



Handbuch

X-OPC-Server

Version 5.2.1204

Alle in diesem Handbuch genannten HIMA Produkte sind mit dem Warenzeichen geschützt. Dies gilt ebenfalls, soweit nicht anders vermerkt, für weitere genannte Hersteller und deren Produkte.

HIQuad[®], HIQuad X[®], HIMax[®], HIMatrix[®], SILworX[®], XMR[®], HICore[®] und FlexSILon[®] sind eingetragene Warenzeichen der HIMA Paul Hildebrandt GmbH.

Alle technischen Angaben und Hinweise in diesem Handbuch wurden mit größter Sorgfalt erarbeitet und unter Einschaltung wirksamer Kontrollmaßnahmen zusammengestellt. Bei Fragen bitte direkt an HIMA wenden. Für Anregungen, z. B. welche Informationen noch in das Handbuch aufgenommen werden sollen, ist HIMA dankbar.

Technische Änderungen vorbehalten. Ferner behält sich HIMA vor, Aktualisierungen des schriftlichen Materials ohne vorherige Ankündigungen vorzunehmen.

Alle aktuellen Handbücher können über die E-Mail-Adresse documentation@hima.com angefragt werden.

© Copyright 2017, HIMA Paul Hildebrandt GmbH

Alle Rechte vorbehalten.

Kontakt

HIMA Adresse:

HIMA Paul Hildebrandt GmbH

Postfach 1261

68777 Brühl

Tel.: +49 6202 709-0

Fax: +49 6202 709-107

E-Mail: info@hima.com

Revisions- index	Änderungen	Art der Änderung	
		technisch	redaktionell
1.00	Erstausgabe des neu erstellten X-OPC Handbuch	X	X

Inhaltsverzeichnis

1	Einleitung	5
1.1	Aufbau und Gebrauch des Handbuchs	5
1.2	Zielgruppe	5
1.3	Darstellungskonventionen	6
1.3.1	Sicherheitshinweise	6
1.3.2	Gebrauchshinweise	7
2	Sicherheit	8
2.1	Bestimmungsgemäßer Einsatz	8
2.2	Restrisiken	8
2.3	Sicherheitsvorkehrungen	8
2.4	Notfallinformationen	8
2.5	Cyber-Security bei HIMA Systemen	8
3	Produktbeschreibung	10
3.1	Benötigte Ausstattung und Systemanforderung	10
3.2	Kompatibilitäten zu den Vorversionen	11
3.2.1	Synchronisationsmodus, Alarm&Event ID und Cookies	11
3.2.2	Forcen von Globalen Variablen auf E/A-Modulen	11
3.3	Eigenschaften der X-OPC Server Version V5.2.1204	12
3.4	Eigenschaften der HIMA Steuerung für X-OPC Verbindung	13
3.5	Erforderliche Aktionen bei Änderungen	14
4	Installation redundanter X-OPC Server	15
4.1	Konfiguration einer X-OPC Server Verbindung	15
4.1.1	Benötigte Software	15
4.1.2	Voraussetzungen für den X-OPC Server Betrieb	15
4.2	Installation auf dem Host-PC	16
4.3	OPC Server-Set in SILworX konfigurieren	19
4.3.1	Einstellungen im safeethernet Editor des OPC Server-Set	20
4.3.2	Erstellen der A&E-Acknowledge-Verbindung zwischen den redundanten X-OPC Servern	21
4.4	Data Access in der Detailansicht des safeethernet Editors konfigurieren	22
4.4.1	Fragment-Definitionen der OPC Empfangsvariablen erstellen	22
4.4.2	OPC Transportvariablen konfigurieren	22
4.5	Alarm&Events im Alarm&Event Editor konfigurieren	23
4.5.1	Codegenerierung und Verifikation	24
4.5.2	Anzeige im OPC Client	24
5	Beschreibung der X-OPC Server Editoren und Objekte	25
5.1	OPC Server-Set	25
5.1.1	Eigenschaften des OPC Server-Set	25
5.1.2	OPC Server Objekt	30
5.1.2.1	OPC Host Objekt	30
5.1.3	OPC A&E-Ack Objekt	30

5.2	safeethernet Editor Objekt	32
5.3	Detailansicht des safeethernet Editors	34
5.3.1	Register <i>OPC Server-Set</i> \leftrightarrow <i>Ressource</i>	34
5.3.2	Register <i>OPC Server-Set</i>	34
5.3.2.1	Register: Systemvariablen	35
6	Alarm&Event Editor der Ressource	39
6.1	Alarm&Event Editor konfigurieren	39
6.1.1	Register Event-Definition BOOL	40
6.1.2	Register Event-Definition Skalar	41
6.1.3	Register Eigenschaften	43
7	Erlaubte IP-Adressen Kombinationen des Masters	44
7.1	Verwendete Netzwerkports für Ethernet-Kommunikation	44
8	Support	45
	Anhang	46
	Glossar	46
	Abbildungsverzeichnis	47
	Tabellenverzeichnis	47

1 Einleitung

Das X-OPC Handbuch beschreibt die Eigenschaften und die Installation und Konfiguration des X-OPC mit dem Programmierwerkzeug SILworX.

Die Kenntnis von Vorschriften und das technisch einwandfreie Umsetzen der in diesem Handbuch enthaltenen Hinweise durch qualifiziertes Personal sind Voraussetzung für die Planung, Projektierung, Programmierung, Installation, Inbetriebnahme, Betrieb und Instandhaltung der HIMA Steuerungen.

Bei nicht qualifizierten Eingriffen in die Geräte, bei Abschalten oder Umgehen (Bypass) von Sicherheitsfunktionen oder bei Nichtbeachtung von Hinweisen dieses Handbuchs (und dadurch verursachten Störungen oder Beeinträchtigungen von Sicherheitsfunktionen) können schwere Personen-, Sach- oder Umweltschäden eintreten, für die HIMA keine Haftung übernehmen kann.

HIMA Automatisierungsgeräte werden unter Beachtung der einschlägigen Sicherheitsnormen entwickelt, gefertigt und geprüft. Nur für die in den Beschreibungen vorgesehenen Einsatzfälle mit den spezifizierten Umgebungsbedingungen verwenden.

1.1 Aufbau und Gebrauch des Handbuchs

Das Handbuch enthält die folgenden Hauptkapitel:

- Einleitung
- Sicherheit
- Produktbeschreibung
- Beschreibung der Konfiguration des X-OPCs in SILworX

Zusätzlich sind die folgenden Dokumente zu beachten:

Name	Inhalt	Dokumenten-Nr.
HIMax Systemhandbuch	Hardware-Beschreibung HIMax System	HI 801 000 D
HIMax Sicherheitshandbuch	Sicherheitsfunktionen des HIMax Systems	HI 801 002 D
HIMatrix Sicherheitshandbuch	Sicherheitsfunktionen des HIMatrix Systems	HI 800 022 D
HIMatrix Kompakt Systemhandbuch	Hardware-Beschreibung HIMatrix Kompakt System	HI 800 140 D
HIMatrix Modular Systemhandbuch	Hardware-Beschreibung HIMatrix Modular System	HI 800 190 D
Erste Schritte	Einführung in SILworX	HI 801 102 D

Tabelle 1: Zusätzlich geltende Handbücher

Die aktuellen Handbücher sind auf der HIMA Webseite www.hima.com zu finden. Anhand des Revisionsindex in der Fußzeile kann die Aktualität eventuell vorhandener Handbücher mit der Internetausgabe verglichen werden.

1.2 Zielgruppe

Dieses Dokument wendet sich an Planer, Projekteure und Programmierer von Automatisierungsanlagen sowie Personen, die zu Inbetriebnahme, Betrieb und Wartung der Anlagen und Systeme berechtigt sind. Vorausgesetzt werden spezielle Kenntnisse auf dem Gebiet der sicherheitsbezogenen Automatisierungssysteme.

1.3 Darstellungskonventionen

Zur besseren Lesbarkeit und zur Verdeutlichung gelten in diesem Dokument folgende Schreibweisen:

Fett	Hervorhebung wichtiger Textteile. Bezeichnungen von Schaltflächen, Menüpunkten und Registern im Programmierwerkzeug, die angeklickt werden können.
<i>Kursiv</i>	Parameter und Systemvariablen, Referenzen.
<i>Courier</i>	Wörtliche Benutzereingaben.
RUN	Bezeichnungen von Betriebszuständen (Großbuchstaben).
Kap. 1.2.3	Querverweise sind Hyperlinks, auch wenn sie nicht besonders gekennzeichnet sind. Im elektronischen Dokument (PDF): Wird der Mauszeiger auf einen Hyperlink positioniert, verändert er seine Gestalt. Bei einem Klick springt das Dokument zur betreffenden Stelle.

Sicherheits- und Gebrauchshinweise sind besonders gekennzeichnet.

1.3.1 Sicherheitshinweise

Um ein möglichst geringes Risiko zu gewährleisten, sind die Sicherheitshinweise unbedingt zu befolgen.

Die Sicherheitshinweise im Dokument sind wie folgt dargestellt.

- Signalwort: Warnung, Vorsicht, Hinweis.
- Art und Quelle des Risikos.
- Folgen bei Nichtbeachtung.
- Vermeidung des Risikos.

Die Bedeutung der Signalworte ist:

- Warnung: Bei Missachtung droht schwere Körperverletzung bis Tod.
- Vorsicht: Bei Missachtung droht leichte Körperverletzung.
- Hinweis: Bei Missachtung droht Sachschaden.

SIGNALWORT



Art und Quelle des Risikos!
Folgen bei Nichtbeachtung.
Vermeidung des Risikos.

HINWEIS



Art und Quelle des Schadens!
Vermeidung des Schadens.

1.3.2 Gebrauchshinweise

Zusatzinformationen sind nach folgendem Beispiel aufgebaut:

i

An dieser Stelle steht der Text der Zusatzinformation.

Nützliche Tipps und Tricks erscheinen in der Form:

TIPP

An dieser Stelle steht der Text des Tipps.

2 Sicherheit

Sicherheitsinformationen, Hinweise und Anweisungen in diesem Dokument unbedingt lesen. Die HIMA Steuerungen nur unter Beachtung aller Richtlinien und Sicherheitsrichtlinien einsetzen.

Die HIMA Steuerungen werden mit SELV oder PELV betrieben. Von diesen Steuerungen selbst geht kein Risiko aus. Einsatz im Ex-Bereich nur mit zusätzlichen Maßnahmen erlaubt.

2.1 Bestimmungsgemäßer Einsatz

Für den Einsatz von HIMA Steuerungen, sind die jeweiligen Bedingungen einzuhalten, siehe zusätzlich geltende Handbücher Tabelle 1.

2.2 Restrisiken

Von einem HIMA System selbst geht kein Risiko aus.

Restrisiken können ausgehen von:

- Fehlern in der Projektierung
- Fehlern im Anwenderprogramm
- Fehlern in der Verdrahtung

2.3 Sicherheitsvorkehrungen

Am Einsatzort geltende Sicherheitsbestimmungen beachten und vorgeschriebene Schutzausrüstung tragen.

2.4 Notfallinformationen

Ein HIMA System ist Teil der Sicherheitstechnik einer Anlage. Der Ausfall einer Steuerung bringt die Anlage in den sicheren Zustand.

Im Notfall ist jeder Eingriff, der die Sicherheitsfunktion des HIMA Systems verhindert, verboten.

2.5 Cyber-Security bei HIMA Systemen

Industrielle Steuerungen müssen gegen IT-typische Problemquellen geschützt werden. Diese Problemquellen sind:

- Angreifer innerhalb und außerhalb der Kundenanlage
- Bedienungsfehler
- Software-Fehler

Die Anforderungen der Sicherheits- und Anwendungsnormen bezüglich des Schutzes vor Manipulationen sind zu beachten. Die Autorisierung von Personal und die notwendigen Schutzmaßnahmen unterliegen der Verantwortung des Betreibers.

WARNUNG



Personenschaden durch unbefugte Manipulation an der Steuerung möglich!

Die Steuerung ist gegen unbefugte Zugriffe zu schützen!

Beispielsweise:

- die Standardeinstellungen für Login und Passwort ändern.
- physischen Zugang zur Steuerung, X-OPC Server und zum PADT kontrollieren!

Sorgfältige Planung sollte die zu ergreifenden Maßnahmen nennen. Nach erfolgter Risikoanalyse sind die benötigten Maßnahmen zu ergreifen. Solche Maßnahmen sind beispielsweise:

- Sinnvolle Einteilung von Benutzergruppen.
- Gepflegte Netzwerkpläne helfen sicherzustellen, dass secure Netzwerke dauerhaft von öffentlichen Netzwerken getrennt sind und, falls nötig, nur ein definierter Übergang (z. B. über eine Firewall oder eine DMZ) besteht.
- Verwendung geeigneter Passwörter.

Ein regelmäßiges Review (z. B. jährlich) der Security-Maßnahmen ist ratsam.

Die für eine Anlage geeignete Umsetzung der benötigten Maßnahmen liegt in der Verantwortung des Anwenders!

Weitere Einzelheiten siehe HIMA Cyber-Security Handbuch HI 801 372 D.

3 Produktbeschreibung

Der HIMA X-OPC Server Version V5.2.1204 dient als Übertragungsschnittstelle zwischen HIMax/HIMatrix Steuerungen und Fremdsystemen, die über eine OPC Schnittstelle verfügen.

OPC steht für *Open Platform Communications* und basiert auf der Microsoft DCOM-Technologie *Distributed Component Object Model* die für die Kommunikation zwischen den DCOM-Objekten (OPC Client und X-OPC Server) verwendet wird.

Der HIMA X-OPC Server wird nach der Installation auf dem PC als Windows-Dienst ausgeführt. Für weitere Informationen, siehe www.opcfoundation.org.

i

Die gesamte Konfiguration und die Bedienung des X-OPC Servers wird in SILworX durchgeführt. Im SILworX Control Panel kann der X-OPC Server wie eine Steuerung geladen, gestartet und gestoppt werden.

Der X-OPC Server unterstützt die folgenden Spezifikationen:

- **Data Access (DA) Versionen 1.0, 2.05a und 3.0**

DA ist speziell für die Übertragung von Echtzeitdaten ausgelegt und wird zum Lesen und Schreiben von globalen Variablen zwischen einer HIMax/HIMatrix Steuerung und dem OPC Client genutzt. Die DA-Spezifikationen sehen keine Schnittstellen vor, um DA-Clients mit historischen Werten zu versorgen.

- **Alarm&Event (A&E) Version 1.10**

A&E wird zur Übertragung von Alarmen und Ereignissen von der HIMax/HIMatrix Steuerung zum OPC Client genutzt. Jede globale Variable der HIMax/HIMatrix Steuerung kann mit der Ereignisaufzeichnung überwacht werden.

Ereignisse sind Änderungen des Zustands einer Variablen durch die Anlage oder der Steuerung, die mit einem Zeitstempel versehen sind.

Alarme sind solche Ereignisse, die eine Erhöhung des Risikopotentials signalisieren.

3.1 Benötigte Ausstattung und Systemanforderung

Die neuen Features vom X-OPC Server Version V5.2.1204 stehen erst ab SILworX V9 zur Verfügung. Es sollten für den Redundanzbetrieb immer die identischen Versionen vom X-OPC Server verwendet werden.

Element	Beschreibung
Aktivierung	Die Freischaltung erfolgt per Software-Freischaltcode, der über die HIMA Webseite Produkt-Registrierung->X-OPC Server generiert wird. Die folgenden Lizenzen können einzeln aktiviert werden: <ul style="list-style-type: none"> ▪ Data Access (DA) Server ▪ Alarm and Events (A&E) Server
Anforderungen an den Host-PC	Es gelten die gleichen Mindestanforderungen an den für den Betrieb eines X-OPC Servers verwendeten Rechners wie für SILworX. Die Mindestanforderungen sind auf der jeweiligen Installations-DVD angegeben. Speziell bei sehr großen Projekten können ältere Rechner möglicherweise lange Verarbeitungszeiten aufweisen und dadurch ungeeignet sein. Die Rechner-Hardware sollte daher möglichst dem Stand der Technik entsprechen. Bessere Hardware-Eigenschaften wie Rechenleistung und Speicherausbaufähigkeit führen zu verbesserter Performance.
	<div style="display: flex; align-items: center;"> <div style="font-size: 2em; margin-right: 10px;">i</div> <div>Die Minimalanforderungen gelten nur für den Betrieb eines X-OPC Servers, wenn keine weiteren Anwendungen (z. B. SILworX, Word usw.) auf dem Host-PC betrieben werden.</div> </div>

Tabelle 2: Systemanforderung und Ausstattung des X-OPC Server

3.2 Kompatibilitäten zu den Vorversionen

Der HIMA X-OPC Server Version 5.2.1204 ist zu allen vorherigen Versionen kompatibel. Ein Upgrade auf die neueste Version kann von allen vorherigen Versionen erfolgen.

3.2.1 Synchronisationsmodus, Alarm&Event ID und Cookies

Diese Features sind ab der Version 5.2.1204 verfügbar:

- Synchronisationsmodus:
Mit dem Synchronisationsmodus kann das Verhalten beim Aufstarten der redundanten X-OPC Server für die Synchronisation von Alarm&Events eingestellt werden, siehe Kapitel 5.1.1.
- Alarm&Event ID und Cookies:
Im Alarm&Event Editor der Steuerung kann mit dem Parameter *Alarm&Event ID* ein eindeutiger Wert (1...511) zugewiesen werden. Dieser wird in der Berechnung der Cookies aufgenommen und dient zur eindeutigen Identifikation der Eventquelle, siehe Kapitel 6.1.3. Wenn die Alarm&Event ID eingetragen ist, bekommen die redundanten X-OPC Server in einem Set identische Cookies unabhängig vom Synchronisationsmodus.

3.2.2 Forcen von Globalen Variablen auf E/A-Modulen

i

Werden von einem E/A-Modul die globale Variablen, die mit dem Prozesswert verbunden sind geforcet, wirken diese nicht auf die globalen Variablen, die mit den Parametern **->Zustand- LL, -L, -N, -H, -HH** verbunden sind.
Dies gilt auch dann, wenn diese Alarmer im Alarm&Event Editor eingetragen sind.
Beim testen müssen diese globalen Variablen einzeln geforcet werden.

3.3 Eigenschaften der X-OPC Server Version V5.2.1204

Element	Beschreibung						
OPC Server	Der X-OPC Server V5.2.1204 unterstützt die Funktionen <ul style="list-style-type: none"> ▪ OPC Data Access Custom Interface in den Versionen 1.0, 2.05a sowie 3.0. ▪ OPC Alarm&Event Interfaces 1.10 						
Sicherheitsbezogen	Der X-OPC Server läuft auf einem PC und ist nicht sicherheitsbezogen.						
Schnittstelle	Empfohlen: Ethernet 1Gbit/s						
Datenaustausch	Datenaustausch über safe ethernet .						
Ethernet Netzwerk	Die Netzwerkgeschwindigkeit des zugrundeliegenden Ethernet-Netzwerks muss dem Datenaufkommen entsprechend ausgelegt sein (min. 100 Mbit/s, empfohlen 1Gbit/s).						
Globale Variablen	Es können globale Variablen aus dem Kontext der Konfiguration verwendet werden.						
Erlaubte Variablentypen	Alle Datentypen, die in SILworX angelegt werden können sind erlaubt. Die Elemente von Strukturen/Arrays werden als Einzelvariablen aufgelöst und stehen nicht als Strukturen/Arrays zur Verfügung.						
Unerlaubte ASCII Zeichen	Die folgenden Zeichen sind reserviert und dürfen nicht (z. B. für globale Variablen) verwendet werden: ! " # ' , . / \ ` :						
HIMax/HIMatrix Steuerungen	Maximal 254 HIMax/HIMatrix Steuerungen können von einem X-OPC Server unterstützt werden. Umgekehrt kann eine Steuerung mit 254 OPC DA-Servern darunter maximal 4 X-OPC Server mit aktiviertem A&E kommunizieren.						
Prozessdatenmenge	Maximale Prozessdatenmenge zu einer Steuerung <table> <tr> <td>HIMax:</td> <td>128 kB</td> </tr> <tr> <td>HIMatrix vor F*03</td> <td>16 kB</td> </tr> <tr> <td>HIMatrix F*03:</td> <td>64 kB</td> </tr> </table>	HIMax:	128 kB	HIMatrix vor F*03	16 kB	HIMatrix F*03:	64 kB
HIMax:	128 kB						
HIMatrix vor F*03	16 kB						
HIMatrix F*03:	64 kB						
X-OPC Server	10 X-OPC Server können auf einem Host-PC betrieben werden.						
X-OPC Clients	Ein X-OPC Server kann 10 OPC Clients unterstützen.						
Data Access Tags	Ein Data Access Server unterstützt maximal 100 000 DA Tags. Definition: Tags: Vom X-OPC Server bereitgestellte Daten. Die Elemente von Strukturen/Arrays zählen als Einzel-Variablen. Items: Vom OPC Client angeforderte Daten.						
Alarm&Event Ereignisdefinitionen	Ein X-OPC Alarm&Event Server unterstützt maximal 100 000 Ereignisdefinitionen.						

Tabelle 3: Eigenschaften des X-OPC Server

i

Bei Änderung von einem Datentyp eines Tags in ein Array/ Struktur oder umgekehrt, muss vor dem Laden des X-OPC Servers, die betroffene Variable im OPC Client gelöscht und nach dem erneuten Laden wieder angelegt werden.

3.4 Eigenschaften der HIMA Steuerung für X-OPC Verbindung

Element	HIMax	HIMatrix F*03	HIMatrix vor F*03	Beschreibung
Prozessdatenmenge	128 kB	128 kB	16 kB	Prozessdatenmenge, die eine HIMA Steuerung maximal je safeethernet Verbindung zu einem X-OPC Server austauschen kann.
Fragment Größe	1100 Byte	1100 Bytes	900 Byte	Pro HIMax Zyklus wird nur ein Fragment zu einem X-OPC Server gesendet.
Ethernet Schnittstellen	10/100/1000BaseT	10/100BaseT	10/100BaseT	Verwendete Ethernet-Schnittstellen, simultan auch für andere Protokolle nutzbar.
Max. Anzahl Systemereignisse (CPU Event)	20 000	4000	n. a	Die als CPU Event definierten Ereignisse werden auf dem Prozessormodul gebildet. Dieses führt die Ereignisbildung komplett in jedem seiner Zyklen durch. Damit kann der Wert von jeder globalen Variablen als Ereignis erfasst und ausgewertet werden.
Max. Anzahl E/A Ereignisse (I/O Event)	6000	n. a	n. a	Die als I/O Event definierten Ereignisse können nur auf SOE E/A-Modulen (z. B. X-AI 32 02 oder X-DI 32 04) gebildet werden.
Größe des Ereignisspeichers	5000	1000 (Nur mit freigeschalteter Lizenz)	n. a	Nichtflüchtiger Ereignis-Puffer des HIMax Prozessormoduls. Ist der Ereignis-Puffer voll, werden keine neuen Ereignisse gespeichert, bis ein Ereigniseintrag von mindestens einem X-OPC A&E Server ausgelesen und damit zum Überschreiben markiert wurde.
Max. Anzahl X-OPC Server mit A&E	4	4	4	Maximale Anzahl X-OPC Server, die auf die HIMA Steuerung zugreifen können und Ereignisse simultan aus dem Ereignis-Puffer des Prozessormoduls lesen.
Max. Anzahl X-OPC Server ohne A&E	254	254	254	Maximale Anzahl X-OPC Server die mit HIMA Steuerung globale Variablen austauschen. Abzüglich der Anzahl X-OPC Server mit aktiviertem A&E.
n. a: nicht anwendbar				

Tabelle 4: Eigenschaften der HIMA Steuerung für X-OPC Verbindung

Wertebereich des Zeitstempels UTC (Universal Time Coordinated):

- sec Anteil seit 1970 in [UDWORD]
- ms Anteil der Sekunde als [UDWORD] von 0-999

Standardwert: 01.01.2000 / 00:00:00 Uhr. Eine automatische Sommer-, Winterzeitumstellung wird nicht unterstützt.

3.5 Erforderliche Aktionen bei Änderungen

Der Anwender hat dafür zu sorgen, dass Konfigurationsänderungen auf der Steuerung als auch auf dem X-OPC Server angewendet werden.

Bei der Durchführung einer Änderung durch Reload ist darauf zu achten, dass der X-OPC Server vor der Steuerung mit der neuen Konfiguration reloaded wird.

i

Die Benutzung von Reload zum Ändern der Ressource-Konfiguration ist mit der zuständigen Prüfstelle abzustimmen! Für weitere Informationen zum Reload, siehe Sicherheitshandbuch der jeweiligen Systemfamilie.

Die folgende Tabelle zeigt die Aktionen, die nach einer Änderung in den einzelnen Systemen durchgeführt werden müssen. Für weitere Informationen zu **safeethernet** Reload, siehe Kommunikationshandbuch HI 801 100 D.

Art der Änderung	Änderungen bei		
	HIMax	HIMatrix	X-OPC
DA			
Tags hinzufügen	C+R	C+R	C+R
Tagnamen (GV Namensänderung)	C+R	C+R	C+R
Tags löschen	C+R	C+R	C+R
Fragmente ändern (Parameter Hinzufügen/Löschen)	C+R	C+R	C+R
A&E			
Event Definition hinzufügen	C+R	C+R ¹⁾	C+R
Event Definition löschen	C+R	C+R ¹⁾	C+R
Ändern Event Source	C+R	C+R ¹⁾	C+R
Ändern Alarm Text	-	-	C+R
Ändern Alarm Severity	-	-	C+R
Ändern Parameter <i>ACK Required</i>	-	-	C+R
Ändern <i>Alarm Alarmwert</i> bei skalarem Event	C+R	C+R ¹⁾	C+R
Ändern Parameter <i>Alarm at False</i> bei boolean Events	C+R	C+R ¹⁾	C+R
Name ändern	C+R	C+R ¹⁾	C+R
E/A-Kanal mit GV verbinden	C+R	C+R ¹⁾	-
Zustandsvariablen mit GV verbinden	C+R	C+R ¹⁾	-
Generell			
Ändern safeethernet Parameter	C+D	C+D	C+D
C: Codegenerierung erforderlich R: Reload erforderlich D: Download erforderlich	n. a: nicht anwendbar -: keine Aktion nötig ¹⁾ ab F*03 mit SMR Lizenz anwendbar		

Tabelle 5: Erforderliche Aktionen bei Änderungen

4 Installation redundanter X-OPC Server

4.1 Konfiguration einer X-OPC Server Verbindung

In diesem Beispiel wird eine redundante X-OPC Server Verbindung mit einer HlMax Steuerung konfiguriert.

Die X-OPC Server stellen die Prozessvariablen und Ereigniswerte der HlMax Steuerung für die OPC Clients bereit. Die OPC Clients greifen auf die bereitgestellten Prozessvariablen und Ereigniswerte zu und stellen diese auf ihrer Benutzeroberfläche dar.

4.1.1 Benötigte Software

- SILworX
- X-OPC Server
- OPC Client

i

Die gesamte Konfiguration und die Bedienung des X-OPC Servers wird in SILworX durchgeführt. Im SILworX Control Panel kann der X-OPC Server wie eine Steuerung geladen, gestartet und gestoppt werden.

4.1.2 Voraussetzungen für den X-OPC Server Betrieb

- Das Ethernet-Netzwerk sollte eine Bandbreite von min. 100 Mbit/s (besser 1Gbit/s) haben.
- Die IP Adressen auf den PCs müsse in unterschiedlichen Subnetzen liegen.
- HIMA empfiehlt die Systemzeit der Rechner/Server zu synchronisieren, z. B. mittels SNTP.
- Es muss sichergestellt werden, dass die Datensätze für Data Access und Alarm&Events auf der Steuerung, den X-OPC Servern und den OPC Clients zueinander passen.
- Wenn OPC Client und X-OPC Server nicht auf dem gleichen PC laufen, dann muss die DCOM Schnittstelle angepasst werden. Für weitere Informationen, siehe www.opcfoundation.org.

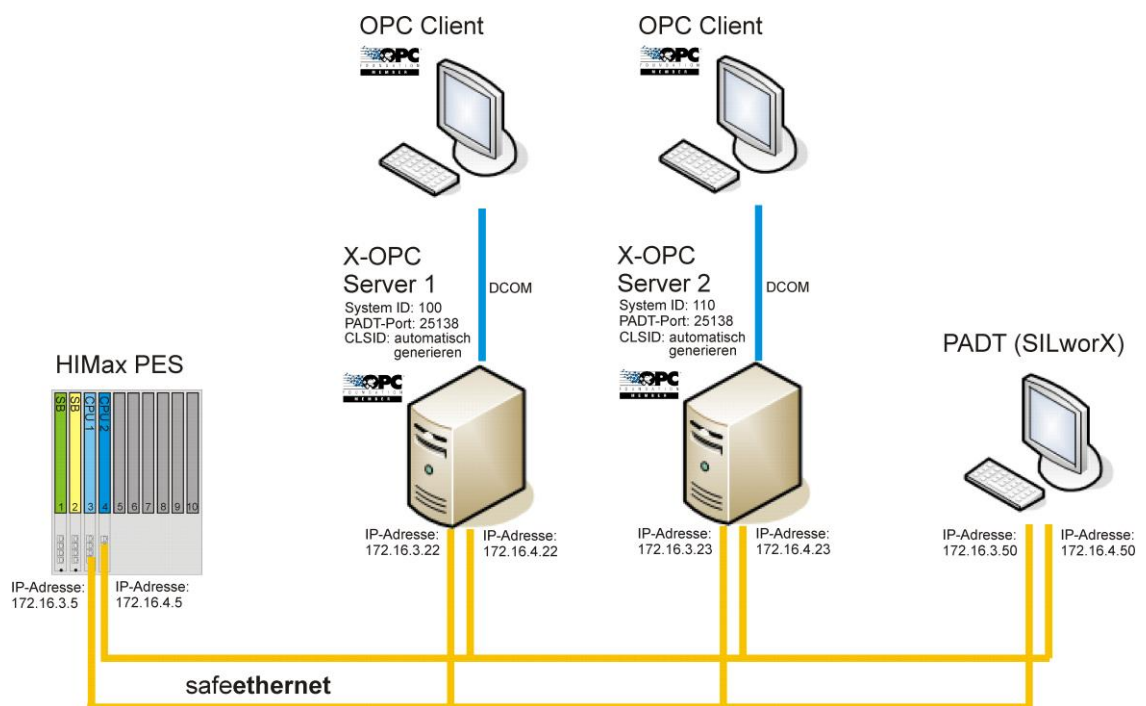


Bild 1: Redundanter X-OPC Betrieb

4.2 Installation auf dem Host-PC

Der X-OPC Server muss auf dem jeweiligen Host-PC installiert werden.

i

Die System-ID und die Nummer des PADT Port notieren. Diese werden zur Generierung des Lizenzschlüssels benötigt!

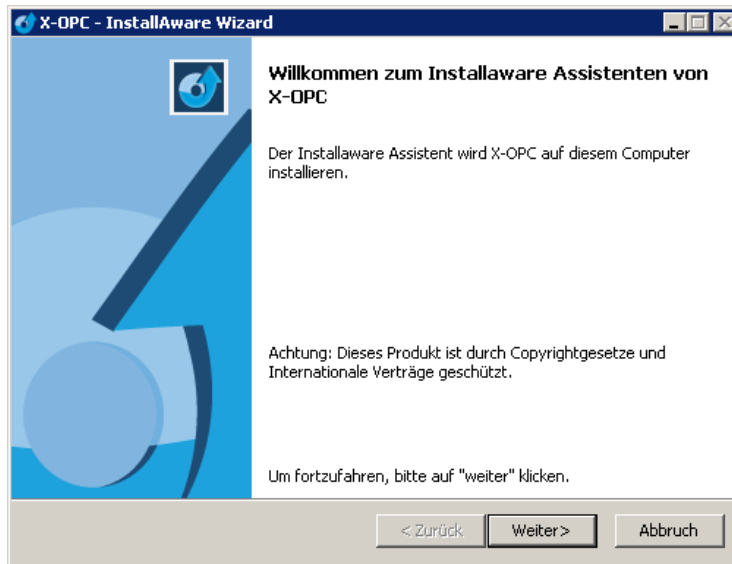


Bild 2: Installationsroutine des X-OPC Servers

X-OPC Server auf dem ersten Host-PC installieren

Datei *X-OPC.exe* auf dem jeweiligen Host-PC starten und der Installationsroutine folgen.

1. Folgende Daten für den X-OPC Server eingeben:
 - System-ID: 100
 - PADT Port: 25138
 - Frei wählbarer Name des X-OPC Servers (wird im OPC Client angezeigt).
2. Zum Installieren des X-OPC Servers **Weiter>** klicken.

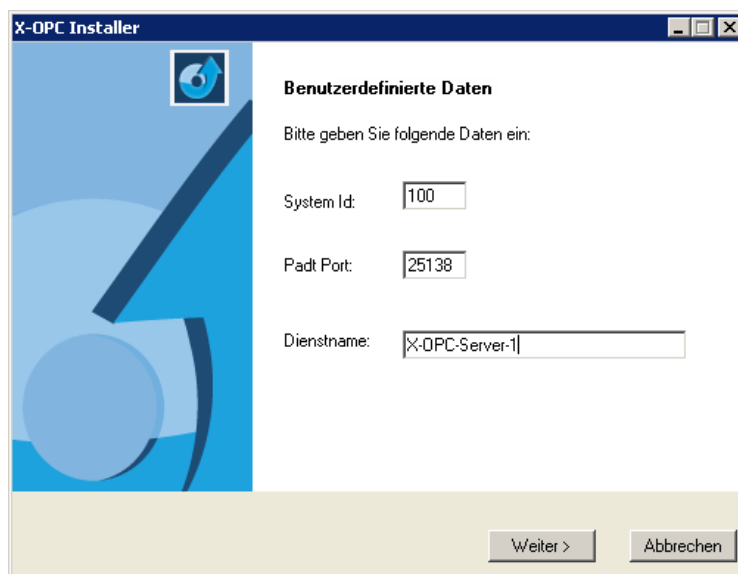


Bild 3: Installationsroutine des X-OPC Servers

Auf dem ersten Host-PC die CLSID automatisch generieren

1. Die CLSID Einstellung **automatisch** für DA und AE wählen.
2. Zum Installieren des X-OPC Servers **Weiter>** klicken.

ClassID des ersten X-OPC Servers ermitteln

Bei der redundanten Verbindung eines OPC Client mit zwei X-OPC Server erwarten einige OPC Client Systeme, dass die CLSID der beiden X-OPC Server gleich ist. Zuerst die CLSID des ersten X-OPC Servers ermitteln und diese notieren.

Die CLSID kann mit einer der folgenden Methoden ermittelt werden:

- Im OPC Client auslesen.
- In der Registry des Rechners/Servers unter `HKEY_CLASSES_ROOT\CLSID` die CLSID des ersten X-OPC Servers auslesen.

X-OPC Server auf dem zweiten Host-PC installieren

Die Datei *X-OPC.exe* auf dem zweiten Host-PC starten und der Installationsroutine folgen.

1. Folgende Daten für den X-OPC Server eingeben:
 - System-ID: 110
 - PADT Port: 25138
 - Frei wählbarer Name des X-OPC Servers (wird im OPC Client angezeigt).

i

PADT Port und HH Port des zweiten X-OPC Servers dürfen gleich dem ersten sein, wenn die X-OPC Server auf unterschiedlichen PCs betrieben werden.

2. Zur Bestätigung **Weiter>** klicken.

Auf dem zweiten Host-PC die gleiche CLSID einstellen**i**

Die CLSIDs der beiden X-OPC Server dürfen nur identisch sein, wenn die X-OPC Server auf unterschiedlichen PCs betrieben werden.

1. Die CLSID Einstellung **manuell** für DA und AE wählen.
2. Die ClassID des ersten X-OPC Servers in die Felder **CLSID** eintragen.
3. Zum Installieren des X-OPC Servers **Weiter>** klicken.

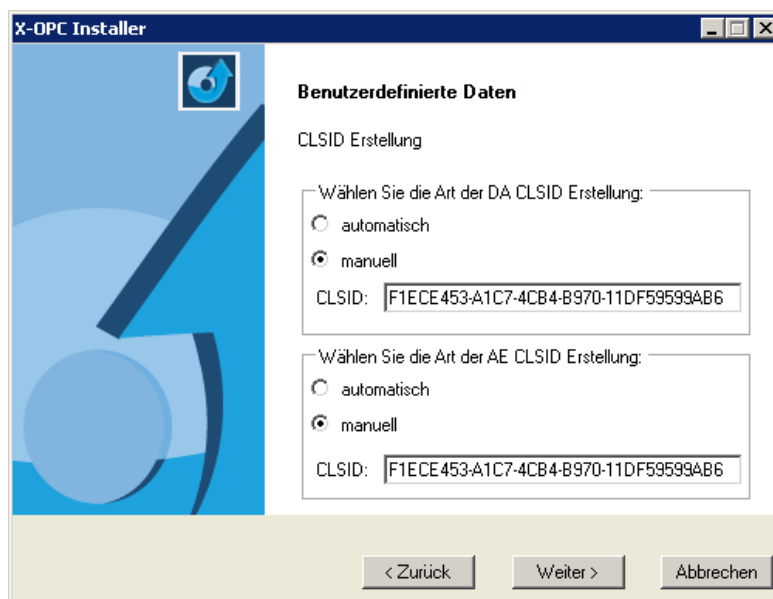


Bild 4: Einstellung manuell für die CLSID des zweiten X-OPC Servers

i

CLSIDs (ClassIdentifier) werden benutzt, um DCOM-Objekte eindeutig identifizieren zu können. Eine Class-ID besteht immer aus 5 Gruppen von Hex-Ziffern 8-4-4-4-12.

Eine mögliche CLSID wäre z. B. 2CA0AB0D-2BD1-48ED-8215-E06B203D44E6

Damit eine Änderung wirksam wird, muss der X-OPC Server (Dienst) neu gestartet werden.

Automatisches Starten der X-OPC Server nach einem Neustart des PCs

1. In Windows **Start, Einstellung, Systemsteuerung, Verwaltung, Dienste** öffnen und **X-OPC Server** aus der Liste wählen.
2. Im Kontextmenü des X-OPC Servers **Eigenschaften** wählen.
3. Im Register **Allgemein** den Starttyp **Automatisch** wählen.

Betrieb des X-OPC Servers auf dem PC sicherstellen

1. *Windows Task-Manager* öffnen und Register **Dienste** wählen.
2. Dienst *X-OPC.exe* starten, wenn X-OPC noch nicht auf dem PC gestartet wurde.

4.3 OPC Server-Set in SILworX konfigurieren

Das OPC Server-Set dient als gemeinsame Parametrierbasis für bis zu zwei OPC Server.

Die Eigenschaften des OPC Server-Set sind automatisch für beide redundanten X-OPC Server identisch.

In SILworX einen neuen OPC Server-Set anlegen

1. Im Strukturbaum **Konfiguration** öffnen.
2. Rechtsklick auf **Konfiguration** und im Kontextmenü **Neu, OPC Server-Set** wählen.
 - ☒ Ein neuer OPC Server-Set mit einem OPC Server wird angelegt. Dieser beinhaltet die **OPC Server-Set Objekte** und **Eigenschaften**, siehe Kapitel 5.1.

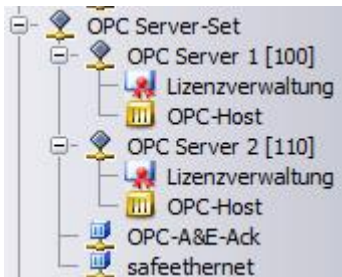


Bild 5: Redundanter X-OPC Betrieb

3. Rechtsklick auf **OPC Server-Set** und im Kontextmenü **Eigenschaften** wählen.
 - ☒ Synchronisationsmodus *Full* wählen.

In SILworX den ersten OPC Server konfigurieren

1. Im Strukturbaum **Konfiguration, OPC Server-Set, OPC Server** auswählen.
 - ☒ Dieser beinhaltet das **OPC Server Objekt**, siehe Kapitel 5.1.2.
2. Rechtsklick auf **OPC Server** und im Kontextmenü **Eigenschaften** wählen.
 - System-ID [SRS] (z. B. 100) eintragen.
3. Rechtsklick auf **OPC Host** und im Kontextmenü **Edit** wählen.
 - ☒ OPC Host Editor zur Konfiguration der IP-Schnittstellen wird geöffnet.
4. Rechtsklick auf eine leere Stelle im OPC Host Editor und im Kontextmenü **Neuer IP-Anschluss** wählen.
 - PADT-Port einstellen (z. B. 25138).
 - Erste IP-Adresse des PC, auf dem der X-OPC Server installiert ist (z. B. 172.16.3.22), einstellen und als Standardschnittstelle markieren.
 - Zweite IP-Adresse des PC, auf dem der X-OPC Server installiert ist (z. B. 172.16.4.22), einstellen.
 - HH-Port einstellen (z. B. 15138).

i

Sind auf einem PC mehrere X-OPC Server installiert, so muss für jeden Server sowohl der PADT-Port als auch der HH-Port eindeutig sein!

Ist auf dem PC eine Firewall installiert, dann müssen in der Konfiguration der Firewall die TCP/UDP PADT- und HH-Ports des X-OPC Servers als Ausnahmen eingetragen werden.

Konfigurieren des zweiten OPC Servers

1. Im Strukturbaum **Konfiguration**, **OPC Server-Set** auswählen.
2. Rechtsklick auf **OPC Server-Set** und im Kontextmenü **Neu, OPC Server** wählen.
 - ☒ Ein zweiter OPC Server wird hinzugefügt. Dieser beinhaltet das **OPC Server Objekt**, siehe Kapitel 5.1.2.
3. Rechtsklick auf diesen **OPC Server** und im Kontextmenü **Eigenschaften** wählen.
 - System-ID [SRS] (z. B. 110) eintragen.
4. Rechtsklick auf **OPC Host** und im Kontextmenü **Edit** wählen.
 - ☒ OPC Host Dialog zur Konfiguration der IP-Schnittstellen wird geöffnet.
5. Rechtsklick auf eine leere Stelle im OPC Host Dialog und im Kontextmenü **Neuer IP-Anschluss** wählen.
 - PADT-Port einstellen (z. B. 25138).
 - Erste IP-Adresse des PC, auf dem der X-OPC Server installiert ist (z. B. 172.16.3.23), einstellen und als Standardschnittstelle markieren.
 - Zweite IP-Adresse des PC, auf dem der X-OPC Server installiert ist (z. B. 172.16.4.23), einstellen.
 - HH-Port einstellen (z. B. 15138).

i

Ist auf dem PC eine Firewall installiert, dann müssen in der Konfiguration der Firewall die UDP PADT- und HH-Ports des X-OPC Servers als Ausnahmen eingetragen werden.

4.3.1 Einstellungen im safeethernet Editor des OPC Server-Set

Eine safeethernet Verbindung zwischen OPC Server-Set und Ressource erstellen

1. Im OPC Server-Set den **safeethernet Editor** öffnen.
 - ☒ Dieser beinhaltet das **safeethernet Editor Objekt**, siehe Kapitel 5.2.
2. In der Objektauswahl auf die gewünschte **Ressource** klicken und per Drag&Drop auf eine freie Stelle im Arbeitsbereich des **safeethernet Editors** ziehen.

safeethernet OPC Server-Set											
	Name	ID	Partner	IF Kanal 1 (lokal)	IF Kanal 2 (lokal)	IF Kanal 1 (fern)	IF Kanal 2 (fern)	Timing Master	Profil	Rsp t	Rcv TMO
1	OPC connection 1	0	HIMax					OPC Server-Set	Fast & Noisy	500	1000
2			OPC Server 1	100.x.x (172.16.3.22:15138)	100.x.x (172.16.4.22:15138)	1.0.1 (172.16.3.5:6010)	1.0.2 (172.16.4.5:6010)				
3			OPC Server 2	110.x.x (172.16.3.23:15138)	110.x.x (172.16.4.23:15138)	1.0.1 (172.16.3.5:6010)	1.0.2 (172.16.4.5:6010)				

Bild 6: safeethernet Editor des OPC Server-Sets

i

Die verwendete Ethernet Schnittstellen der PCs werden in der Spalte **IF Kanal1 (lokal)** abgebildet. Die Ethernet Schnittstellen der Ressource (Steuerung) müssen in der Spalte **IF Kanal1 (fern)** ausgewählt werden.

Die Standardwerte der **safeethernet** Parameter für die X-OPC Server Kommunikation sind auf die maximale Verfügbarkeit ausgelegt.

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

Informationen zu den **safeethernet** Parametern, siehe Kommunikationshandbuch HI 801 100 D.

Prioritäten für Alarm&Event Fragmente einstellen

Die im Alarm&Event Editor angelegten Ereignisse werden automatisch über **safeethernet** übertragen.

Die Priorität für die Ereignisse werden im **safeethernet** Editor des OPC Server-Set in den Spalten **Priorität Ereignisse** und **Priorität Zustandswerte** eingegeben. Diese Prioritäten gelten dann für alle Alarm&Event Fragmente dieser **safeethernet** Verbindung.

1. Den **safeethernet** Editor nach rechts scrollen.

☒ Der Parameter *A&E aktiv.* ist standardmäßig für Alarm&Events aktiviert.

safeethernet OPC Server-Set														
IF Kanal 2 (fern)	Timing Master	Profil	Rsp t	Rcv TMO	Rsnd TMO	Ack TMO	Prod Rate	Speicher	Verhalten	Diag.Eintr.	Prio A&E	Prio Sync	A&E aktiv.	Codegen
1	OPC Server-Set	Fast & Noisy	500	1000	500	0	0	2	Initialwert verwenden	1	1	10	<input checked="" type="checkbox"/>	ab V6
2 0.2 (172.16.4.5:6010)														
3 0.2 (172.16.4.5:6010)														

Bild 7: **safeethernet** Editor des OPC Server-Sets

2. Doppelklick auf **Prio A&E**, um die Priorität der Ereignisse zu ändern.
Alle Ereignisse dieser Ressource erhalten die in der Spalte **Prio A&E** eingetragene Priorität (z. B. 1). Damit wird festgelegt, mit welcher Priorität der X-OPC Server Ereignisse von der Steuerung anfordert. Sind zu diesem Zeitpunkt in der Steuerung keine Ereignisse vorhanden, werden auch keine übertragen.
3. Doppelklick auf **Prio Sync**, um die Priorität der Zustandswerte der Ereignisse zu synchronisieren. Alle Zustandswerte der Ereignisse dieser Ressource erhalten die in der Spalte **Prio Sync** eingetragene Priorität (z. B. 10).

i

Die Zustandswerte der Ereignisse werden nur zur Synchronisation (z. B. beim Verbindungsaufbau) benötigt, und können daher in einem größeren Zeitabstand als die Ereignisse übertragen werden.

4.3.2 Erstellen der A&E-Acknowledge-Verbindung zwischen den redundanten X-OPC Servern

Die Acknowledgements zur Quittierung der Alarme können auf den redundanten X-OPC Servern synchronisiert werden. Dazu wird im OPC Server-Set eine Acknowledge Verbindung angelegt.

HINWEIS



Die A&E-Acknowledge-Verbindung wird für den Synchronisations-Modus Full zwingend benötigt.

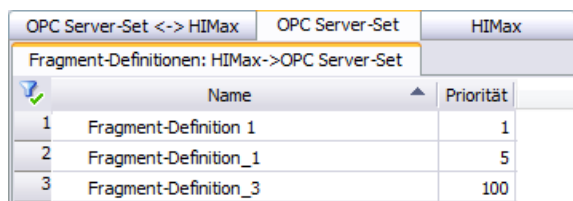
1. Im Strukturbaum **Konfiguration, OPC Server-Set, Neu** wählen.
2. Rechtsklick auf **OPC Server-Set** und im Kontextmenü **Neu, OPC A&E-Ack** wählen.
☒ Dieser beinhaltet das **OPC Server-Set Objekt**, siehe Kapitel 5.1.3.
3. Im OPC A&E-Ack Dialog die folgenden IP-Verbindungen wählen.
 - IF Kanal1 (OPC Server 1, z. B. 172.16.3.22).
 - IF Kanal2 (OPC Server 1, z. B. 172.16.4.22).
 - IF Kanal1 (OPC Server 2, z. B. 172.16.3.23).
 - IF Kanal2 (OPC Server 2, z. B. 172.16.4.23).

4.4 Data Access in der Detailansicht des safeethernet Editors konfigurieren

Die Konfiguration von DA findet in der Detailansicht des X-OPC safeethernet Editors statt.

4.4.1 Fragment-Definitionen der OPC Empfangsvariablen erstellen

1. Im OPC Server-Set den **safeethernet Editor** öffnen.
2. Rechtsklick auf die Zeile der **Ressource**, um das Kontextmenü der Ressource zu öffnen.
3. Im Kontextmenü **Edit** wählen, um die Detailansicht der **safeethernet** Verbindung zu öffnen.
☒ Diese beinhaltet die Detailansicht der **safeethernet** Verbindung, siehe Kapitel 5.3.
4. Register **OPC Server-Set: Fragment-Definitionen** wählen.
5. Rechtsklick auf eine freie Stelle im Arbeitsbereich und **Neue Fragment-Definition** wählen.
 In der Spalte *Priorität* wird eingestellt, wie oft dieses Fragment im Verhältnis zu den anderen Fragmenten gesendet wird (ein Fragment hat die Größe 1100 Byte).
 Für jede Fragment-Definition kann die Priorität des Fragments eingestellt werden. Mit der Priorität wird bestimmt, wie oft diese Variablen aktualisiert werden.
 - Eine Fragment-Definition mit globalen Variablen, die häufig aktualisiert werden, sollte eine hohe Priorität (z. B. 1) erhalten.
 - Eine Fragment-Definition mit globalen Variablen, die seltener aktualisiert werden, sollte eine niedrigere Priorität (z. B. 10) erhalten.



	Name	Priorität
1	Fragment-Definition 1	1
2	Fragment-Definition_1	5
3	Fragment-Definition_3	100

Bild 8: Detailansicht der **safeethernet** Verbindung

4.4.2 OPC Transportvariablen konfigurieren

Die OPC Sende- und Empfangsvariablen müssen im OPC Server-Set nur einmal angelegt werden. Diese werden automatisch von beiden X-OPC Servern im OPC Server-Set verwendet.

OPC Empfangsvariablen hinzufügen

OPC Empfangsvariablen werden von der Ressource zum OPC Server gesendet.

1. Detailansicht des X-OPC **safeethernet** Editors öffnen und Register **OPC Server-Set<->Ressource** wählen.
☒ Diese beinhaltet die Register **OPC Server-Set <-Ressource** und **OPC Server-Set->Ressource**, siehe Kapitel 5.3.1.
2. In der Objektauswahl eine **globale Variable** wählen und per Drag&Drop in den Bereich **OPC Server-Set <-Ressource-** ziehen.
3. Doppelklick auf Spalte **Fragmentname** und zuvor angelegte **Fragment Definition** wählen.
4. Diesen Schritt für weitere OPC Empfangsvariablen wiederholen.

OPC Sendevariablen hinzufügen:

OPC Sendevariablen werden vom OPC Server zur Ressource gesendet.

1. Detailansicht des X-OPC **safeethernet** Editors öffnen und Register **OPC Server-Set<->Ressource** wählen.
☒ Diese beinhaltet die Register **OPC Server-Set <-Ressource** und **OPC Server-Set->Ressource**, siehe Kapitel 5.3.1.
2. In der Objektauswahl eine **globale Variable** wählen und per Drag&Drop in den Bereich **OPC Server-Set->Ressource** ziehen.
3. Diesen Schritt für weitere OPC Sendevariablen wiederholen.

4.5 Alarm&Events im Alarm&Event Editor konfigurieren

Die Konfiguration der Alarm&Events findet im Alarm&Event Editor der Ressource statt. Die im Alarm&Event Editor angelegten Ereignisse werden automatisch über die konfigurierte **safeethernet** Verbindung übertragen, siehe Kapitel 4.3.1.

Alarm&Event Editor einer Ressource anlegen

1. Im Strukturbaum **Konfiguration, Ressource** selektieren.
2. Rechtsklick auf **Ressource** und im Kontextmenü **Neu, Alarm&Events** wählen.
 - ☒ Der Alarm&Event Editor wird neu hinzugefügt. Diese beinhaltet die Event-Definitionen und Eigenschaften, siehe Kapitel 6.

Alarm&Events anlegen

1. Rechtsklick auf **Alarm&Events** und **Edit** wählen.
2. Register **Event Definition Bool** für boolsche Ereignisse wählen, siehe Kapitel 6.1.1.
3. Register **Event Definition Skalar** für skalare Ereignisse wählen, siehe Kapitel 6.1.2.
4. In der Objektauswahl auf die **globale Variable** klicken und per Drag&Drop auf eine freie Stelle im Arbeitsbereich des Alarm&Event Editors ziehen.

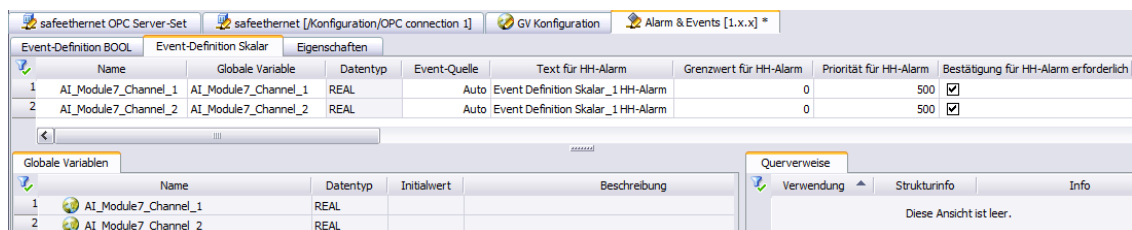


Bild 9: Alarm&Event Editor

Alarm&Events ID für Generierung eindeutiger Cookies der Ressource anlegen

1. Im Register **Eigenschaften** des Alarm&Events Editors wählen und neben dem Feld *Alarm&Event ID* die Schaltfläche ... anklicken.
 - ☒ Der *Alarm&Event ID* Dialog öffnet sich.
2. **Alarm&EventID** wählen und eine eindeutige *Alarm&Event ID* eintragen, siehe Kapitel 6.1.3.

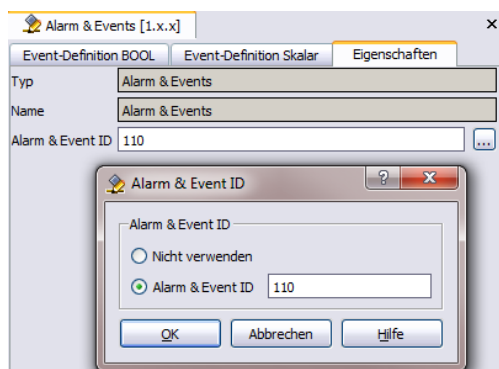


Bild 10: Alarm&Event ID

4.5.1 Codegenerierung und Verifikation

Codegenerierung und Laden der Ressource

1. Im Strukturbaum **Konfiguration, Ressource** selektieren.
2. Rechtsklick und im Kontextmenü **Codegenerierung** wählen.
3. Einträge im Logbuch sorgfältig überprüfen und Fehler gegebenenfalls korrigieren.
4. Den generierten Code in die Ressource laden.

Codegenerierung und Verifikation des OPC Server-Set

1. Im Strukturbaum **Konfiguration, OPC Server-Set** wählen.
2. Rechtsklick und im Kontextmenü **Codegenerierung** wählen.
3. Einträge im Logbuch sorgfältig überprüfen und Fehler gegebenenfalls korrigieren.

Den generierten Code in den X-OPC Server laden

1. Rechtsklick auf den **OPC Server** und aus dem Kontextmenü **Online** zum System-Login wählen.
2. Zugangsdaten eingeben:
 - IP-Adresse des PC, auf dem der X-OPC Server installiert ist (z. B. 172.16.3.23).
 - Benutzername: Administrator
 - Passwort: Feld leer lassen
3. Klick auf **Login** zum Öffnen des Control Panels.
4. In der SILworX Menüleiste auf das Symbol **Ressource Download** klicken.
 - ☒ Code wird in den X-OPC Server geladen.
5. In der SILworX Menüleiste auf das Symbol **Ressource Kaltstart** klicken.
 - ☒ X-OPC Server läuft.

4.5.2 Anzeige im OPC Client

Der im OPC Client angezeigte Name des X-OPC Servers setzt sich zusammen aus: **HIMA** (Hersteller).**Dienstname** (siehe Bild 3) **-DA** (Data Access).

Die Verbindung zum X-OPC Server herstellen. Die konfigurierten Data Access Daten sollten jetzt zum OPC Client übertragen werden.

Verbindung zum X-OPC Server herstellen. Die konfigurierten Alarm&Events sollten jetzt zum OPC Client übertragen werden.

i

Im Synchronisationsmodus *Nur Acknowledge* und *Full* erfolgt eine Aufsynchronisierung des X-OPC Servers, sobald eine Steuerung und ein X-OPC Server verbunden werden. Dazu liest der X-OPC Server von allen Variablen, die als Ereignis definiert sind, den aktuellen Zustand aus und überträgt die anstehenden Alarme zum OPC Client. Im OPC Client kann damit ein aktuelles Abbild über den Zustand der Steuerung gebildet werden. Erst ab diesem Zeitpunkt werden die Ereignisse ausgelesen. Weitere Informationen zum Synchronisationsmodus, siehe Kapitel 5.1.1.

5 Beschreibung der X-OPC Server Editoren und Objekte

Dieses Kapitel beschreibt die Eigenschaften des X-OPC Servers sowie die Menüfunktionen und Dialoge in SILworX, die zur Konfiguration des X-OPC Server benötigt werden.

i

Die gesamte Konfiguration und die Bedienung des X-OPC Servers wird in SILworX durchgeführt. Im SILworX Control Panel kann der X-OPC Server wie eine Steuerung geladen, gestartet und gestoppt werden.

5.1 OPC Server-Set

Das OPC Server-Set dient als gemeinsame Parametrierbasis für bis zu zwei OPC Server.

Die Eigenschaften des OPC Server-Set sind automatisch für beide redundanten X-OPC Server identisch.

Das OPC Server-Set beinhaltet die folgenden Objekte:

- OPC Server
- OPC A&E-Ack
- safeethernet Editor

Einen neuen OPC Server-Set anlegen

1. Im Strukturbaum **Konfiguration** selektieren.
2. Im Kontextmenü der Konfiguration **Neu, OPC Server-Set** wählen, um einen neuen OPC Server-Set hinzuzufügen.
3. Die Standardwerte im Kontextmenü von OPC Server-Set **Eigenschaften** übernehmen.

5.1.1 Eigenschaften des OPC Server-Set

Der Dialog *Eigenschaften* des OPC Server-Set enthält die folgenden Parameter:

Name	Beschreibung
Name	Name für den OPC Server-Set. Maximal 31 Zeichen.
Sicherheitszeit [ms]	Die Sicherheitszeit ist die Zeit in Millisekunden, innerhalb welcher der X-OPC Server auf einen Fehler reagieren muss. Bedingung: Sicherheitszeit $\geq 2 \times$ Watchdog-Zeit Wertebereich: 2000...400 000 ms Standardeinstellung: 20 000 ms
Watchdog-Zeit [ms]	Die Watchdog-Zeit ist die Zeit in Millisekunden, die der X-OPC Server zum Ausführen eines Programmzyklus maximal benötigen darf. Wird die vorgegebene Watchdog-Zeit überschritten, wird der X-OPC Server beendet. Bedingung: Watchdog-Zeit ≥ 1000 ms und $\leq 0.5 \times$ Sicherheitszeit Wertebereich: 1000...200 000 ms Standardeinstellung: 10 000 ms
Sollzykluszeit [ms]	Sollzykluszeit des X-OPC Servers Standardeinstellung: 50 ms
Sollzykluszeit-Modus	Dieser Parameter ist dazu verwendbar, die Zykluszeit möglichst konstant auf dem Wert von <i>Sollzykluszeit [ms]</i> zu halten. Aktivitäten wie Reload und Aufsynchrisation redundanter X-OPC Server werden soweit begrenzt, dass die Sollzykluszeit eingehalten wird.

Name	Beschreibung	
	fest	Ist ein X-OPC Zyklus kürzer als die definierte Sollzykluszeit, wird der X-OPC Zyklus bis zur Sollzykluszeit verlängert. Ist der X-OPC Zyklus länger als die Sollzykluszeit, setzt der X-OPC den Zyklus ohne Verzögerung fort.
	fest-tolerant	Wie <i>fest</i> , jedoch mit dem folgenden Unterschied: Wenn erforderlich wird bei der Aufsynchroisation die Sollzykluszeit für einen X-OPC Zyklus nicht eingehalten, um die Aufsynchroisation erfolgreich durchführen zu können.
	dynamisch	Der X-OPC führt jeden X-OPC Zyklus so schnell wie möglich aus. Dies entspricht einer eingestellten Sollzykluszeit von 0 ms.
	dynamisch-tolerant	Wie <i>dynamisch</i> , jedoch mit dem folgenden Unterschied: Wenn erforderlich wird bei der Aufsynchroisation die Sollzykluszeit für einen X-OPC Zyklus automatisch erhöht, um die Aufsynchroisation erfolgreich durchführen zu können.
	Standardeinstellung: fest-tolerant	
Max. Kom.-Zeitscheibe [ms]	Die max. Kom.-Zeitscheibe ASYNC [ms] ist die Zeit in Millisekunden, die pro X-OPC Server-Zyklus reserviert wird, um alle anstehenden Kommunikationsaufgaben für die Peer-to-Peer Kommunikation abzuarbeiten. Standardeinstellung: 500 ms	
Optimierte Nutzung Kom.-Zeitscheibe	Bei Aktivierung können für die Kommunikation über das Prozessormodul niedrigere Antwortzeiten erzielt werden. Achtung: Durch diesen Modus kann sich die zeitliche Ausnutzung der Async- Kom.-Zeitscheibe und somit auch Max. Dauer Konfigurationsverbindungen zum PADT in der Form ändern, dass diese stärker beansprucht werden kann (z. B beim Reload).	
Online-Einstellungen erlauben	Die Einstellung des OPC Schalters <i>Online-Einstellungen</i> erlauben beeinflusst die Funktion der anderen OPC Schalter. Wenn die Hauptfreigabe ausgeschaltet ist, können die Einstellungen der anderen OPC Schalter nicht verändert werden, während das Anwenderprogramm abgearbeitet wird (Steuerung in RUN). Standardeinstellung: aktiviert	
Autostart	Autostart legt fest, ob die OPC Konfigurationen nach dem Einschalten, oder nach dem Booten des OPC Servers per Kaltstart, per Warmstart oder nicht (Aus) automatisch gestartet werden dürfen. Wenn Autostart deaktiviert ist, geht der X-OPC Server nach dem Booten in den Zustand STOPP/GÜLTIGE KONFIGURATION. Standardeinstellung: deaktiviert	
Start erlaubt	Nur wenn <i>Start erlaubt</i> aktiviert ist, kann ein X-OPC Server vom Programmiergerät aus gestartet werden. Ist <i>Start erlaubt</i> ausgeschaltet, kann der X-OPC Server nicht vom Programmiergerät aus gestartet werden. In diesem Fall kann der X-OPC Server nur gestartet werden,	

Name	Beschreibung
	<p>wenn <i>Autostart</i> aktiviert ist und der Host-PC eingeschaltet oder neu gebootet wird.</p> <p>Ist weder <i>Autostart</i> noch <i>Start erlaubt</i> aktiviert, kann der X-OPC Server nicht mehr starten. Dies kann z. B. bei Wartungsarbeiten erforderlich sein, um das Anlaufen einer Anlage zu verhindern.</p> <p>Standardeinstellung: aktiviert</p>
Laden erlaubt	<p>Wenn <i>Laden erlaubt</i> deaktiviert ist, kann keine (neue) OPC Konfiguration in die Steuerung geladen werden.</p> <p><i>Laden erlauben</i> deaktivieren, wenn verhindert werden soll, dass in dem X-OPC Server eine geladene OPC Konfiguration überschrieben werden kann.</p> <p>Standardeinstellung: aktiviert</p>
Reload erlaubt	Noch keine Funktion!
Globales Forcen erlaubt	<p>Nur wenn <i>Globales Forcen erlaubt</i> aktiviert ist, kann globales Forcen gestartet werden.</p> <p>Standardeinstellung: deaktiviert</p> <p>Der Force-Editor kann auch dann zum Anzeigen von Variableninhalten aufgerufen werden, wenn <i>Globales Forcen erlaubt</i> ausgeschaltet ist.</p>
Globale Force-Timeout-Reaktion	<p>Wenn <i>Ressource stoppen</i> eingestellt ist, geht der X-OPC Server nach Ablauf der voreingestellten Force-Zeit in den Zustand STOPP. Alle Ausgänge des X-OPC Servers werden auf LOW gesetzt.</p> <p>Wenn <i>Nur Forcen beenden</i> eingestellt ist, setzt der X-OPC Server die Ausführung der OPC Konfiguration fort, auch nachdem die Force-Zeit abgelaufen ist.</p> <p>Standardeinstellung: <i>Nur Forcen beenden</i></p> <p>Falls <i>Globales Forcen erlaubt</i> eingestellt ist, ist die Einstellung für Stoppen bei Force-Timeout sorgfältig zu prüfen. Hierzu sind auch die Anmerkungen im Sicherheitshandbuch zu beachten.</p>
Minimale Konfigurationsversion	<p>-SILworX V2</p> <p>-SILworX V6</p> <p>-SILworX V9</p>
Systemvariablen	<p>Über die Schaltfläche Edit wird der Dialog <i>Systemvariablen</i> geöffnet.</p> <p>Dieser Dialog dient dazu, den normalerweise automatisch erzeugten OPC Tags für Systeminformationen entsprechende Alias-Namen für die Übertragung zum Client zu zuweisen.</p> <p>Beispiel:</p> <p>Die Systemvariable hat den Namen <i>Date/Time [ms portion]</i>. Da aber nicht jeder Client mit solchen Sonderzeichen im Namen zurechtkommt, kann stattdessen ein Alias-Name in diesem Dialog zugewiesen werden, z. B.</p> <p><i>Date_Time_s_portion</i>.</p> <p>Systemvariablen, die nicht an den OPC Client übertragen werden sollen, können mit <i>Ausblenden</i> ausgefiltert werden.</p>

Name	Beschreibung						
Synchronisationsmodus	<p>Dieser Parameter bestimmt den Synchronisationsmodus für die Synchronisierung der Conditions zwischen den redundanten X-OPC Server (Synchronisation z. B. beim Verbindungsaufbau).</p> <table border="1"> <tr> <td>Nur Acknowledge</td><td>Synchronisation mit der Ereignisquelle der Steuerung (globale Variable). Keine Synchronisation mit dem redundanten X-OPC Server. Damit ergeben sich beim Aufstarten unterschiedliche Zeitstempel der redundanten X-OPC Server gegenüber dem Client.</td></tr> <tr> <td>Simple</td><td>Synchronisation mit dem Ereignispuffer der Steuerung anhand des aktuellen Zeitstempels. Im Unterschied zu <i>Nur Acknowledge</i> und <i>Full</i> werden keine Zustände oder Zeitstempel mit dem redundanten X-OPC Server abgeglichen und auch nicht an den OPC Client gesendet. Nur Zustände und Zeitstempel neu auftretender Ereignisse sind identisch und werden an den OPC Client gesendet.</td></tr> <tr> <td>Full</td><td>Synchronisation mit der Ereignisquelle der Steuerung (globale Variable) erfolgt durch den zuerst aufstartenden X-OPC Server. Anschließend Synchronisation mit dem redundanten X-OPC Server.</td></tr> </table> <p>Standardeinstellung: Full</p>	Nur Acknowledge	Synchronisation mit der Ereignisquelle der Steuerung (globale Variable). Keine Synchronisation mit dem redundanten X-OPC Server. Damit ergeben sich beim Aufstarten unterschiedliche Zeitstempel der redundanten X-OPC Server gegenüber dem Client.	Simple	Synchronisation mit dem Ereignispuffer der Steuerung anhand des aktuellen Zeitstempels. Im Unterschied zu <i>Nur Acknowledge</i> und <i>Full</i> werden keine Zustände oder Zeitstempel mit dem redundanten X-OPC Server abgeglichen und auch nicht an den OPC Client gesendet. Nur Zustände und Zeitstempel neu auftretender Ereignisse sind identisch und werden an den OPC Client gesendet.	Full	Synchronisation mit der Ereignisquelle der Steuerung (globale Variable) erfolgt durch den zuerst aufstartenden X-OPC Server. Anschließend Synchronisation mit dem redundanten X-OPC Server.
Nur Acknowledge	Synchronisation mit der Ereignisquelle der Steuerung (globale Variable). Keine Synchronisation mit dem redundanten X-OPC Server. Damit ergeben sich beim Aufstarten unterschiedliche Zeitstempel der redundanten X-OPC Server gegenüber dem Client.						
Simple	Synchronisation mit dem Ereignispuffer der Steuerung anhand des aktuellen Zeitstempels. Im Unterschied zu <i>Nur Acknowledge</i> und <i>Full</i> werden keine Zustände oder Zeitstempel mit dem redundanten X-OPC Server abgeglichen und auch nicht an den OPC Client gesendet. Nur Zustände und Zeitstempel neu auftretender Ereignisse sind identisch und werden an den OPC Client gesendet.						
Full	Synchronisation mit der Ereignisquelle der Steuerung (globale Variable) erfolgt durch den zuerst aufstartenden X-OPC Server. Anschließend Synchronisation mit dem redundanten X-OPC Server.						
Peer Connection Timeout [ms]	<p>Dieser Parameter legt fest, wie lange der X-OPC auf den Aufbau der Verbindung zum redundanten X-OPC Server warten soll. Der Zustand der Verbindung wird innerhalb dieses Zeitraums zyklisch überprüft.</p> <p>Wertebereich: UDWORD Standardeinstellung: 2000 ms</p>						
Peer Synchronisation Timeout [ms]	<p>Dieser Parameter legt fest, wie lange der X-OPC auf die Synchronisationsdaten vom redundanten X-OPC Server warten soll. Beim Empfang der Synchronisationsdaten wird der Timer auf diesen festgelegten Wert zurückgesetzt.</p> <p>Wertebereich: UDWORD Standardeinstellung: 5000 ms</p>						
Namensraumtrennzeichen	<p>Wichtig für OPC Clients, welche verschiedene Trennzeichen benötigen.</p> <p>Punkt . Slash / Doppelpunkt : Backslash \</p> <p>Beispiel für Anzeigenamen im OPC Client: ResName . TagName ResName / TagName</p> <p>Standardeinstellung: Punkt</p>						
Namensraumtyp	<p>Je nach Anforderung des OPC Clients kann der Namensraumtyp eingestellt werden:</p> <ul style="list-style-type: none"> -Hierarchischer Namensraum -Flacher Namensraum 						

Name	Beschreibung
	Standardwert: Hierarchischer Namensraum
Changeless update	<p>Einstellung je nach Anforderung des OPC Clients.</p> <p>Aktiviert: Ist <i>Changeless update</i> aktiviert, liefert der X-OPC Server nach Ablauf der OPC Group-UpdateRate immer alle Items zum OPC Client.</p> <p>Deaktiviert: Ist <i>Changeless update</i> deaktiviert, werden nur geänderte Werte dem OPC Client geliefert (dieses Verhalten entspricht der OPC Spezifikation).</p>
Zyklusverzögerung [ms]	<p>Die Zyklusverzögerung begrenzt die CPU-Auslastung des PCs durch den X-OPC Server, damit auch andere Programme noch zur Abarbeitung kommen.</p> <p>Wertebereich: 1...100 ms</p> <p>Standardwert: 5 ms</p>
Short Tag-Names für DA	<p>Nur wenn <i>Flacher Namenraum</i> gewählt wurde, kann dieser Parameter aktiviert werden.</p> <p>Ist eine Option, bei der Daten und Event-Quellen ohne weiteren Kontext (Pfadname) dem OPC Client angeboten werden.</p> <p>Standardeinstellung: deaktiviert</p>
Simple-Events für CPU/EA Ereignisse	<ul style="list-style-type: none"> - Nie - Nur beim Start - Immer <p>Standardeinstellung: Nur beim Start</p>
Short Tag-Names für A&E	<p>Nur wenn <i>Flacher Namenraum</i> gewählt wurde, kann dieser Parameter aktiviert werden.</p> <p>Ist eine Option, bei der Daten und Events ohne weiteren Kontext (Pfadname) dem OPC Client angeboten werden.</p> <p>Standardeinstellung: deaktiviert</p>

Tabelle 6: Eigenschaften

5.1.2 OPC Server Objekt

Einen neuen OPC Server anlegen

1. Im Strukturbaum **Konfiguration**, **OPC Server-Set** selektieren.
2. Im Kontextmenü des OPC Server-Set **Neu**, **OPC Server** wählen, um einen neuen OPC Server hinzuzufügen.
3. Im Kontextmenü von OPC Server **Eigenschaften** wählen.

Der Dialog *Eigenschaften* des OPC Servers enthält die folgenden Parameter:

Element	Beschreibung
Name	Name für den OPC Server.
System-ID [SRS]	Standardwert: 60 000
Namensraumpräfix	Standardwert: Leer

Tabelle 7: Eigenschaften

5.1.2.1 OPC Host Objekt

OPC Host öffnen

1. Im Strukturbaum **Konfiguration**, **OPC Server-Set**, **OPC Server** selektieren:
2. Im Kontextmenü des OPC Host **Edit** wählen, um die Übersicht der IP-Schnittstellen zu öffnen.

Der Dialog *Edit* des OPC Host enthält die folgenden Parameter:

Element	Beschreibung
PADT-Port	Standardwert: 25138
Name	Name für den OPC Server-Set.
IP-Adresse	IP-Adresse des Host-PC. Standardwert: 192.168.0.1
Standard-Schnittstelle	Muss aktiviert werden, wenn der Host-PC mehr als einen Ethernet-Port besitzt. Standardwert: aktiviert
HH-Port	Standardwert: 15138

Tabelle 8: Edit

5.1.3 OPC A&E-Ack Objekt

Einen neuen OPC A&E-Ack anlegen

1. Im Strukturbaum **Konfiguration**, **OPC Server-Set** selektieren.
2. Im Kontextmenü des OPC Server-Set **Neu**, **OPC A&E-Ack** wählen, um einen neuen OPC A&E-Ack hinzuzufügen.
3. Im Kontextmenü von OPC A&E-Ack **Eigenschaften** wählen.

Das Register **Eigenschaften** des OPC A&E-Ack enthält die folgenden Parameter:

Element	Beschreibung
Typ	OPC A&E-Ack

Element	Beschreibung
Profil	Kombination zueinander passender safeethernet Parameter. Fast & Cleanroom Fast & Noisy Fixed Standardwert: Fast & Noisy
Response Time [ms]	Response Time ist die Zeit bis zur Empfangsbestätigung einer Nachricht beim Absender. Standardwert: 500
Receive Timeout [ms]	Receive Timeout ist die Überwachungszeit auf PES1, innerhalb der eine korrekte Antwort von PES2 empfangen werden muss. Standardwert: 1000
Resend Timeout [ms]	Resend Timeout ist die Überwachungszeit in ms auf PES1, innerhalb welcher PES2 den Empfang eines Datenpaketes bestätigt haben muss, ansonsten wird das Datenpaket wiederholt.
Acknowledge Timeout [ms]	Acknowledge Timeout ist die Zeit in ms, nach der ein empfangenes Datenpaket von der CPU spätestens bestätigt werden muss.
Produktionsrate	Produktionsrate ist das kleinste Zeitintervall zwischen zwei Datenpaketen.
Speicher	Anzahl der Datenpakete, die ohne Empfangsbestätigung versendet werden können.
Codegenerierungskompatibilität	Ab V6: optimierte safeethernet Signatur Vor V6: Standard safeethernet Signatur Standardwert: ab V6
safeethernet Verbindung ID	safeethernet Verbindungs-ID Wertebereich: 0...63
Timing Master	Der Timing-Master gibt für diese safeethernet Verbindung die <i>Receive Timeout</i> , <i>Resend Timeout</i> und die <i>Acknowledge Timeout</i> vor. Die gegenüberliegende Steuerung ist dann der Timing-Slave und übernimmt diese Werte. Wenn kein Timing-Master ausgewählt wurde, bestimmt die Steuerung mit der kleineren IP-Adresse diese safeethernet Parameter. *Partner A* *Partner B* Standardwert: *Partner A*

Tabelle 9: Eigenschaften

Das Register **Partner** des OPC A&E-Ack enthält die folgenden Parameter:

Element	Beschreibung
Partner	Auswahl des (ersten) OPC Servers aus dem OPC Set
IF Kanal 1	Erste IP-Adresse des Host-PC.
IF Kanal 2	Zweite IP-Adresse des Host-PC.
Partner	Auswahl des (zweiten) OPC Servers aus dem OPC Set
IF Kanal 1	Erste IP-Adresse des Host-PC.
IF Kanal 2	Zweite IP-Adresse des Host-PC.

Tabelle 10: Partner

5.2 safeethernet Editor Objekt

Der **safeethernet** Editor wird zum konfigurieren der **safeethernet** Verbindung der Ressourcen zu dem X-OPC Server-Set verwendet.

Öffnen des safeethernet Editors des X-OPC Server-Set

1. Im Strukturbaum **Konfiguration, OPC Server-Set** öffnen.
2. Rechtsklick auf **safeethernet** und im Kontextmenü **Edit** wählen.
☒ Der **safeethernet** Editor enthält den Arbeitsbereich und die Objektauswahl.

Dazu die Ressourcen aus der Objektauswahl in den Arbeitsbereich ziehen, die mit dem X-OPC Server verbunden werden sollen.

Zur Konfiguration der **safeethernet** Verbindung müssen die folgenden **safeethernet** Protokoll-Parameter eingestellt werden:

Parameter	Beschreibung
Name	Name der safeethernet Verbindung
ID	safeethernet Verbindungs ID Wertebereich: 0...63
Partner	Ressource-Name des Linkpartners
IF Kanal...	Verfügbare Ethernet-Schnittstellen auf der Ressource (lokal) und Ressource (fern).
Timing Master	Der Timing-Master gibt für diese safeethernet Verbindung die <i>Receive-Timeout</i> , <i>Resend-Timeout</i> und die <i>Acknowledge-Timeout</i> vor. Die gegenüberliegende Steuerung ist dann der Timing-Slave und übernimmt diese Werte. Wenn kein Timing-Master ausgewählt wurde, bestimmt die Steuerung mit der kleineren IP-Adresse diese safeethernet Parameter.
Profil	Kombination zueinander passender safeethernet Parameter.
Rsp t	Response Time ist die Zeit bis zur Empfangsbestätigung einer Nachricht beim Absender. Standardwert: 500 ms
Rcv TMO	Receive Timeout ist die Überwachungszeit auf PES1, innerhalb der eine korrekte Antwort von PES2 empfangen werden muss. Standardwert: 1000 ms
Rsnd TMO	Resend Timeout ist die Überwachungszeit in ms auf PES1, innerhalb welcher PES2 den Empfang eines Datenpaketes bestätigt haben muss, ansonsten wird das Datenpaket wiederholt.
Ack TMO	Acknowledge Timeout ist die Zeit in ms, nach der ein empfangenes Datenpaket von der CPU spätestens bestätigt werden muss.
Prod Rate	Produktionsrate ist das kleinste Zeitintervall zwischen zwei Datenpaketen.
Speicher	Anzahl der Datenpakete, die ohne Empfangsbestätigung versendet werden können.

Parameter	Beschreibung
Verhalten	Verhalten der Eingangsvariablen dieser safeethernet Verbindung bei Verbindungsunterbrechung.
	Initialwert verwenden Für die Eingangsvariablen werden die Initialdaten verwendet.
	Prozesswert unbegrenzt einfrieren Die Eingangsvariablen werden auf dem momentanen Wert eingefroren und bis zur erneuten Verbindungsaufnahme verwendet.
	Begrenzt Eingabe: Doppelklick auf Dropdown-Feld und Zeit eingeben. Die Eingangsvariablen werden auf dem momentanen Wert eingefroren und bis nach dem parametrierten Timeout verwendet. Danach werden die Initialdaten verwendet. Der Timeout kann sich um bis zu einem CPU-Zyklus verlängern.
Diag.Eintr.	Ist die Anzahl von Warnungen, die hintereinander in der Zeitspanne <i>Zeitraum Warnungen [ms]</i> auftreten müssen, bis diese in die Diagnose oder in die Kommunikations-Fehlerstatistik eingehen.
Prio A&E	Funktion ist nur für Verbindung zu X-OPC Server aktiviert. Damit wird festgelegt, mit welcher Priorität der X-OPC Server Ereignisse von der Steuerung anfordert. Fragmente mit der Priorität n und Fragmente mit der Priorität m werden im Verhältnis n zu m mal versendet.
Prio Sync	Funktion ist nur für Verbindung zu X-OPC Server aktiviert. Damit wird festgelegt, mit welcher Priorität der X-OPC Server Zustandswerte von der Steuerung anfordert. Fragmente mit der Priorität n und Fragmente mit der Priorität m werden im Verhältnis n zu m mal versendet.
A&E aktiv.	Der Parameter aktiviert die Übertragung der Ereignisse und Alarme der Steuerung zum X-OPC Server über diese safeethernet Verbindung. Die Ereignisse und Alarme werden im Alarm&Event Editor der jeweiligen Steuerung (Resource) konfiguriert, siehe Kapitel 6. Aktiviert: Über diese safeethernet Verbindung können Ereignisse und Alarme aus der Steuerung ausgelesen werden. Deaktiviert: Über diese safeethernet Verbindung können keine Ereignisse und Alarme aus der Steuerung ausgelesen werden. Standardwert: aktiviert
Codegen	Standardwert: ab V6 Ab V6: optimierte safeethernet Signatur Vor V6: Standard safeethernet Signatur

Tabelle 11: Parameter **safeethernet** Protokoll

5.3 Detailansicht des safeethernet Editors

Die Detailansicht hat immer den Bezug auf die Ressource, für die der **safeethernet** Editor gestartet wurde.

Öffnen der Detailansicht einer safeethernet Verbindung

1. Rechtsklick auf **safeethernet** Verbindung und Kontextmenü öffnen.
2. **Edit** wählen.

Die Detailansicht beinhaltet die folgenden drei Register:

- OPC Server-Set<->Ressource
- OPC Server-Set
- Ressource

5.3.1 Register *OPC Server-Set<->Ressource*

Das Register *OPC Server-Set<->Ressource* ist in zwei Bereiche *Ressource->OPC Server-Set* und *OPC Server-Set->Ressource* aufgeteilt.

In diese beiden Bereiche für die jeweilige gewünschte Transportrichtung können aus der Objektauswahl *globale Variablen* per Drag&Drop für den Transport gezogen werden.

5.3.2 Register *OPC Server-Set*

Das Register *OPC Server-Set* enthält die *Fragment-Definitionen*.

Eine HIMA Steuerung kann je nach Typ 128 kB oder 16 kB je **safeethernet** Verbindung zu einem X-OPC Server senden, jedoch nur ein Fragment (1100 Byte oder 900 Byte) pro HIMA CPU-Zyklus. Um mehr Daten über eine **safeethernet** Verbindung zu senden, werden die Daten fragmentiert. Mit dem Parameter *Priorität* dieser Fragmente kann bestimmt werden, wie häufig diese Fragmente aktualisiert werden sollen.

i

Fragmente mit der Priorität **n** und Fragmente mit der Priorität **m** werden im Verhältnis **n** zu **m** mal versendet.

Für die Reaktionszeit von der Steuerung zum X-OPC Server ist zusätzlich die Anzahl der Fragmente und Kommandos (z. B. Stopp, Start) von SOE zu berücksichtigen.

$T_R = t_1 + t_2 + t_3 + t_4$; gilt nur, wenn die Priorität aller Fragmente für Zustandsdaten 1 ist

T_R	Worst Case Reaction Time
t_1	Sicherheitszeit des PES 1
t_2	<i>Anzahl Fragmente * ReceiveTMO</i>
t_3	Sicherheitszeit des X-OPC Servers
t_4	Zeitverzug durch SOE Funktion; abhängig von Ereignisaufkommen und Verbindungsaufnahme

Für die umgekehrte Richtung kann die Reaktionszeit mit der selben Formel ermittelt werden, nur dass hierbei in der Regel nur ein Fragment zum Tragen kommt, da der X-OPC Server nur die von OPC Clients geschriebenen Daten transferiert.

Maximale Anzahl der Fragmente: 1024

Maximale Größe eines Fragments: 1100 Byte oder 900 Byte

Wertebereich der Prioritäten: 1 (höchste) bis 65 535 (niedrigste)

5.3.2.1 Register: Systemvariablen

Die safe**ethernet** Verbindung zum jeweiligen X-OPC Server des Sets kann mit Hilfe von Systemvariablen gesteuert und ausgewertet werden.

Name	Datentyp	R/W	Beschreibung										
Die folgenden Status und Parameter können globalen Variablen zugewiesen und im Anwenderprogramm verwendet werden													
Ack-Frame-Nr.	UDINT	R	Empfangszähler (umlaufend).										
Anzahl defekter Nachrichten	UDINT	R	Anzahl aller defekter Nachrichten pro Kanal (falscher CRC, falscher Header, sonstige Fehler).										
Anzahl defekter Nachrichten des Red. Kanal	UDINT	R											
Anzahl Verbindungserfolge	UDINT	R	Anzahl der Verbindungserfolge seit Reset der Statistik.										
Anzahl verlorener Nachrichten	UDINT	R	Anzahl der auf einem der beiden Transportwege ausgefallenen Nachrichten seit Reset der Statistik. Der Zähler wird nur bis zum Komplettausfall eines Kanals geführt.										
Anzahl verlorener Nachrichten des Red.-Kanal	UDINT	R											
Early Queue Usage	UDINT	R	Anzahl der Nachrichten die in Early Queue gelegt wurden seit Reset der Statistik.										
Fehlerhafte Nachrichten	UDINT	R	Anzahl verworfener Nachrichten seit Reset der Statistik.										
Frame-Nr.	UDINT	R	Sendungszähler (umlaufend).										
Kanalzustand	USINT	R	Aktueller Kanalzustand von Kanal 1.										
			<table><tr><th>Status</th><th>Beschreibung</th></tr><tr><td>0</td><td>Keine Nachricht zum Zustand von Kanal 1.</td></tr><tr><td>1</td><td>Kanal 1 OK.</td></tr><tr><td>2</td><td>Letzte Nachricht war Fehlerhaft, aktuelle ist OK.</td></tr><tr><td>3</td><td>Fehler auf Kanal 1.</td></tr></table>	Status	Beschreibung	0	Keine Nachricht zum Zustand von Kanal 1.	1	Kanal 1 OK.	2	Letzte Nachricht war Fehlerhaft, aktuelle ist OK.	3	Fehler auf Kanal 1.
			Status	Beschreibung									
			0	Keine Nachricht zum Zustand von Kanal 1.									
			1	Kanal 1 OK.									
			2	Letzte Nachricht war Fehlerhaft, aktuelle ist OK.									
3	Fehler auf Kanal 1.												
Letzte Kanal Latenz	UDINT	R	Die <i>Kanal Latenz</i> gibt die Verzögerung zwischen beiden redundanten Transportpfaden zum Empfangszeitpunkt von Nachrichten mit identischer SeqNo an. Hierfür wird eine Statistik mit durchschnittlicher, minimaler, maximaler und letzter Latenz geführt. Ist der Min-Wert > dem Max-Wert, so sind die Statistikwerte ungültig. <i>Letzte Kanal Latenz</i> und <i>Mittlere Kanal Latenz</i> sind dann 0.										
Letzte Latenz des Red.-Kanal	UDINT	R											
Max. Kanal Latenz	UDINT	R											
Max. Latenz des Red. Kanal	UDINT	R											
Min. Kanal Latenz	UDINT	R											
Min. Latenz des Red. Kanal	UDINT	R											
Mittlere Kanal Latenz	UDINT	R											
Mittlere Latenz des Red. Kanal	UDINT	R											
Monotonie	UDINT	R	Nutzdatensendungszähler (umlaufend).										

Name	Datentyp	R/W	Beschreibung																		
Qualität Kanal 1	BYTE	R	Zustand des Haupt-Transportweges.																		
			<table><tr><th>Bit Nr.</th><th>Bit = 0</th><th>Bit = 1</th></tr><tr><td>0</td><td>Transportweg nicht freigegeben</td><td>Transportweg freigegeben</td></tr><tr><td>1</td><td>Transportweg nicht genutzt</td><td>Transportweg aktiv genutzt</td></tr><tr><td>2</td><td>Transportweg nicht verbunden</td><td>Transportweg verbunden</td></tr><tr><td>3</td><td>-</td><td>Transportweg liefert Nachricht zuerst</td></tr><tr><td>4 - 7</td><td>Reserviert</td><td>Reserviert</td></tr></table>	Bit Nr.	Bit = 0	Bit = 1	0	Transportweg nicht freigegeben	Transportweg freigegeben	1	Transportweg nicht genutzt	Transportweg aktiv genutzt	2	Transportweg nicht verbunden	Transportweg verbunden	3	-	Transportweg liefert Nachricht zuerst	4 - 7	Reserviert	Reserviert
			Bit Nr.	Bit = 0	Bit = 1																
			0	Transportweg nicht freigegeben	Transportweg freigegeben																
			1	Transportweg nicht genutzt	Transportweg aktiv genutzt																
			2	Transportweg nicht verbunden	Transportweg verbunden																
			3	-	Transportweg liefert Nachricht zuerst																
4 - 7	Reserviert	Reserviert																			
Qualität Kanal 2	BYTE	R	Zustand des redundanten Transportweges, siehe Zustand Kanal 1 (Haupt-Transportweg).																		
Receive Timeout	UDINT	R	Zeit in Millisekunden (ms) auf PES1, innerhalb der eine gültige Antwort von PES2 empfangen werden muss.																		
Response Time	UDINT	R	Zeit in Millisekunden (ms) bis zur Empfangsbestätigung einer Nachricht beim Absender.																		
safe ethernet Statistik zurücksetzen	BYTE	W	Statistikwerte für die Kommunikationsverbindung im Anwenderprogramm zurücksetzen (z. B. <i>Anzahl defekter Nachrichten, Kanalzustand, Zeitstempel des letzten Fehlers des Red.-Kanal ..., Wiederholungen</i>).																		
			<table><tr><th>Wert</th><th>Funktion</th></tr><tr><td>0</td><td>Kein Reset</td></tr><tr><td>1-255</td><td>Reset der safeethernet Statistik</td></tr></table>	Wert	Funktion	0	Kein Reset	1-255	Reset der safe ethernet Statistik												
			Wert	Funktion																	
			0	Kein Reset																	
1-255	Reset der safe ethernet Statistik																				
Signatur N	UDINT	R																			
Signatur N+1	UDINT	R																			
Transport-Steuerung Kanal1	BYTE	W	Transportsteuerung von Kanal1																		
			<table><tr><th>Bit 0</th><th>Funktion</th></tr><tr><td>FALSE</td><td>Transportweg freigegeben</td></tr><tr><td>TRUE</td><td>Transportweg gesperrt</td></tr></table>	Bit 0	Funktion	FALSE	Transportweg freigegeben	TRUE	Transportweg gesperrt												
			Bit 0	Funktion																	
			FALSE	Transportweg freigegeben																	
			TRUE	Transportweg gesperrt																	
			<table><tr><th>Bit 1</th><th>Funktion</th></tr><tr><td>FALSE</td><td>Transportweg für Tests freigegeben</td></tr><tr><td>TRUE</td><td>Transportweg gesperrt</td></tr></table>	Bit 1	Funktion	FALSE	Transportweg für Tests freigegeben	TRUE	Transportweg gesperrt												
			Bit 1	Funktion																	
FALSE	Transportweg für Tests freigegeben																				
TRUE	Transportweg gesperrt																				
Bit 2...7 reserviert.																					
Transport-Steuerung Kanal2	BYTE	W	Transportsteuerung von Kanal 2, siehe Transportsteuerung Kanal 1.																		

Name	Datentyp	R/W	Beschreibung								
Verbindungssteuerung	WORD	W	Mit dieser Systemvariablen kann die safeethernet Verbindung vom Anwenderprogramm gesteuert werden.								
			<table><tr><th>Befehl</th><th>Beschreibung</th></tr><tr><td>Autoconnect (0x0000)</td><td>Standardwert: Nach Verlust der safeethernet Kommunikation versucht die Steuerung im nächsten CPU-Zyklus, die Verbindung wieder aufzunehmen.</td></tr><tr><td>Toggle Mode 0 (0x0100) Toggle Mode 1 (0x0101)</td><td>Nach dem Kommunikationsverlust kann durch einen programmgesteuerten Wechsel des Toggle-Modus die Verbindung erneut aufgebaut werden.<ul style="list-style-type: none">▪ TOGGLE MODE 0 (0x100) gesetzt: Auf TOGGLE MODE 1 (0x101) setzen um die Verbindung wieder aufzunehmen.▪ TOGGLE MODE 1 (0x101) gesetzt: Auf TOGGLE MODE 0 (0x100) setzen um die Verbindung wieder aufzunehmen.</td></tr><tr><td>Disabled (0x8000)</td><td>safeethernet Kommunikation abgeschaltet.</td></tr></table>	Befehl	Beschreibung	Autoconnect (0x0000)	Standardwert: Nach Verlust der safeethernet Kommunikation versucht die Steuerung im nächsten CPU-Zyklus, die Verbindung wieder aufzunehmen.	Toggle Mode 0 (0x0100) Toggle Mode 1 (0x0101)	Nach dem Kommunikationsverlust kann durch einen programmgesteuerten Wechsel des Toggle-Modus die Verbindung erneut aufgebaut werden. <ul style="list-style-type: none">▪ TOGGLE MODE 0 (0x100) gesetzt: Auf TOGGLE MODE 1 (0x101) setzen um die Verbindung wieder aufzunehmen.▪ TOGGLE MODE 1 (0x101) gesetzt: Auf TOGGLE MODE 0 (0x100) setzen um die Verbindung wieder aufzunehmen.	Disabled (0x8000)	safeethernet Kommunikation abgeschaltet.
			Befehl	Beschreibung							
			Autoconnect (0x0000)	Standardwert: Nach Verlust der safeethernet Kommunikation versucht die Steuerung im nächsten CPU-Zyklus, die Verbindung wieder aufzunehmen.							
Toggle Mode 0 (0x0100) Toggle Mode 1 (0x0101)	Nach dem Kommunikationsverlust kann durch einen programmgesteuerten Wechsel des Toggle-Modus die Verbindung erneut aufgebaut werden. <ul style="list-style-type: none">▪ TOGGLE MODE 0 (0x100) gesetzt: Auf TOGGLE MODE 1 (0x101) setzen um die Verbindung wieder aufzunehmen.▪ TOGGLE MODE 1 (0x101) gesetzt: Auf TOGGLE MODE 0 (0x100) setzen um die Verbindung wieder aufzunehmen.										
Disabled (0x8000)	safeethernet Kommunikation abgeschaltet.										
Verbindungszustand	UINT	R	Der Verbindungszustand wertet den Status der Kommunikation zwischen zwei Steuerungen im Anwenderprogramm aus.								
			<table><tr><th>Status/Wert</th><th>Beschreibung</th></tr><tr><td>Closed (0)</td><td>Verbindung ist geschlossen und es wird auch nicht versucht sie zu öffnen.</td></tr><tr><td>Try_open (1)</td><td>Es wird versucht, die Verbindung zu öffnen. Dieser Zustand gilt gleichermaßen für die aktive und auch für die passive Seite.</td></tr><tr><td>Connected (2)</td><td>Die Verbindung ist hergestellt und in Betrieb (aktive Zeitüberwachung und Datenaustausch)</td></tr></table>	Status/Wert	Beschreibung	Closed (0)	Verbindung ist geschlossen und es wird auch nicht versucht sie zu öffnen.	Try_open (1)	Es wird versucht, die Verbindung zu öffnen. Dieser Zustand gilt gleichermaßen für die aktive und auch für die passive Seite.	Connected (2)	Die Verbindung ist hergestellt und in Betrieb (aktive Zeitüberwachung und Datenaustausch)
			Status/Wert	Beschreibung							
			Closed (0)	Verbindung ist geschlossen und es wird auch nicht versucht sie zu öffnen.							
Try_open (1)	Es wird versucht, die Verbindung zu öffnen. Dieser Zustand gilt gleichermaßen für die aktive und auch für die passive Seite.										
Connected (2)	Die Verbindung ist hergestellt und in Betrieb (aktive Zeitüberwachung und Datenaustausch)										
Versions-Zustand	UINT	R	Reload-Versionszustand dieser safeethernet Verbindung. unknown: 0x0000 up to date: 0x0001 updated: 0x0002 outdated: 0x0003								
Wiederholungen	UDINT	R	Anzahl der Wiederholungen seit Reset der Statistik.								
Zeitstempel des letzten Fehlers des Red.-Kanal [ms]	UDINT	R	Millisekunden-Anteil des Zeitstempels (aktuelle Systemzeit).								
Zeitstempel des letzten Fehlers des Red.-Kanals [s]	UDINT	R	Sekunden-Anteil des Zeitstempels (aktuelle Systemzeit).								
Zeitstempel des letzten Fehlers [ms]	UDINT	R	Millisekunden-Anteil des Zeitstempels (aktuelle Systemzeit).								
Zeitstempel des letzten Fehlers [s]	UDINT	R	Sekunden-Anteil des Zeitstempels (aktuelle Systemzeit).								

Name	Datentyp	R/W	Beschreibung										
Zustand des Red.-Kanal	USINT	R	Aktueller Kanalzustand von Kanal 2. Der Kanalzustand ist der aktuelle Zustand des Kanal 2 zum Zeitpunkt (Seq-No X-1) beim Empfang einer Nachricht mit Seq-No X.										
			<table><tr><th>Status</th><th>Beschreibung</th></tr><tr><td>0</td><td>Keine Nachricht zum Zustand von Kanal 2.</td></tr><tr><td>1</td><td>Kanal 2 OK.</td></tr><tr><td>2</td><td>Letzte Nachricht war Fehlerhaft, aktuelle ist OK.</td></tr><tr><td>3</td><td>Fehler auf Kanal 2.</td></tr></table>	Status	Beschreibung	0	Keine Nachricht zum Zustand von Kanal 2.	1	Kanal 2 OK.	2	Letzte Nachricht war Fehlerhaft, aktuelle ist OK.	3	Fehler auf Kanal 2.
			Status	Beschreibung									
			0	Keine Nachricht zum Zustand von Kanal 2.									
			1	Kanal 2 OK.									
			2	Letzte Nachricht war Fehlerhaft, aktuelle ist OK.									
3	Fehler auf Kanal 2.												

Tabelle 12: Register Systemvariablen des safe**ethernet**-Editors

6 Alarm&Event Editor der Ressource

Der Alarm&Event Editor dient der Parametrierung der Alarme und Ereignisse der HIMax/HIMatrix Steuerung.

- Ereignisse sind Änderungen des Zustands von Anlage oder Steuerung, die mit einem Zeitstempel versehen sind.
- Alarme sind solche Ereignisse, die eine Erhöhung des Risikopotenzials signalisieren.

Damit der X-OPC Server über die **safeethernet** Verbindung Ereignisse und Alarme aus der Steuerung auslesen kann, muss der Parameter *A&E aktiv* aktiviert sein.

Das HIMA System zeichnet als Ereignisse die Zustandsänderungen zusammen mit dem Zeitpunkt ihres Auftretens auf. Der X-OPC Server kann die Ereignisse auf OPC Clients wie Leitsysteme übertragen, die die Ereignisse darstellen oder auswerten.

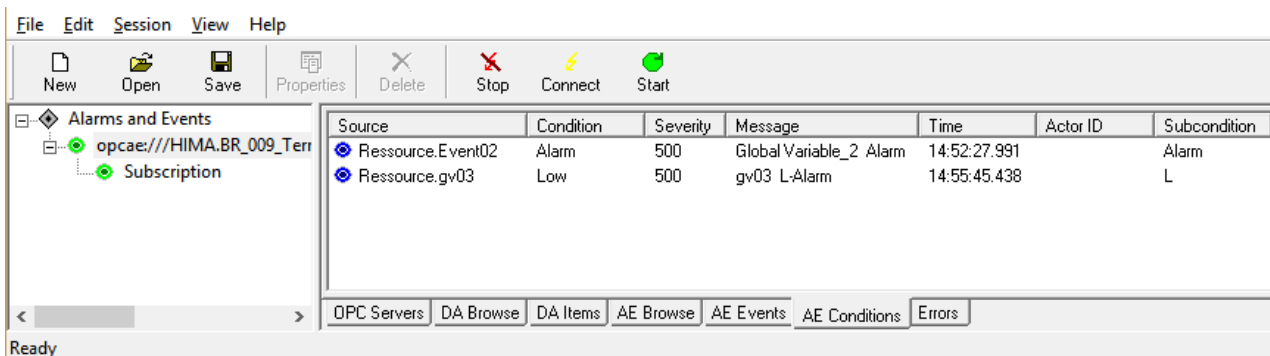


Bild 11: Anzeige der Alarm&Events in einem X-OPC Client

6.1 Alarm&Event Editor konfigurieren

Der Alarm&Event Editor beinhaltet die folgenden drei Register:

- Event-Definition BOOL
- Event-Definition Skalar
- Eigenschaften

Einen Alarm&Event Editor anlegen

1. Im Strukturbaum **Konfiguration, Ressource** selektieren.
2. Rechtsklick auf **Ressource** und im Kontextmenü **Neu, Alarm&Events** wählen.
 - ☒ Ein neues Objekt Alarm&Events wird hinzugefügt.

6.1.1 Register Event-Definition BOOL

- Änderungen von booleschen Variablen, z. B. von digitalen Eingängen.
- Alarm- und Normalzustand: Diese Werte können den Zuständen der Variablen beliebig zugeordnet werden.

Die Parameter der **booleschen** Ereignisse werden im Alarm&Event Editor der Ressource eingegeben, der die folgenden Spalten enthält:

Spalte	Beschreibung	Wertebereich
Name	Name der Ereignisdefinition Dies ist der Name der als <i>Source</i> im OPC Client erscheint.	Text
Globale Variable	Name der zugewiesenen globalen Variable (Eingefügt z. B. durch Drag&Drop)	
Datentyp	Datentyp der globalen Variable, nicht änderbar	BOOL
Event-Quelle	CPU Der Zeitstempel wird auf einem Prozessormodul gebildet. Dieses führt die Ereignisbildung komplett in jedem seiner Zyklen durch. E/A Der Zeitstempel wird auf einem geeigneten E/A-Modul gebildet (z. B. DI 32 04). Auto Es wird ein CPU Event und wenn vorhanden IO Events der E/A-Module gebildet. Bei E/A-Events wird der <i>Name</i> zusätzlich mit der Position als <i>Source</i> im OPC Client angezeigt. z. B. "Name_0_10_3" Standardwert: Auto	CPU, E/A, Auto
Alarm bei FALSE	Aktiviert Die Wertänderung TRUE->FALSE der globalen Variablen löst ein Ereignis aus Deaktiviert Die Wertänderung FALSE->TRUE der globalen Variablen löst ein Ereignis aus Standardwert: deaktiviert	Kontrollkästchen aktiviert, deaktiviert
Alarm Text	Text, der den Alarmzustand benennt	Text
Alarm-Priorität	Priorität des Alarmzustands Standardwert: 500	1...1000
Alarmbestätigung erforderlich	Aktiviert Bestätigung des Alarmzustandes durch den Bediener erforderlich (Quittierung) Deaktiviert Bestätigung des Alarmzustandes durch den Bediener nicht erforderlich Standardwert: deaktiviert	Kontrollkästchen aktiviert, deaktiviert
Return to Normal Text	Text, der den Alarmzustand benennt	Text
Return to Normal Severity	Priorität des Normalzustands	1...1000
Return to Normal Ack Required	Bestätigung des Normalzustandes durch den Bediener erforderlich (Quittierung) Standardwert: deaktiviert	Kontrollkästchen aktiviert, deaktiviert

Tabelle 13: Parameter für boolesche Ereignisse

6.1.2 Register Event-Definition Skalar

- Übergänge über Grenzwerte, die für eine skalare Variable definiert sind.
- Skalare Variable haben einen numerischen Datentyp, z. B. INT, REAL.
- Es sind zwei obere und zwei untere Grenzen möglich.
- Für die Grenzwerte muss gelten: Oberste Grenze \geq obere Grenze \geq Normalbereich \geq untere Grenze \geq unterste Grenze.
- Eine Hysterese kann in folgenden Fällen wirken:
 - Bei Unterschreitung einer oberen Grenze.
 - Bei Überschreitung einer unteren Grenze.

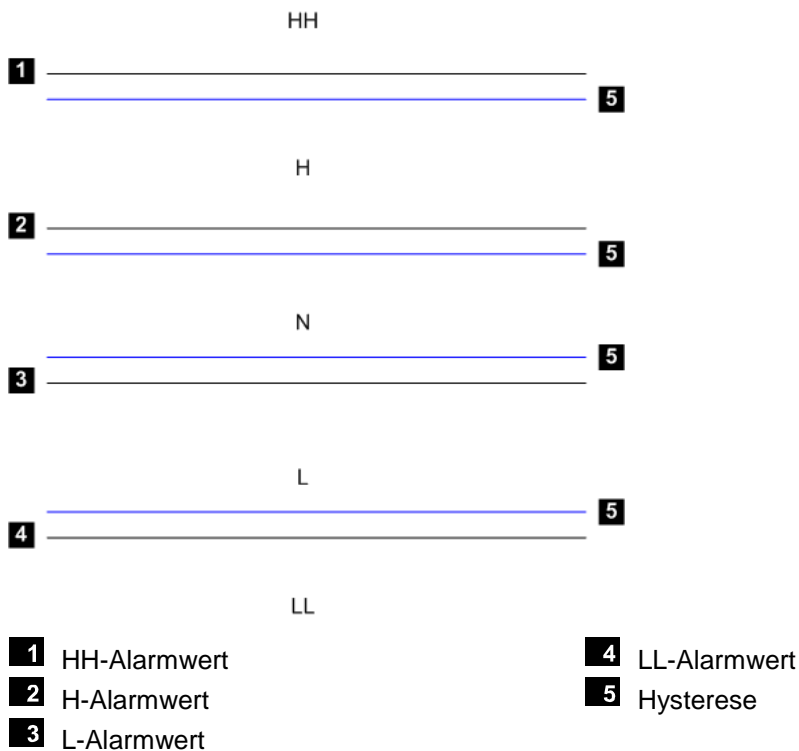


Bild 12: Fünf Bereiche eines skalaren Ereignisses

i

Die Angabe einer Hysterese vermeidet eine unnötig große Menge an Ereignissen, wenn die globale Variable stark um einen Grenzwert schwankt.

Die Parameter der **skalaren** Ereignisse werden im Alarm&Event Editor der Ressource eingegeben, der die folgenden Spalten enthält:

Spalte	Beschreibung	Wertebereich
Name	Name der Ereignisdefinition Dies ist der Name der als <i>Source</i> im OPC Client erscheint.	Text
Globale Variable	Name der zugewiesenen globalen Variable (z. B. eingefügt durch Drag&Drop)	
Datentyp	Datentyp der globalen Variable, nicht änderbar.	abhängig vom Typ der globalen Variablen
Event-Quelle	<p>CPU Der Zeitstempel wird auf einem Prozessormodul gebildet. Dieses führt die Ereignisbildung komplett in jedem seiner Zyklen durch.</p> <p>E/A Der Zeitstempel wird auf einem geeigneten E/A-Modul gebildet (z. B. AI 32 02).</p> <p>Auto Es wird ein CPU Event und wenn vorhanden IO Events der E/A-Module gebildet.</p> <p>Bei E/A-Events wird der <i>Name</i> zusätzlich mit der Position als <i>Source</i> im OPC Client angezeigt. Beispiel: "Name_0_10_3" Standardwert: Auto</p>	CPU, E/A, Auto
HH-Alarmtext	Text, der den Alarmzustand des obersten Grenzwerts benennt	Text
HH-Alarmwert	Oberster Grenzwert, der ein Ereignis auslöst. Bedingung: $(\text{HH-Alarmwert} - \text{Hysterese}) > \text{H-Alarmwert}$ oder $\text{HH-Alarmwert} = \text{H-Alarmwert}$	abhängig vom Typ der globalen Variablen
HH-Alarmpriorität	Priorität des obersten Grenzwerts Standardwert: 500	1...1000
HH-Alarmbestätigung erforderlich	<p>Aktiviert Bediener muss Überschreitung des obersten Grenzwerts bestätigen (Quittierung).</p> <p>Deaktiviert Bediener muss Überschreitung des obersten Grenzwerts nicht bestätigen.</p> <p>Standardwert: deaktiviert</p>	Kontrollkästchen aktiviert, deaktiviert
H-Alarmtext	Text, der den Alarmzustand des oberen Grenzwerts benennt	Text
H-Alarmwert	Oberer Grenzwert, der ein Ereignis auslöst. Bedingung: $(\text{H-Alarmwert} - \text{Hysterese}) > (\text{L-Alarmwert} + \text{Hysterese})$ oder $\text{H-Alarmwert} = \text{L-Alarmwert}$	abhängig vom Typ der globalen Variablen
H-Alarmpriorität	Priorität des oberen Grenzwerts Standardwert: 500	1...1000
H-Alarmbestätigung erforderlich	<p>Aktiviert Bediener muss Überschreitung des oberen Grenzwerts bestätigen (Quittierung).</p> <p>Deaktiviert Bediener muss Überschreitung des oberen Grenzwerts nicht bestätigen.</p> <p>Standardwert: deaktiviert</p>	Kontrollkästchen aktiviert, deaktiviert
Return to Normal Text	Text, der den Alarmzustand benennt	Text
Return to Normal Severity	Priorität des Normalzustands Standardwert: 500	1...1000
Return to Normal Ack Required	<p>Aktiviert Bediener muss den Normalzustand bestätigen (Quittierung).</p> <p>Deaktiviert Bediener muss den Normalzustand nicht bestätigen.</p> <p>Standardwert: deaktiviert</p>	Kontrollkästchen aktiviert, deaktiviert

Spalte	Beschreibung	Wertebereich
L-Alarmtext	Text, der den Alarmzustand des unteren Grenzwerts benennt	Text
L-Alarmwert	Unterer Grenzwert, der ein Ereignis auslöst. Bedingung: $(L\text{-Alarmwert} + \text{Hysterese}) < (H\text{-Alarmwert} - \text{Hysterese})$ oder $L\text{-Alarmwert} = H\text{-Alarmwert}$	abhängig vom Typ der globalen Variablen
L-Alarmpriorität	Priorität des unteren Grenzwerts. Standardwert: 1	1...1000
L-Alarmbestätigung erforderlich	Aktiviert Bediener muss Unterschreitung des unteren Grenzwerts bestätigen (Quittierung). Deaktiviert Bediener muss Unterschreitung des unteren Grenzwerts nicht bestätigen. Standardwert: deaktiviert	Kontrollkästchen aktiviert, deaktiviert
LL-Alarmtext	Text, der den Alarmzustand des untersten Grenzwerts benennt	Text
LL-Alarmwert	Untester Grenzwert, der ein Ereignis auslöst. Bedingung: $(LL\text{-Alarmwert} + \text{Hysterese}) < (L\text{-Alarmwert})$ oder $LL\text{-Alarmwert} = L\text{-Alarmwert}$	abhängig vom Typ der globalen Variablen
LL-Alarmpriorität	Priorität des untersten Grenzwerts. Standardwert: 1	1...1000
LL-Alarmbestätigung erforderlich	Aktiviert Bediener muss Unterschreitung des untersten Grenzwerts bestätigen (Quittierung). Deaktiviert Bediener muss Unterschreitung des untersten Grenzwerts nicht bestätigen. Standardwert: deaktiviert	Kontrollkästchen aktiviert, deaktiviert
Alarm-Hysterese	Die Hysterese verhindert ein ständiges Erzeugen von vielen Ereignissen, wenn der Prozesswert häufig um einen Grenzwert schwankt.	abhängig vom Typ der globalen Variablen

Tabelle 14: Parameter für skalare Ereignisse

6.1.3 Register Eigenschaften

Das Register **Eigenschaften** enthält die folgenden Parameter:

Bezeichnung	Beschreibung
Typ	Alarm&Events
Name	Name des Alarm&Event Editors
Alarm&Event ID	<p>Ein A&E Cookie ist ein eindeutiger 32-bit-Wert und wird für jeden einzelnen Alarm generiert.</p> <p>Ein A&E Cookie dient dazu, dass ein OPC Client einen Alarm eindeutig identifizieren kann. Auch die OPC Client-Server Interaktion (z. B. Ack.) funktioniert über A&E Cookie. Damit ein OPC Client einen Alarm von redundanten X-OPC Servern als identisch identifizieren kann, muss sowohl der Source-Name als auch der zugehörige A&E Cookie identisch sein.</p> <p>Nicht verwendet Der A&E Cookie berechnet sich wie bisher aus dem Namen und der Server-System-ID. Damit ist er wegen der nötigen Eindeutigkeit von IDs für redundante Server unterschiedlich.</p> <p>Alarm&Event ID Der A&E Cookie berechnet sich aus dem Namen und der Event-ID. Damit ist er über Server hinweg für ein Event aus einer Steuerung immer identisch. Wertebereich: 1...511 Standardwert: Nicht verwendet</p>

Tabelle 15: Standardwerte der Prioritäten

7 Erlaubte IP-Adressen Kombinationen des Masters

Allgemein gültige Regeln für die Vergabe von IP-Adressen und Subnet Mask müssen beachtet werden.

7.1 Verwendete Netzwerkports für Ethernet-Kommunikation

Alle im folgenden aufgeführten Ports sind Destination Ports.

UDP-Ports / Verwendung

- | | |
|------|--|
| 123 | SNTP (Zeitsynchronisation zwischen PES und Remote I/O, sowie externen Geräten) |
| 6010 | safeethernet und OPC
6010 ist der Port auf der HIMax/HIMatrix Steuerung.
Beim X-OPC Server ist dies der in SILworX konfigurierte HH-Port.
Für das PADT wird vom X-OPC Server der bei der Installation eingegebene PADT-Port genutzt. |
| 8000 | Programmierung und Bedienung mit SILworX |

8 Support

Bei Fragen zur Bedienung, oder zur Meldung von Programmfehlern und Verbesserungsvorschlägen stehen Ihnen verschiedene Möglichkeiten zur Auswahl:

Bereich	Webseite oder Telefon
News, Handbücher	Alle aktuellen Handbücher können über die E-Mail-Adresse documentation@hima.com angefragt werden.
Ansprechpartner: Vor-Ort-Services	https://www.hima.com/de/unternehmen/ansprechpartner-weltweit/
Technischer Support	https://www.hima.com/de/produkte-services/support/
Seminarangebote	https://www.hima.com/de/produkte-services/seminarangebot

Tabelle 16: HIMA Support

Anhang

Glossar

Begriff	Beschreibung
ARP	Address Resolution Protocol: Netzwerkprotokoll zur Zuordnung von Netzwerkadressen zu Hardware-Adressen
COM	Kommunikationsmodul
CPU	Prozessormodul
CRC	Cyclic Redundancy Check, Prüfsumme
EN	Europäische Normen
FB	Feldbus
FBS	Funktionsbausteinsprache
IEC	Internationale Normen für die Elektrotechnik
MAC-Adresse	Hardware-Adresse eines Netzwerkanschlusses (Media Access Control)
PADT	Programming and Debugging Tool (nach IEC 61131-3), PC mit SILworX
PELV	Protective Extra Low Voltage: Funktionskleinspannung mit sicherer Trennung
PES	Programmierbares Elektronisches System
Rack-ID	Identifikation eines Basisträgers (Nummer)
rückwirkungsfrei	Es seien zwei Eingangsschaltungen an dieselbe Quelle (z. B. Transmitter) angeschlossen. Dann wird eine Eingangsschaltung „rückwirkungsfrei“ genannt, wenn sie die Signale der anderen Eingangsschaltung nicht verfälscht.
SIL	Safety Integrity Level (nach IEC 61508)
SILworX	Programmiersoftware für HIMA Steuerungen
SRS	System.Rack.Slot
TMO	Timeout
WDZ	Watchdog-Zeit

Abbildungsverzeichnis

Bild 1:	Redundanter X-OPC Betrieb	15
Bild 2:	Installationsroutine des X-OPC Servers	16
Bild 3:	Installationsroutine des X-OPC Servers	16
Bild 4:	Einstellung manuell für die CLSID des zweiten X-OPC Servers	17
Bild 5:	Redundanter X-OPC Betrieb	19
Bild 6:	safeethernet Editor des OPC Server-Sets	20
Bild 7:	safeethernet Editor des OPC Server-Sets	21
Bild 8:	Detailansicht der safeethernet Verbindung	22
Bild 9:	Alarm&Event Editor	23
Bild 10:	Alarm&Event ID	23
Bild 11:	Anzeige der Alarm&Events in einem X-OPC Client	39
Bild 12:	Fünf Bereiche eines skalaren Ereignisses	41

Tabellenverzeichnis

Tabelle 1:	Zusätzlich geltende Handbücher	5
Tabelle 2:	Systemanforderung und Ausstattung des X-OPC Server	10
Tabelle 3:	Eigenschaften des X-OPC Server	12
Tabelle 4:	Eigenschaften der HIMA Steuerung für X-OPC Verbindung	13
Tabelle 5:	Erforderliche Aktionen bei Änderungen	14
Tabelle 6:	Eigenschaften	29
Tabelle 7:	Eigenschaften	30
Tabelle 8:	Edit	30
Tabelle 9:	Eigenschaften	31
Tabelle 10:	Partner	31
Tabelle 11:	Parameter safeethernet Protokoll	33
Tabelle 12:	Register Systemvariablen des safeethernet-Editors	38
Tabelle 13:	Parameter für boolesche Ereignisse	40
Tabelle 14:	Parameter für skalare Ereignisse	43
Tabelle 15:	Standardwerte der Prioritäten	43
Tabelle 16:	HIMA Support	45

HANDBUCH

X-OPC Server Version 5.2.1204

HI 801 479 D

Für weitere Informationen kontaktieren Sie:

HIMA Paul Hildebrandt GmbH

Albert-Bassermann-Str. 28

68782 Brühl, Germany

Telefon +49 6202 709-0

Fax +49 6202 709-107

E-Mail info@hima.com

Erfahren Sie online mehr über HIMA Lösungen:

 www.hima.com/de/



www.hima.com