can be read out of a controller via this safe**ethernet** connection. Deactivated: No alarms and events can be read out of a controller via this safe**ethernet** connection. Default value: Activated
Codegen	Default value: V6 and higher V6 and higher: Optimized safe**ethernet** signature Prior to V6: Standard safe**ethernet** signature

Table 11: safe**ethernet** Protocol Parameters

5.3 Detail View of the safeethernet Editor

The detail view always refers to the resource for which the safeethernet Editor was started.

To open the detail view for a safeethernet connection

1. Right-click the safe**ethernet** connection to open the context menu.
2. Select **Edit**.

The detail view contains the following three tabs:

- OPC Server Set<->Resource
- OPC Server Set
- Resources

5.3.1 The *OPC Server Set<->Resource* Tab

The *OPC Server Set* <-> *Resource* tab is divided into two areas: *Resource->OPC Server Set* and *OPC Server Set ->Resource*.

For the transport direction required, global variables can be dragged from the object panel onto these two areas.

5.3.2 The *OPC Server Set* Tab

The *OPC Server Set* contains the *fragment definitions.*

Depending on its type and for each safeethernet connection, a HIMA controller can send 128 kB or 16 kB to an X-OPC Server, but only one fragment (1100 bytes or 900 bytes) per HIMA CPU cycle. To send more data via a safe**ethernet** connection, data must be fragmented. The *Priority* parameter associated with these fragments is used to define how often these fragments should be updated.

i Fragments with priority **n** and fragments with priority **m** are sent at a ratio of **n** to **m** times.

For the response time from the controller to the X-OPC Server, also observe the number of SOE fragments and commands (e.g., stop, start).

T_R = t_1 + t_2 + t3 +t4 only applies if the priority of all fragments for state data is equal to 1.

T_R	Worst Case Reaction Time
t_1	Safety Time of PES 1
t_2	*Number of Fragments * Receive TMO*
t_3	Safety Time of X-OPC Server
t_4	Delay due to SOE function; depending on the number of events and on how the connection is established.

The response time for the inverse direction can be determined using the same formula, but only one fragment is usually relevant in this case, since the X- OPC Server only transfers the data written by OPC Clients.

Maximum number of fragments: 1024

Maximum size of a fragment: 1100 bytes or 900 bytes

Range of values for the priorities: 1 (highest) to 65 535 (lowest)

5.3.2.1 The System Variables Tab

The safe**ethernet** connection to the X-OPC Server of the Sets can be controlled and evaluated using system variables.

<table>
<tr><th>Name</th><th>Data type</th><th>R/W</th><th>Description</th></tr>
<tr><td colspan="4">The following statuses and parameters can be assigned global variables and used in the user program.</td></tr>
<tr><td>Ack.Frame No.</td><td>UDINT</td><td>R</td><td>Receive counter (revolving)</td></tr>
<tr><td>Number of Faulty Messages</td><td>UDINT</td><td>R</td><td rowspan="2">Number of All Bad Messages per Channel (Invalid CRC, Invalid Header, Other Faults).</td></tr>
<tr><td>Number of faulty messages for the redundant channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Number of Successful Connections</td><td>UDINT</td><td>R</td><td>Number of successful connections since statistics reset.</td></tr>
<tr><td>Number of Lost Messages</td><td>UDINT</td><td>R</td><td rowspan="2">Number of messages dropped out on one of the two transport paths since statistics reset.
The counter only continues to run until a channel completely fails.</td></tr>
<tr><td>Number of lost messages for theredundant channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Early Queue Usage</td><td>UDINT</td><td>R</td><td>Number of messages stored in Early Queue since statistics reset.</td></tr>
<tr><td>Bad Messages</td><td>UDINT</td><td>R</td><td>Number of rejected messages since statistics reset.</td></tr>
<tr><td>Frame No.</td><td>UDINT</td><td>R</td><td>Send counter (revolving).</td></tr>
<tr><td>Channel State</td><td>USINT</td><td>R</td><td>Current state of Channel 1.
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>0</td><td>No message on the state of channel 1.</td></tr>
<tr><td>1</td><td>Channel 1 OK.</td></tr>
<tr><td>2</td><td>The last message was faulty, the current one is OK.</td></tr>
<tr><td>3</td><td>Error on Channel 1.</td></tr>
</table></td></tr>
<tr><td>Last Channel Latency</td><td>UDINT</td><td>R</td><td rowspan="8"><i>Channel Latency</i> specifies the delay between two redundant transport paths and the reception time of messages with identical SeqNo.
A statistic is kept specifying the average, minimum, maximum and last latency.
If the minimum value is greater that the maximum value, the statistics values are invalid.
The values of <i>Last Channel Latency</i> and <i>Avg. Channel Latency</i> are then 0.</td></tr>
<tr><td>Last latency of the redundant channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Max. Channel Latency</td><td>UDINT</td><td>R</td></tr>
<tr><td>Maximum latency of the redundant channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Min. Channel Latency</td><td>UDINT</td><td>R</td></tr>
<tr><td>Minimum latency of the redundant channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Avg. Channel Latency</td><td>UDINT</td><td>R</td></tr>
<tr><td>Average latency of the redundant channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Monotony</td><td>UDINT</td><td>R</td><td>User data send counter (revolving).</td></tr>
</table>

<table>
<tr><th>Name</th><th>Data type</th><th>R/W</th><th>Description</th></tr>
<tr><td>Quality of Channel 1</td><td>BYTE</td><td>R</td><td>State of the main transport path.
<table>
<tr><th>Bit no.</th><th>Bit = 0</th><th>Bit = 1</th></tr>
<tr><td>0</td><td>Transport path not enabled</td><td>Transport path enabled</td></tr>
<tr><td>1</td><td>Transport path not used</td><td>Transport path actively used</td></tr>
<tr><td>2</td><td>Transport path not connected</td><td>Transport path connected</td></tr>
<tr><td>3</td><td>-</td><td>Transport path first provides message</td></tr>
<tr><td>4 - 7</td><td>Reserved</td><td>Reserved</td></tr>
</table></td></tr>
<tr><td>Quality of Channel 2</td><td>BYTE</td><td>R</td><td>State of the redundant transport path, see state of Channel 1 (main transport path).</td></tr>
<tr><td>Receive Timeout</td><td>UDINT</td><td>R</td><td>Time in milliseconds (ms) of PES1 within which a valid response must be received from PES2.</td></tr>
<tr><td>Response Time</td><td>UDINT</td><td>R</td><td>Time in milliseconds (ms) until the acknowledgment of a message is received by the sender.</td></tr>
<tr><td>Reset safe**ethernet** Statistics</td><td>BYTE</td><td>W</td><td>*In the user program, reset the statistical values for the communication connection (e.g., number of faulty messages, channel state, timestamp for the last fault on the red. channel [s], resends).*
<table>
<tr><th>Value</th><th>Function</th></tr>
<tr><td>0</td><td>No reset</td></tr>
<tr><td>1-255</td><td>Reset the safe**ethernet** statistics</td></tr>
</table></td></tr>
<tr><td>Signatur N</td><td>UDINT</td><td>R</td><td></td></tr>
<tr><td>Signatur N+1</td><td>UDINT</td><td>R</td><td></td></tr>
<tr><td>Transmission Control for Channel 1</td><td>BYTE</td><td>W</td><td>Transmission control of channel 1
<table>
<tr><th>Bit 0</th><th>Function</th></tr>
<tr><td>FALSE</td><td>Transport path enabled</td></tr>
<tr><td>TRUE</td><td>Transport path locked</td></tr>
</table>
<table>
<tr><th>Bit 1</th><th>Function</th></tr>
<tr><td>FALSE</td><td>Transport path enabled for tests</td></tr>
<tr><td>TRUE</td><td>Transport path locked</td></tr>
</table>
Bits 2...7 reserved.</td></tr>
<tr><td>Transmission Control for Channel 2</td><td>BYTE</td><td>W</td><td>Transmission control of channel 2,
see Transmission Control for Channel 1.</td></tr>
</table>

<table>
<tr><th>Name</th><th>Data type</th><th>R/W</th><th>Description</th></tr>
<tr><td>Connection Control</td><td>WORD</td><td>W</td><td>Use this system variable to control the safe<b>ethernet</b> connection from within the user program.
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>AUTOCONNECT (0x0000)</td><td>Default value:
After a safe<b>ethernet</b> communication loss, the controller attempts to re-establish the connection in the following CPU cycle.</td></tr>
<tr><td>Toggle Mode 0 (0x0100)Toggle Mode 1 (0x0101)</td><td>After a communication loss, the user program can change the toggle mode to re-establish the connection.
▪ TOGGLE MODE 0 (0x100) set: Set to TOGGLE MODE 1 (0x101) to re-establish the connection.
▪ TOGGLE MODE 1 (0x101) set: Set to TOGGLE MODE 0 (0x100) to re-establish the connection.</td></tr>
<tr><td>Disabled (0x8000)</td><td>safe<b>ethernet</b> communication is disabled.</td></tr>
</table></td></tr>
<tr><td>Connection State</td><td>UINT</td><td>R</td><td>The connection state evaluates the status of the communication between two controllers from within the user program.
<table>
<tr><th>Status/Value</th><th>Description</th></tr>
<tr><td>Closed (0)</td><td>The connection is closed and no attempt is made to open it.</td></tr>
<tr><td>Try_open (1)</td><td>Attempts are made to open the connection. This state applies for both the active and the passive sides.</td></tr>
<tr><td>Connected (2)</td><td>The connection is established and functioning (active time monitoring and data exchange)</td></tr>
</table></td></tr>
<tr><td>Version State</td><td>UINT</td><td>R</td><td>Reload version state of this safe<b>ethernet</b> connection
<table>
<tr><td>unknown</td><td>0x0000</td></tr>
<tr><td>up-to-date</td><td>0x0001</td></tr>
<tr><td>updated</td><td>0x0002</td></tr>
<tr><td>outdated</td><td>0x0003</td></tr>
</table></td></tr>
<tr><td>Resends</td><td>UDINT</td><td>R</td><td>Number of resends since statistics reset [UDINT].</td></tr>
<tr><td>Timestamp for the last fault on the red. channel [ms]</td><td>UDINT</td><td>R</td><td>Millisecond fraction of the timestamp
(current system time).</td></tr>
<tr><td>Timestamp for the last fault on the red. channel [s]</td><td>UDINT</td><td>R</td><td>Second fraction of the timestamp (current system time).</td></tr>
<tr><td>Timestamp of Last Error [ms]</td><td>UDINT</td><td>R</td><td>Millisecond fraction of the timestamp (current system time).</td></tr>
<tr><td>Timestamp of Last Error [ms]</td><td>UDINT</td><td>R</td><td>Second fraction of the timestamp (current system time).</td></tr>
</table>

<table>
<tr><th>Name</th><th>Data type</th><th>R/W</th><th>Description</th></tr>
<tr><td>Redundant Channel State</td><td>USINT</td><td>R</td><td>Current state of channel 2.
It is the current state of channel 2 when a message with Seq. no. X is being received (Seq. no X-1).
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>0</td><td>No message on the state of channel 2.</td></tr>
<tr><td>1</td><td>Channel 2 OK.</td></tr>
<tr><td>2</td><td>The last message was faulty, the current one is OK.</td></tr>
<tr><td>3</td><td>Error on channel 2.</td></tr>
</table></td></tr>
</table>

Table 12: System Variables Tab in the safeethernet Editor

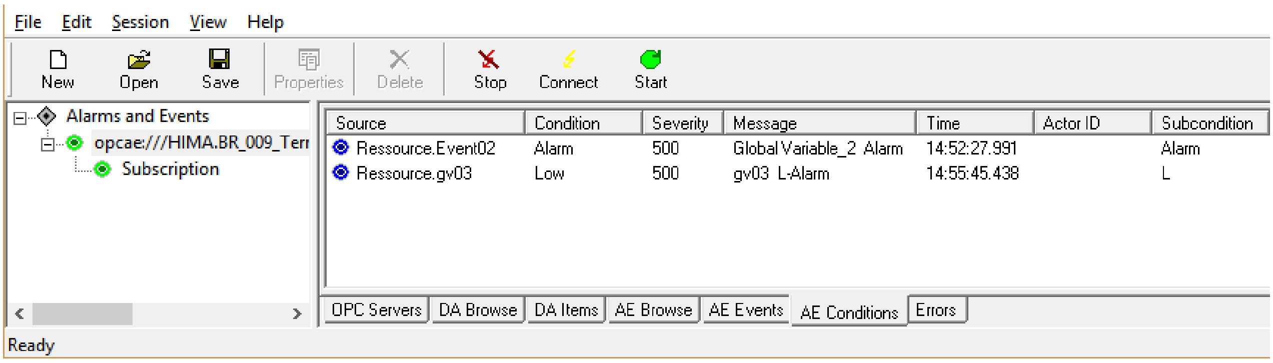
6 The A&E Editor of a Resource

The A&E Editor is used to configure the alarms and events of the HIMax/HIMatrix controller.

- Events are changes in the state of a system or controller that are provided with a timestamp.
- Alarms are events that signalize increased risk potential.

The *Activate A&E* parameter must be active to allow the X-OPC Server to read the alarms and events from the controller via the safe**ethernet** connection.

The HIMA system records the state changes as events specifying the time point when they occurred. The X-OPC Server transfers the events to OPC Clients such as control systems that display or evaluate the events.



Source	Condition	Severity	Message	Time	Actor ID	Subcondition
Ressource.Event02	Alarm	500	Global Variable_2 Alarm	14:52:27.991		Alarm
Ressource.gv03	Low	500	gv03 L-Alarm	14:55:45.438		L

Figure 11: Alarms and Events Displayed in an X-OPC Client

6.1 Configuring the A&E Editor

The A&E Editor contains the following three tabs:

- Event Definition BOOL
- Event Definition SCALAR
- Properties

To create an A&E Editor

1. In the structure tree, select **Configuration**, **Resource.**
2. Right-click **Resource** and select **New, Alarms&Events** from the context menu.
   ☑ A new Alarms&Events object is created.

6.1.1 The Event Definition BOOL Tab

- Changes of Boolean variables, e.g., of digital inputs.
- Alarm and normal state: These values can be arbitrarily assigned to the variable states.

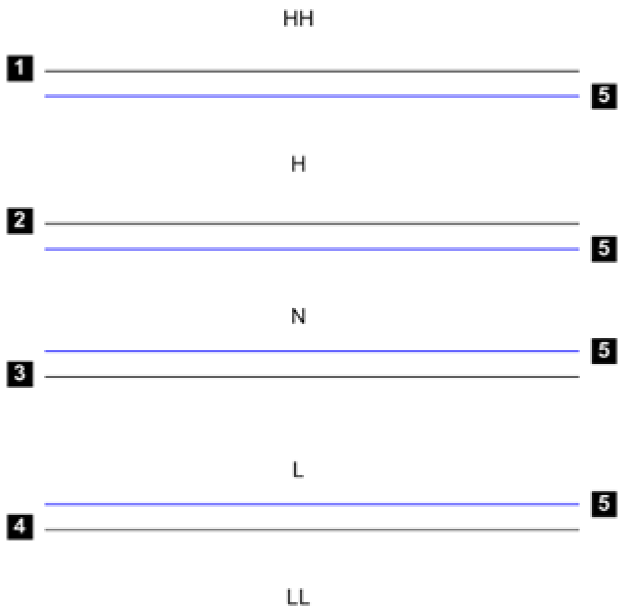
The parameters for **Boolean** events are entered in the A&E Editor of the resource. The editor contains the following tabs:

Column	Description	Range of values
Name	Name of the event definition Name that is displayed as *Source* in the OPC Client.	Text
Global Variable	Name of the assigned global variable (added using drag&drop).	
Data type	Data type of the global variable; cannot be changed.	BOOL
Event Source	CPU The timestamp is created on a processor module. The processor module creates all events in each of its cycles. I/O The time stamp is built on a suitable I/O module (e.g., DI 32 04). Auto A CPU event and, if available, IO events of the I/O module are created. For I/O events, the OPC Client displays as *Source* both the *Name* and the position. Example: Name_0_10_3 Default value: Auto	CPU, I/O, Auto
Alarm when FALSE	Activated If the global variable value changes from TRUE to FALSE, an event is triggered. Deactivated If the global variable value changes from FALSE to TRUE, an event is triggered. Default value: Deactivated	Checkbox activated, deactivated
Alarm Text	Text specifying the alarm state.	Text
Alarm Priority	Priority of the alarm state. Default value: 500	1...1000
Alarm Acknowledgment Required	Activated The alarm state must be confirmed by the user (acknowledgement). Deactivated The alarm state need not be confirmed by the user. Default value: Deactivated	Checkbox activated, deactivated
Return to Normal Text	Text specifying the alarm state.	Text
Return to Normal Severity	Priority of the normal state.	1...1000
Return to Normal Ack Required	The normal state must be confirmed by the user (acknowledgement). Default value: Deactivated	Checkbox activated, deactivated

Table 13: Parameters for Boolean Events

6.1.2 The Event Definition Scalar Tab

- Crossing the upper and lower limit values defined for a scalar variable.
- Scalar variables have a numeric data type, e.g., INT, REAL.
- Two upper limits and two lower limits are possible.
- The following condition must be met for the limits: Highest limit (HH) ≥ high limit (H) ≥ normal range ≥ low limit (L) ≥ lowest limit (LL).
- A hysteresis can be effective in the following cases:
  - If the value falls below one of the upper limits.
  - If the value exceeds one of the lower limits.



1 HH Alarm Value

2 H Alarm Value

3 L Alarm Value

4 LL Alarm Value

5 Hysteresis

Figure 12: Five Areas of a Scalar Event

A hysteresis is defined to avoid a needlessly large number of events when a global variable strongly oscillates around a limit.

The parameters for **scalar** events are entered in the A&E Editor of the resource. The editor contains the following tabs:

Column	Description	Range of values
Name	Name of the event definition Name that is displayed as *Source* in the OPC Client.	Text
Global Variable	Name of the assigned global variable (added using drag&drop).	
Data type	Data type of the global variable; cannot be changed.	Depending on the global variable type.
Event Source	CPU: The timestamp is created on a processor module. The processor module creates all events in each of its cycles. I/O: The timestamp is built on an appropriate I/O module (e.g., AI 32 02). Auto: A CPU event and, if available, IO events of the I/O module are created. For I/O events, the OPC Client displays as *Source* both the *Name* and the position. Example: "Name_0_10_3" Default value: Auto	CPU, I/O, Auto
HH Alarm Text	Text specifying the alarm state of the highest limit (HH).	Text
HH Alarm Value	Highest limit (HH) triggering an event. Condition: (HH alarm value - hysteresis) > H alarm value or HH alarm value = H alarm value	Depending on the global variable type.
HH Alarm Priority	Priority of the highest limit (HH) Default value: 500	1...1000
HH Alarm Acknowledgment Required	Activated: The operator must confirm that the highest limit (HH) has been overrun (acknowledgment). Deactivated: The operator need not confirm that the highest limit (HH) has been overrun. Default value: Deactivated	Checkbox activated, deactivated
H Alarm Text	Text specifying the alarm state of the high limit (H).	Text
H Alarm Value	High limit (H) triggering an event. Condition: (H alarm value - hysteresis) > (L alarm value + hysteresis) or H alarm value = L alarm value	Depending on the global variable type.
H Alarm Priority	Priority of the high limit (H) Default value: 500	1...1000
H Alarm Acknowledgment Required	Activated: The operator must confirm that the high limit (H) has been overrun (acknowledgment). Deactivated: The operator need not confirm that the high limit (H) has been overrun. Default value: Deactivated	Checkbox activated, deactivated
Return to Normal Text	Text specifying the alarm state.	Text
Return to Normal Severity	Priority of the normal state. Default value: 500	1...1000
Return to Normal Ack Required	Activated: The operator has to confirm the normal state (acknowledgment). Deactivated: The operator does not have to confirm the normal state. Default value: Deactivated	Checkbox activated, deactivated

Column	Description	Range of values
L Alarm Text	Text specifying the alarm state of the low limit (L).	Text
L Alarm Value	Low limit (L) triggering an event. Condition: (L alarm value + hysteresis) < (H alarm value - hysteresis) or L alarm value = H alarm value	Depending on the global variable type.
L Alarm Priority	Priority of low limit (L). Default value: 1	1...1000
L Alarm Acknowledgment Required	Activated: The operator must confirm that the low limit (L) has been underrun (acknowledgment). Deactivated: The operator need not confirm that the low limit (L) has been underrun. Default value: Deactivated	Checkbox activated, deactivated
LL Alarm Text	Text specifying the alarm state of the lowest limit (LL).	Text
LL Alarm Value	Lowest limit (LL) triggering an event. Condition: (LL alarm value + hysteresis) < (L alarm value) or LL alarm value = L alarm value	Depending on the global variable type.
LL Alarm Priority	Priority of the lowest limit (LL). Default value: 1	1...1000
LL Alarm Acknowledgment Required	Activated: The operator must confirm that the lowest limit (LL) has been underrun (acknowledgment). Deactivated: The operator need not confirm that the lowest limit (LL) has been underrun. Default value: Deactivated	Checkbox activated, deactivated
Alarm Hysteresis	The hysteresis avoids a continuous creation of many events if the process value often oscillates around a limit.	Depending on the global variable type.

Table 14: Parameters for Scalar Events

6.1.3 The Properties Tab

The **Properties** tab contains the following parameters:

Designation	Description
Type	Alarms&Events
Name	Name of the A&E Editor
A&E ID	An A&E Cookie is a unique 32-bit value and is generated for each individual alarm. An A&E Cookie allows an OPC Client to unambiguously identify an alarm. The interaction between OPC Client and Server (e.g., Ack.) functions via A&E Cookie. The OPC Client can only identify alarms from redundant X-OPC Servers as identical if the source name and the name of the corresponding A&E Cookie are identical. Not used: The A&E Cookie is still calculated based on the name and the server system ID. It is therefore different due to the requirement of unique IDs for redundant servers. A&E ID: The A&E Cookie is calculated based on the name and the event ID. This means that it remains the same for any event from a controller irrespective of the server. Range of values: 1...511 Default value: Not used

Table 15: Default Values Associated with the Priorities

7 Permitted Master IP Address Combinations

The general rules for assigning IP address and subnet masks must be adhered to.

7.1 Network Ports in Use for Ethernet Communication

All the following ports are destination ports.

UDP ports / use

123 SNTP (time synchronization between PES and remote I/O, PES and external devices).

6010 safe**ethernet** and OPC
6010 is the port on the HIMax/HIMatrix controller.
For X-OPC Server, this is the HH port configured in SILworX.
For the PADT, the X-OPC Server uses the PADT port specified during installation.

8000 Programming and operation with SILworX .

8 Support

Refer to the following table for any question, concern or suggestion related to the programming tool.

Area	Website or telephone
News, manuals	All the current manuals can be obtained upon request by sending an e-mail to: documentation@hima.com.
Contact details: On-site services	https://www.hima.com/en/about-hima/contacts-worldwide/
Technical support	https://www.hima.com/en/products-services/support/
Seminar program	https://www.hima.com/en/products-services/seminars/

Table 16: HIMA Support Service

Appendix

Glossary

Term	Description
ARP	Address resolution protocol, network protocol for assigning the network addresses to hardware addresses
COM	Communication module
CPU	Processor module
CRC	Cyclic redundancy check
EN	European standard
FB	Fieldbus
FBD	Function block diagrams
IEC	International electrotechnical commission
Interference-free	Supposing that two input circuits are connected to the same source (e.g., a transmitter). An input circuit is termed "interference-free" if it does not distort the signals of the other input circuit.
MAC address	Media access control address, hardware address of one network connection
PADT	Programming and debugging tool (in accordance with IEC 61131-3), PC with SILworX
PELV	Protective extra low voltage
PES	Programmable electronic system
Rack ID	Base plate identification (number)
SIL	Safety integrity level (in accordance with IEC 61508)
SILworX	Programming tool for HIMA controllers
SRS	System.Rack.Slot
TMO	Timeout
WDT	Watchdog time

Index of Figures

Index of Tables

MANUAL
X-OPC Server Version 5.2.1204

HI 801 480 E

For further information, please contact:

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone +49 6202 709-0
Fax +49 6202 709-107
E-mail info@hima.com

Learn more about HIMA solutions online:

🌐 www.hima.com/en/

www.hima.com