



Handbuch

Kommunikation

Konfiguration in SILworX



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 2020, HIMA Paul Hildebrandt GmbH

Alle Rechte vorbehalten.

Kontakt

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
11.00	Neue Ausgabe zu SILworX V11	X	X
12.00	Aktualisierte Ausgabe zu SILworX V12 Geändert: Tabelle 2, HIMA OPC UA Server hinzugefügt.	X	X

Inhaltsverzeichnis

1	Einleitung	6
1.1	Aufbau und Gebrauch des Handbuchs	7
1.2	Zielgruppe	7
1.3	Darstellungskonventionen	8
1.3.1	Sicherheitshinweise	8
1.3.2	Gebrauchshinweise	9
1.4	Safety Lifecycle Services	10
2	Sicherheit	11
2.1	Bestimmungsgemäßer Einsatz	11
2.2	Restrisiken	11
2.3	Sicherheitsvorkehrungen	11
2.4	Notfallinformationen	11
2.5	Automation Security bei HIMA Systemen	11
3	Produktbeschreibung	13
3.1	HIMA System Mengengerüst für nicht-sicherheitsbezogene Protokolle	15
3.2	Registrierung und Aktivierung der Protokolle	16
3.3	Ethernet-Schnittstellen	18
3.3.1	HIMax Ethernet Schnittstellen	18
3.3.2	HIQuad X und HIMatrix Ethernet Schnittstellen	19
3.3.3	Konfiguration der Ethernet-Schnittstellen	19
3.3.4	Verwendete Netzwerk-Ports für Ethernet-Kommunikation	24
3.3.5	Switchports durch VLAN trennen	25
3.4	Feldbus-Schnittstellen	26
3.4.1	Registrierung und Aktivierung	26
3.4.2	Installation der Feldbus-Submodule	26
3.4.3	HIMax und HIMatrix Feldbus-Schnittstellen	28
3.4.4	HIQuad X F-COM 01 Feldbus-Schnittstellen	31
3.5	Technische Eigenschaften der RS-485-Übertragung	34
3.6	RS485 Bus-Topologie	35
3.6.1	Klemmenbelegung H 7506	36
3.6.2	Busanschluss und Busabschluss	36
3.7	Anforderungen an die Kommunikationskabel	37
3.7.1	Patchkabel	37
3.7.2	CAN Kabel	37
3.7.3	RS485 (RS422, RS232, SSI) Kabel	37
3.7.4	PROFINET Kabel	37
3.7.5	PROFIBUS DP Kabel	37
4	safeethernet	38
4.1	Allgemeines zu safeethernet	38
4.2	Benutzerauflagen für safeethernet in einem störungsbehafteten Netzwerk	41
4.3	HIMA System Mengengerüst für safeethernet	42
4.4	Konfiguration einer redundanten safeethernet Verbindung	44
4.4.1	safeethernet Verbindung erstellen	44
4.4.2	Konfiguration im safeethernet Verbindungseditor	45

4.4.3	Prüfung der safeethernet Kommunikation	46
4.5	safeethernet-Verbindungsübersicht	47
4.6	Verbindungs-Editor einer safeethernet Verbindung	49
4.6.1	Register: <i>Ressource A</i> <-> <i>Ressource B</i>	49
4.6.2	Register: <i>Ressource A</i>	49
4.6.3	Register: <i>Ressource B</i>	49
4.7	Netzwerkstrukturen für safeethernet Verschaltungen	54
4.7.1	Mono safeethernet Verbindung (Kanal 1)	54
4.7.2	Redundante safeethernet Verbindung (Kanal 1 und Kanal 2)	55
4.8	safeethernet Parameter	57
4.8.1	Berechnung einer geeigneten Watchdog-Zeit (max. Zykluszeit)	57
4.8.2	Receive Timeout	57
4.8.3	ResponseTime	58
4.8.4	Sync/Async	58
4.8.5	ResendTMO	59
4.8.6	Acknowledge Timeout	59
4.8.7	Production Rate	59
4.8.8	Speicher	60
4.9	Maximale Reaktionszeit für safeethernet	61
4.9.1	Maximale Reaktionszeit zweier HIMax Steuerungen	62
4.9.2	Maximale Reaktionszeit zweier HIQuad X Steuerungen	62
4.9.3	Maximale Reaktionszeit einer HIMax mit einer HIMatrix Steuerung	63
4.9.4	Maximale Reaktionszeit einer HIQuad X mit einer HIMatrix Steuerung	63
4.9.5	Maximale Reaktionszeit einer HIMax mit zwei HIMatrix Steuerungen oder Remote I/Os	64
4.9.6	Maximale Reaktionszeit einer HIMatrix mit zwei HIMax Steuerungen	65
4.9.7	Maximale Reaktionszeit zweier HIMatrix Steuerungen	65
4.9.8	Maximale Reaktionszeit einer HIMatrix Steuerung mit zwei Remote I/Os	66
4.10	safeethernet Profile	67
4.10.1	Profil I (Fast & Cleanroom)	68
4.10.2	Profil II (Fast & Noisy)	68
4.10.3	Profil III (Medium & Cleanroom)	69
4.10.4	Profil IV (Medium & Noisy)	69
4.10.5	Profil V (Slow & Cleanroom)	70
4.10.6	Profil VI (Slow & Noisy)	70
4.11	Control Panel (safeethernet)	71
4.11.1	Anzeigefeld (safeethernet Verbindung)	71
4.12	safeethernet Reload	73
4.12.1	Voraussetzungen	73
4.12.2	Technisches Konzept	73
4.12.3	Einzuhaltende Vorgehensweise	74
4.12.4	Integrierte Schutzmechanismen	77
4.12.5	safeethernet Reload Zustand	78
4.12.6	Maximale Anzahl safeethernet Verbindungen während des Reloads	78
4.12.7	safeethernet Verbindung über Kommunikationsmodul	79
4.12.8	Änderungen der safeethernet Konfiguration	79
4.13	Projektübergreifende Kommunikation	80
4.13.1	Konfiguration in SILworX	81
4.13.2	Konfiguration A im Projekt B	84
5	SNTP-Protokoll	87

5.1	Benötigte Ausstattung und Systemanforderung	87
5.2	SNTP-Client	87
5.2.1	SNTP-Server Info	89
5.3	SNTP-Server	90
5.4	Konfiguration der Zeitsynchronisation über SNTP	91
5.4.1	Anlegen einer IP-Verbindung zu einem Netzwerkzeitserver	91
5.4.2	SNTP Zeitsynchronisation einer Remote I/O durch eine HIMA Ressource	92
6	HART	93
6.1	Systemanforderung	93
6.1.1	Eigenschaften HART-Protokoll	93
6.2	HART-Kommunikation für sicherheitsbezogene Anwendungen	94
6.2.1	Sicherheitsfunktion	94
6.3	Konfiguration einer HART-IP-Protokollinstanz	95
6.3.1	HART OPC Server oder FDT/DTM Asset-Management-System	95
6.3.2	HART-Feldgeräte	96
6.3.3	X-HART-Modul, X-COM-Modul und analoge E/A-Module konfigurieren	96
6.3.4	Konfiguration der HART-IP Protokollinstanz	98
6.4	Online-Ansicht des X-COM-Moduls	99
6.4.1	Anzeigefeld (HART-Protokoll)	99
6.4.2	Online-Ansicht der Geräteliste	100
7	Allgemein	102
7.1	Maximale Kommunikationszeitscheibe	102
7.1.1	Ermitteln der maximalen Dauer der Kommunikationszeitscheibe	102
7.2	Lastbegrenzung	102
7.3	Konfiguration der Funktionsbausteine	103
7.3.1	Beschaffung der Funktionsbausteinbibliotheken	103
7.3.2	Konfiguration der Funktionsbausteine im Anwenderprogramm	103
7.3.3	Konfiguration der Funktionsbausteine im Strukturbaum von SILworX	104
	Anhang	105
	Glossar	105
	Abbildungsverzeichnis	106
	Tabellenverzeichnis	107
	Index	108

1 Einleitung

Das Kommunikationshandbuch für sicherheitsbezogene HIMA Systeme bietet einen Überblick der zur Verfügung stehenden Protokolle und den physikalischen Eigenschaften der Ethernet- und Feldbus-Schnittstellen. Für Protokolle, die nicht in diesem Handbuch beschrieben werden, gibt es separate Handbücher, siehe Tabelle 2.

Voraussetzung für die risikolose Installation und Inbetriebnahme sowie für die Sicherheit bei Betrieb und Instandhaltung des Systems sind:

- Die Kenntnis von Vorschriften.
- Die technisch einwandfreie Umsetzung der in diesem Handbuch enthaltenen Sicherheitshinweise durch qualifiziertes Personal.

Durch Störungen oder Beeinträchtigungen von Sicherheitsfunktionen können in folgenden Fällen schwere Personen-, Sach- oder Umweltschäden eintreten, für die HIMA keine Haftung übernehmen kann:

- Bei nicht qualifizierten Eingriffen in die Systeme.
- Bei Abschalten oder Umgehen (Bypass) von Sicherheitsfunktionen.
- Bei Nichtbeachtung von Hinweisen dieses Handbuchs.

HIMA entwickelt, fertigt und prüft die HIMA Systeme unter Beachtung der einschlägigen Sicherheitsnormen. Die Verwendung der Systeme ist nur zulässig, wenn die folgenden Voraussetzungen erfüllt sind:

- Die in den Beschreibungen vorgesehenen Einsatzfälle wurden eingehalten.
- Die spezifizierten Umgebungsbedingungen wurden eingehalten.

1.1 Aufbau und Gebrauch des Handbuchs

Das Handbuch enthält die folgenden Hauptkapitel:

- Einleitung
- Sicherheit
- Produktbeschreibung
- **safeethernet**
- SNTP
- HART
- Allgemein

Zusätzlich sind die folgenden Dokumente zu beachten:

Name	Inhalt	Dokumenten-Nr.
HIMax Systemhandbuch	Hardware-Beschreibung HIMax System	HI 801 000 D
HIMax Sicherheitshandbuch	Sicherheitsfunktionen HIMax Systems	HI 801 002 D
HIMatrix Sicherheitshandbuch	Sicherheitsfunktionen 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 F 60	HI 800 190 D
HIQuad X Systemhandbuch	Hardware-Beschreibung HIQuad X System	HI 803 210 D
HIQuad X Sicherheitshandbuch	Sicherheitsfunktionen HIQuad X System	HI 803 208 D
Automation Security Handbuch	Beschreibung von Automation Security Aspekten bei HIMA Systemen	HI 801 372 D
SILworX Erste Schritte	Einführung in SILworX	HI 801 102 D

Tabelle 1: Zusätzlich geltende Handbücher

Alle aktuellen Handbücher können über die E-Mail-Adresse documentation@hima.com angefragt werden. Für registrierte Kunden stellt HIMA die Dokumentationen im Download-Bereich <https://www.hima.com/de/downloads/> zur Verfügung.

1.2 Zielgruppe

Dieses Dokument wendet sich an Planer, Projektoren, Programmierer und Personen, die zur Inbetriebnahme, zur Wartung und zum Betreiben von Automatisierungsanlagen 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.
<code>Courier</code>	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.

1.4 Safety Lifecycle Services

HIMA unterstützt Sie in allen Phasen des Sicherheitslebenszyklus der Anlage: Von der Planung, der Projektierung, über die Inbetriebnahme, bis zur Aufrechterhaltung der Sicherheit.

Für Informationen und Fragen zu unseren Produkten, zu Funktionaler Sicherheit und zu Automation Security stehen Ihnen die Experten des HIMA Support zur Verfügung.

Für die geforderte Qualifizierung gemäß Sicherheitsstandards, führt HIMA produkt- oder kundenspezifische Seminare in eigenen Trainingszentren, oder bei Ihnen vor Ort durch. Das aktuelle Seminarangebot zu Funktionaler Sicherheit, Automation Security und zu HIMA Produkten finden Sie auf der HIMA Webseite.

Safety Lifecycle Services:

Onsite+ / Vor-Ort-Engineering	In enger Abstimmung mit Ihnen führt HIMA vor Ort Änderungen oder Erweiterungen durch.
Startup+ / Vorbeugende Wartung	HIMA ist verantwortlich für die Planung und Durchführung der vorbeugenden Wartung. Wartungsarbeiten erfolgen gemäß der Herstellervorgabe und werden für den Kunden dokumentiert.
Lifecycle+ / Lifecycle-Management	Im Rahmen des Lifecycle-Managements analysiert HIMA den aktuellen Status aller installierten Systeme und erstellt konkrete Empfehlungen zu Wartung, Upgrade und Migration.
Hotline+ / 24-h-Hotline	HIMA Sicherheitsingenieure stehen Ihnen für Problemlösung rund um die Uhr telefonisch zur Verfügung.
Standby+ / 24-h-Rufbereitschaft	Fehler, die nicht telefonisch gelöst werden können, werden von HIMA Spezialisten innerhalb vertraglich festgelegter Zeitfenster bearbeitet.
Logistic+/ 24-h-Ersatzteilservice	HIMA hält notwendige Ersatzteile vor und garantiert eine schnelle und langfristige Verfügbarkeit.

Ansprechpartner:

Safety Lifecycle Services	https://www.hima.com/de/unternehmen/ansprechpartner-weltweit/
Technischer Support	https://www.hima.com/de/produkte-services/support/
Seminarangebot	https://www.hima.com/de/produkte-services/seminarangebot/

2 Sicherheit

Sicherheitsinformationen, Hinweise und Anweisungen in diesem Dokument unbedingt lesen. Das Produkt nur unter Beachtung aller Richtlinien und Sicherheitsrichtlinien einsetzen.

Dieses Produkt wird mit SELV oder PELV betrieben. Vom Produkt selbst geht kein Risiko aus. Einsatz im Ex-Bereich nur mit zusätzlichen Maßnahmen erlaubt.

2.1 Bestimmungsgemäßer Einsatz

Für den Einsatz von HIMA Systemen sind die jeweiligen Bedingungen einzuhalten, siehe zusätzlich geltende Handbücher, siehe 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 Automation Security bei HIMA Systemen

Automation Security hat die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Daten. In Bezug auf Automation Security muss von gezielten Angriffen ausgegangen werden. Insbesondere an Schnittstellen, wie sie in diesem Handbuch beschrieben werden, ist von möglichen Angriffen auszugehen.

WARNUNG



Personenschaden durch unbefugte Manipulation an der Steuerung möglich!

Die Steuerung ist gegen unbefugte Zugriffe zu schützen!

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

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 Netzwerkläne 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.

Weitere Einzelheiten siehe HIMA Automation Security Handbuch HI 801 372 D.

3 Produktbeschreibung

Mit den bereitgestellten Protokollen können HIMA Systeme untereinander und mit Steuerungen anderer Hersteller verbunden werden. Die Konfiguration dieser Protokolle wird in dem Programmierwerkzeug SILworX durchgeführt.

Für eine optimale Integration der HIMA Systeme mit Feldgeräten und Leitsystemen stehen herstellerübergreifende Standardprotokolle zur Verfügung. Hierfür finden sowohl Ethernet als auch Feldbus-Protokolle Verwendung. Die Standardprotokolle sind rückwirkungsfrei auf das sichere Prozessorsystem der HIMA Systeme.

Die folgenden Protokolle stehen für die HIMA Systeme zur Verfügung:

Protokoll	SIL ¹⁾	HIMax	HIQuad X	HIMatrix	Kapitel oder Handbuch
safeethernet	4	X	X	X	Kapitel 4
SNTP	-	X	X	X	Kapitel 5
HART-Protokoll	-	X	--	--	Kapitel 6
HIMA X-OPC Server ²⁾	-	X	X	X	HI 801 479 D
HIMA OPC UA Server	-	X	X	X	HI 801 548 D
ISOfast	3	--	--	X	HI 801 464 D
Send/Receive TCP	-	X	--	X	HI 801 516 D
HIPRO-S V2	3	X	X	X	HI 800 722 D
PROFINET IO Controller	-	X	--	X	HI 801 514 D
PROFINET IO Device	-	X	--	X	
PROFIsafe F-Host	3	X	--	X	
PROFIsafe F-Device	3	X	--	X	
PROFIBUS DP Master	-	X	--	X	
PROFIBUS DP Slave	-	X	X	X	
Modbus Master	-	X	X	X	HI 801 515 D
Modbus Slave Set	-	X	X	X	HI 801 474 D
Modbus Slave Set V2	-	X	X	X	
Synchronous Serial Interface (SSI)	-	X	--	X	
ComUserTask ³⁾	-	X	X	X	HI 801 517 D

¹⁾ --: kein SIL.
3: SIL 3 gemäß IEC 61508-2:2010, IEC 61784-3:2019.
4: SIL 4 gemäß IEC 61508-2:2010, IEC 61784-3:2019 und EN 50159:2010, siehe Kapitel 4.

²⁾ Der HIMA X-OPC Server wird auf einem Host-PC installiert und dient als Übertragungsschnittstelle zwischen bis zu 255 HIMA Steuerungen und Fremdsystemen, die über eine OPC Schnittstelle verfügen.

³⁾ In der ComUserTask kann ein C-Programm des Anwenders mit Anbindung an diverse Kommunikationsschnittstellen des COM-Moduls implementiert werden.

Tabelle 2: Verfügbare Protokolle für die HIMA Systeme

Die sicherheitsbezogenen Protokolle werden auf dem jeweiligen Prozessormodul des HIMA Systems betrieben. Die Prozessdatenmenge wird durch den zur Verfügung stehenden freien Speicher für globale Prozessdaten auf dem Prozessormodul begrenzt:

- HIMax, HIMatrix, HIQuad X = 512 kByte.

1

Der Speicher für globale Prozessdaten wird für alle Variablen des HIMA Systems (z. B. Protokoll-, Anwenderprogramm- und Systemvariablen) verwendet. Wird dieser Speicher überschritten, so lehnt das HIMA System eine Konfiguration beim Download/Reload ab und informiert den Anwender im SILworX Logbuch.

Eine Reihe von Standard Protokollen erlaubt nur eine nicht-sicherheitsbezogene Übertragung von Daten. Diese nicht-sicheren Daten dürfen in Verantwortung des Anwenders nur dann für

sicherheitstechnische Funktionen verwendet werden, wenn ausreichende Zusatzmaßnahmen ergriffen wurden.

⚠ WARNUNG



Verwendung von unsicheren Importdaten in Sicherheitstechnischen Funktionen!


Personenschaden durch Verwendung unsicherer Importdaten möglich!

**Aus nicht sicheren Quellen importierte Daten nicht für die
Sicherheitstechnischen Funktionen des Anwenderprogramms verwenden!**

3.1 HIMA System Mengengerüst für nicht-sicherheitsbezogene Protokolle

Die nicht-sicherheitsbezogene Protokolle (NSIP), werden auf dem jeweiligen Kommunikationsmodul (COM-Modul) der HIMA Systeme betrieben.

Eigenschaften	HIMax	HIQuad X	Beschreibung
Systemansicht			Bilder sind exemplarisch für die jeweilige Systemfamilie. Zu sehen sind eine HIMax und eine HIQuad X H51X.
Kommunikationsmodule pro HIMA Steuerung	Bei X-CPU 01: 1 ... 20 X-COM 01 Bei X-CPU 31: 1 ... 4 X-COM 01	H51X: 1 ... 10 F-COM 01 H41X: 1 ... 2 F-COM 01	NSIP werden auf den Kommunikationsmodulen ausgeführt.
Ethernet-Schnittstellen und Feldbus-Schnittstellen	Auf der X-COM 01	Auf der F-COM 01	Weitere Informationen, siehe Tabelle 5.
Maximale Anzahl NSIP	<ul style="list-style-type: none"> 20¹⁾ pro HIMax Steuerung. 6¹⁾ pro X-COM-Modul. 	<ul style="list-style-type: none"> 20¹⁾ pro HIQuad X 5¹⁾ pro F-COM 01 	Verfügbare NSIP, siehe Tabelle 2.
Prozessdatenmenge ¹⁾²⁾ aller NSIP einer Steuerung	128 kB senden 128 kB empfangen	64 kB senden 64 kB empfangen	Die maximale Prozessdatenmenge der Steuerung darf nicht überschritten werden. In diesem Fall wird die Parametrierung der Steuerung beim Laden abgelehnt.

Eigenschaften	HIMatrix	Beschreibung
Systemansicht		Bild ist exemplarisch für die jeweilige Systemfamilie. Zu sehen ist eine F30.
Kommunikationsmodule pro HIMA Steuerung	Integriertes Kommunikationsmodul	NSIP werden auf den Kommunikationsmodulen ausgeführt.
Ethernet-Schnittstellen und Feldbus-Schnittstellen	Auf der Steuerung.	Weitere Informationen, siehe Tabelle 5.
Maximale Anzahl NSIP	6 ¹⁾	Verfügbare NSIP, siehe Tabelle 2.
Prozessdatenmenge ¹⁾²⁾ aller NSIP einer Steuerung	64 kB senden 64 kB empfangen	Die maximale Prozessdatenmenge der Steuerung darf nicht überschritten werden. In diesem Fall wird die Parametrierung der Steuerung beim Laden abgelehnt.

¹⁾ X-OPC Server, SNTP-Client und SNTP-Server gehen in diese Rechnung nicht mit ein ²⁾ Die Prozessdatenmenge der nicht-sicherheitsbezogenen Protokolle (NSIP) enthält die ausgetauschten Daten und die Systemvariablen der nicht-sicherheitsbezogenen Protokolle, sowie die von PROFIsafe.		
--	--	--

Tabelle 3: HIMA System Mengengerüst für nicht-sicherheitsbezogene Protokolle

3.2 Registrierung und Aktivierung der Protokolle

Die folgenden Protokolle sind für HIMA Systeme verfügbar und können wie folgt aktiviert werden:

Protokoll	Schnittstellen	HIMax	HIQuad X	HIMatrix
HIMA safeethernet	Ethernet	I	I	I
SNTP	Ethernet	I	I	I
HART-Protokoll	Ethernet	I	--	--
HIMA X-OPC Server (läuft auf Host-PC)	Ethernet	II	II	II
HIMA OPC UA Server	Ethernet	II	II	II
ISOfast	Ethernet	--	--	II
Send/Receive TCP	Ethernet	II	--	II
HIPRO-S V2	Ethernet	II	II	II
PROFINET IO Controller	Ethernet	II	--	II
PROFINET IO Device	Ethernet	II	--	II
PROFIsafe F-Host ¹⁾	Ethernet	II	--	II
PROFIsafe F-Device ¹⁾	Ethernet	II	--	II
PROFIBUS DP Master	Feldbus	III	--	III
PROFIBUS DP Slave	Feldbus	III	II	III
Modbus Master Eth	Ethernet	II	II	II
Modbus Slave Eth	Ethernet	II	II	II
Modbus Master RS485	Feldbus	IV	II	IV
Modbus Slave RS485	Feldbus	IV	II	IV
Synchronous Serial Interface (SSI)	Feldbus	IV	--	IV
ComUserTask	Ethernet, Feldbus	IV	II	IV
I Diese Protokolle sind standardmäßig freigeschaltet. II Für diese Protokolle muss eine Lizenz (Software-Freischaltcode) erworben werden. III Für diese Protokolle erfolgt die Freischaltung mit dem Einbau eines Feldbus-Submoduls. IV Für diese Protokolle muss eine Lizenz (Software-Freischaltcode) und gegebenenfalls das entsprechende Feldbus-Submodul erworben werden.				
¹⁾ Zusätzliche PROFINET Lizenz nötig				

Tabelle 4: Registrierung und Aktivierung der Protokolle

Der Software-Freischaltcode mit den benötigten Lizenzen wird auf der HIMA Webseite mit der System-ID der Steuerung generiert. Dazu den Anweisungen auf der HIMA Webseite folgen www.hima.com-> *Produkte & Services*-> *Produkt-Registrierung*-> *Optionen SILworX*.

i

Die Lizenz ist untrennbar mit der System-ID verbunden. Eine Lizenz kann nur einmalig für eine bestimmte System-ID genutzt werden. Deshalb sollte die Freischaltung erst durchgeführt werden, wenn die System-ID eindeutig feststeht.

Ein Software-Freischaltcode kann maximal 32 Lizenzen enthalten. Es können auch mehrere Freischaltcodes in der Lizenzverwaltung eingetragen werden. In eine Steuerung können maximal 64 Lizenzen geladen werden.

i

Wird auf einer COM ein Modbus Master RS485 über mehrere Schnittstellen betrieben, so handelt es sich intern trotzdem nur um eine Instanz des Modbus Masters. Somit wird lediglich eine Lizenz benötigt.

Den Software-Freischaltcode in SILworX eintragen

1. Im Strukturbaum **Konfiguration, Ressource, Lizenzverwaltung** wählen.
2. Rechtsklick auf **Lizenzverwaltung** und im Kontextmenü **Neu, Lizenzschlüssel** wählen.
☒ Der Lizenzschlüssel wird neu hinzugefügt.
3. Rechtsklick auf **Lizenzschlüssel** und im Kontextmenü **Eigenschaften** wählen.
4. Im Feld **Freischaltcode** den generierten Software-Freischaltcode eintragen.

i

Rechtzeitig die Lizenz bestellen!

Alle lizenzpflichtigen Funktionalitäten (z. B. Protokolle) können ohne Lizenz für 5000 Betriebsstunden getestet werden.

Beim Betrieb von Funktionalitäten ohne gültige Lizenz leuchtet die Error-LED (bei HIMax/HIMatrix und HIQuad X).

Nach Ablauf der 5000 Betriebsstunden läuft die Funktionalität (z. B. Protokolle) weiter, bis die Steuerung gestoppt wird. Danach lässt sich das Anwenderprogramm ohne gültige Lizenz für die projektierten Funktionalitäten nicht mehr starten (fehlerhafte Konfiguration).

3.3 Ethernet-Schnittstellen

Die Kommunikation mit externen Systemen und die Programmierung kann über Ethernet-Schnittstellen der CPU und der COM der HIMA Systeme erfolgen. Die Ethernet-Schnittstellen können mehrere Protokolle simultan verarbeiten.

Davon ausgenommen sind Systembusschnittstellen (der Module X-SB 01, X-CPU 31 und F-IOP 01). Die Verwendung dieser Schnittstellen ist in dem jeweiligen Systemhandbuch beschrieben.

Jedes CPU- und COM-Modul hat eine frei konfigurierbare IPv4-Adresse und einen Ethernet-Switch.

Der Ethernet-Switch baut eine gezielte Verbindung zwischen zwei Kommunikationspartnern für die Übertragung von Daten auf. Das verhindert Kollisionen und entlastet das Netzwerk.

Zur gezielten Weiterleitung der Daten wird eine MAC-/IP Adressen Zuordnungstabelle (ARP-Cache) angelegt und MAC-Adressen bestimmten IP-Adressen zugeordnet. Datenpakete werden jetzt nur noch an die IP-Adressen weitergeleitet, die im ARP-Cache gelistet sind.

i

Austausch eines CPU- oder COM-Moduls mit gleicher IP-Adresse.

Wird ein Gerät ausgetauscht, für welches *ARP Aging Time* = 5 Minuten und *MAC-Learning* = Konservativ eingestellt wurde, so übernimmt der Kommunikationspartner erst nach minimal 5 Minuten bis maximal 10 Minuten die neue MAC-Adresse. In dieser Zeit ist keine Kommunikation über das getauschte Gerät möglich.

Neben der einstellbaren ARP Aging Time muss mindestens die nicht änderbare MAC Aging Time des Switch (ca. 10 Sekunden) abgewartet werden, bis wieder eine Kommunikation über das getauschte Gerät möglich ist.

3.3.1 HIMax Ethernet Schnittstellen

Die folgende Tabelle zeigt die HIMax Ethernet Schnittstellen für die Kommunikation mit externen Systemen:

Eigenschaft	HIMax X-CPU 01	HIMax X-CPU 31	HIMax X-COM 01
Ports	4	2 für Protokolle 2 für Systembus UP/DOWN	4
Übertragungsstandard	10/100/1000BASE-T, Halb- und Vollduplex	10/100BASE-T, Halb- und Vollduplex	
Auto Negotiation	Ja		
Auto-Crossover	Ja		
Anschlussbuchse	RJ 45		
IP-Adresse	Frei Konfigurierbar ¹⁾		
Subnet Mask	Frei Konfigurierbar ¹⁾		
Unterstützte Protokolle	safe ethernet , X-OPC (DA & A+E), HIPRO-S V2 Programmiergerät (PADT), SNTP		
	--	--	Standardprotokolle ²⁾

¹⁾ Allgemein gültige Regeln für die Vergabe von IP-Adressen und Subnet Mask müssen beachtet werden.

²⁾ Als Standardprotokolle werden in diesem Handbuch Protokolle bezeichnet, die zur Anbindung von Fremdsystemen dienen.

Tabelle 5: HIMax Ethernet Schnittstellen

3.3.2 HIQuad X und HIMatrix Ethernet Schnittstellen

Die folgende Tabelle zeigt die HIQuad X und HIMatrix Ethernet Schnittstellen für die Kommunikation mit externen Systemen:

Eigenschaft	HIQuad X F-CPU 01	HIQuad X F-COM 01	HIMatrix Steuerung
Ports	2	2	4
Übertragungsstandard	10BASE-T/ 100BASE-Tx, Halb- und Vollduplex		
Auto Negotiation	Ja		
Auto-Crossover	Ja		
Anschlussbuchse	RJ 45		
IP-Adresse	Frei Konfigurierbar ¹⁾		
Subnet Mask	Frei Konfigurierbar ¹⁾		
Unterstützte Protokolle	safeethernet, X-OPC (DA & A+E), HIPRO-S V2 Programmiergerät (PADT), SNTP		
	--	Standardprotokolle ²⁾	Standardprotokolle ²⁾
¹⁾ Allgemein gültige Regeln für die Vergabe von IP-Adressen und Subnet Mask müssen beachtet werden.			
²⁾ Als Standardprotokolle werden in diesem Handbuch Protokolle bezeichnet, die zur Anbindung von Fremdsystemen dienen.			

Tabelle 6: HIQuad X und HIMatrix Ethernet Schnittstellen

3.3.3 Konfiguration der Ethernet-Schnittstellen

Die Konfiguration der Ethernet-Schnittstellen erfolgt in SILworX über die Detailansicht des CPU- oder COM-Moduls.

Für HIMA Systeme sind die Standardwerte der Parameter *Speed Modus* und *Flow-Control Modus* auf *AutoNeg* eingestellt.



Kommunikationsverlust!

Bei einer ungünstigen Einstellung der Ethernet-Parameter ist das Gerät nicht mehr erreichbar. Reset des Geräts durchführen!

Detailansicht des CPU-/COM-Moduls öffnen

1. Im Strukturbaum **Konfiguration, Ressource, Hardware** selektieren.
2. Rechtsklick und im Kontextmenü **Edit** wählen, um den Hardware Editor zu öffnen.
3. Rechtsklick auf das **CPU-/COM-Modul** und im Kontextmenü **Detailansicht** wählen, um die Detailansicht zu öffnen.



Die Einträge in den Eigenschaften der CPU-/COM-Module müssen mit dem Anwenderprogramm neu kompiliert und in die Steuerung übertragen werden, damit sie für die Kommunikation des HIMA Systems wirksam werden.

3.3.3.1 Register: Modul

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

Bezeichnung	Beschreibung
Name	Name des Moduls.
Max. μ P-Budget für HH-Protokoll aktivieren	<ul style="list-style-type: none"> Aktiviert: Limit der CPU-Last aus dem Feld <i>Max. μP-Budget für HH-Protokoll [%]</i> übernehmen. Deaktiviert: Kein Limit der CPU-Last, für safeethernet verwenden.
Max. μ P-Budget für HH-Protokoll [%]	<p>Maximale CPU-Last des Moduls, welche bei der Abarbeitung des safeethernet Protokolls produziert werden darf.</p> <hr/> <p>i Die Maximale Last muss unter allen verwendeten Protokollen aufgeteilt werden, welche dieses Kommunikationsmodul benutzen.</p> <hr/>
Codegenerierung	<p>Dieser Parameter ist nur für HIMax und HIMatrix Systeme einstellbar, da HIQuad X erst ab V10 verfügbar.</p> <p>vor V6 Kompatible Einstellung für bestehende Projekte.</p> <p>ab V6 Empfohlene Einstellung für neue Projekte, insbesondere wenn safeethernet Verbindungen über dieses Kommunikationsmodul geleitet werden. Änderungen an der safeethernet Verbindung können per Reload geladen werden.</p>
IP-Adresse	IP-Adresse der Ethernet-Schnittstelle Standardwert: 192.168.0.99
Subnet-Mask	32-Bit-Adressmaske zur Unterteilung einer IP-Adresse in Netzwerk- und Host-Adresse.
Standard-Schnittstelle	Aktiviert: Schnittstelle wird als Standardschnittstelle für den System-Login verwendet. Standardeinstellung: Deaktiviert
Default-Gateway	IP-Adresse des Default Gateway Standardwert: 0.0.0.0
ARP Aging Time [s]	<p>Ein CPU- oder COM-Modul speichert die MAC-Adressen seiner Kommunikationspartner in einer MAC-/IP Adresse Zuordnungstabelle (ARP-Cache). Die MAC-Adresse im ARP-Cache bleibt erhalten, wenn während einer Zeitspanne von 1x ... 2x <i>ARP Aging Time</i> Nachrichten vom Kommunikationspartner eintreffen. Die MAC-Adresse wird aus dem ARP-Cache gelöscht, wenn während einer Zeitspanne von 1x ... 2x <i>ARP Aging Time</i> keine Nachrichten vom Kommunikationspartner eintreffen.</p> <p>Der typische Wert für die <i>ARP Aging Time</i> in einem lokalen Netzwerk ist 5 ... 300 s. Der Inhalt des ARP-Cache kann vom Anwender nicht ausgelesen werden. Wertebereich: 1 ... 3600 s Standardwert: 60 s</p> <p>Hinweis: Bei der Verwendung von Routern oder Gateways <i>ARP Aging Time</i> an die zusätzlichen Verzögerungen für Hin- und Rückweg anpassen (erhöhen). Ist die <i>ARP Aging Time</i> zu klein, wird die MAC-Adresse des Kommunikationspartners im ARP-Cache gelöscht und die Kommunikation wird nur verzögert ausgeführt oder bricht ab. Für einen effizienten Einsatz muss die <i>ARP Aging Time</i> > der <i>ReceiveTimeouts</i> der verwendeten Protokolle sein.</p>

Bezeichnung	Beschreibung
MAC Learning	<p>Mit MAC Learning und <i>ARP Aging Time</i> stellt der Anwender ein, wie schnell eine MAC-Adresse gelernt werden soll.</p> <p>Folgende Einstellungen sind möglich:</p> <ul style="list-style-type: none"> ▪ konservativ (Empfohlen): Wenn sich im ARP-Cache bereits MAC-Adressen von Kommunikationspartnern befinden, so sind diese Einträge für die Dauer von mindestens 1 mal <i>ARP Aging Time</i> bis maximal 2 mal <i>ARP Aging Time</i> verriegelt und können nicht durch andere MAC-Adressen ersetzt werden. ▪ tolerant: Beim Empfang einer Nachricht wird die IP-Adresse in der Nachricht mit den Daten im ARP-Cache verglichen und die gespeicherte MAC-Adresse im ARP-Cache sofort mit der MAC-Adresse aus der Nachricht überschrieben. Die Einstellung <i>Tolerant</i> ist zu verwenden, wenn die Verfügbarkeit der Kommunikation wichtiger ist als der sichere Zugriff (authorized access) auf die Steuerung. <p>Standardeinstellung: konservativ</p>
ICMP Mode	<p>Das Internet Control Message Protocol (ICMP) ermöglicht den höheren Protokollschichten, Fehlerzustände auf der Vermittlungsschicht zu erkennen und die Übertragung der Datenpakete zu optimieren.</p> <p>Meldungstypen des Internet Control Message Protocol (ICMP), die von dem CPU-Modul unterstützt werden:</p> <ul style="list-style-type: none"> ▪ keine ICMP-Antworten Alle ICMP-Befehle sind abgeschaltet. Dadurch wird eine hohe Sicherheit gegen Sabotage erreicht, die über das Netzwerk erfolgen könnte. ▪ Echo Response Wenn Echo Response eingeschaltet ist, antwortet der Knoten auf einen Ping-Befehl. Es ist somit feststellbar, ob ein Knoten erreichbar ist. Die Sicherheit ist immer noch hoch. ▪ Host unerreichbar Für den Anwender nicht von Bedeutung. Nur für Tests beim Hersteller. ▪ alle implementierten ICMP-Antworten Alle ICMP-Befehle sind eingeschaltet. Dadurch wird eine genauere Fehlerdiagnose bei Netzwerkstörungen erreicht. <p>Standardeinstellung: Echo Response</p>

Tabelle 7: Konfigurationsparameter

3.3.3.2 Register: Routings

Das Register **Routings** enthält die Routing-Tabelle. Diese ist bei neu eingefügten Modulen leer. Es sind maximal 8 Routing-Einträge möglich.

Bezeichnung	Beschreibung
Name	Bezeichnung der Routing-Einstellung.
IP Adresse	Ziel IP-Adresse des Kommunikationspartners (bei direktem Host-Routing) oder Netzwerkadresse (bei Subnet-Routing). Wertebereich: 0.0.0.0 ... 255.255.255.255 Standardwert: 0.0.0.0
Subnet Mask	Definiert Ziel-Adressbereich für einen Routing-Eintrag. 255.255.255.255 (bei direktem Host-Routing) oder Subnet-Maske des adressierten Subnetzes. Wertebereich: 0.0.0.0 ... 255.255.255.255 Standardwert: 255.255.255.255
Gateway	IP-Adresse des Gateways zum adressierten Netzwerk. Wertebereich: 0.0.0.0 ... 255.255.255.255 Standardwert: 0.0.0.1

Tabelle 8: Routing Parameter

3.3.3.3 Register: Ethernet-Switch

Das Register **Ethernet-Switch** enthält die folgenden Parameter:

Bezeichnung	Beschreibung
Name	Nummer des Ports wie Gehäuseaufdruck; pro Port darf nur eine Konfiguration vorhanden sein. Wertebereich: 1 ... 4
Speed [Mbit/s]	10 MBit/s: Datenrate 10 MBit/s 100 MBit/s: Datenrate 100 MBit/s 1000 MBit/s: Datenrate 1000 MBit/s (nur X-CPU 01 Modul). Autoneg (10/100/1000): automatische Einstellung der Baudrate. Standardwert: Autoneg
Flow-Control	Vollduplex: Kommunikation in beide Richtungen gleichzeitig. Halbduplex: Kommunikation in eine Richtung. Autoneg: Automatische Kommunikationssteuerung. Standardwert: Autoneg
Autoneg auch bei festen Werten	Das <i>Advertising</i> (Übermitteln der Speed und Flow-Control Eigenschaften) wird auch bei fest eingestellten Werten von <i>Speed</i> und <i>Flow-Control</i> durchgeführt. Hierdurch erkennen andere Geräte, deren Ports auf <i>Autoneg</i> eingestellt sind, die Einstellung der Ports.
Limit	Eingehende Multicast- und/oder Broadcast-Pakete limitieren. Aus: Keine Limitierung. Broadcast: Broadcast limitieren (128 kbit/s). Multicast und Broadcast: Multicast und Broadcast limitieren (1024 kbit/s). Standardwert: Broadcast

Tabelle 9: Ethernet-Switch-Parameter

3.3.3.4 Register: VLAN (Port based VLAN)

Konfiguriert die Verwendung von port-based VLAN, siehe auch Kapitel 3.3.5.

i

Soll VLAN unterstützt werden, muss Port based VLAN abgeschaltet sein, so dass jeder Port mit jedem anderen Port des Switches kommunizieren kann.

Für jeden Port eines Switches kann eingestellt werden, zu welchem anderen Port des Switches empfangene Ethernet Frames gesendet werden dürfen.

Die Tabelle im Register VLAN enthält Einträge, mit denen die Verbindung zwischen zwei Ports *aktiv* oder *inaktiv* geschaltet werden kann.

Name	Eth1	Eth2	Eth3	Eth4
Eth1				
Eth2	aktiv			
Eth3	aktiv	aktiv		
Eth4	aktiv	aktiv	aktiv	
CPU	aktiv	aktiv	aktiv	aktiv

Tabelle 10: Register VLAN

Standardeinstellung: alle Verbindungen zwischen den Ports *aktiv*

3.3.3.5 Register: LLDP

LLDP (Link Layer Discovery Protocol) sendet per Multicast in periodischen Abständen Informationen über das eigene Gerät (z. B. MAC-Adresse, Gerätenamen, Portnummer) und empfängt die gleichen Informationen von Nachbargeräten.

Abhängig ob Profinet auf dem Kommunikationsmodul konfiguriert ist, werden von LLDP folgende Werte verwendet:

Profinet auf COM-Modul	ChassisID	TTL (Time to Live)
verwendet	Stationsname	20 s
nicht verwendet	MAC-Adresse	120 s

Tabelle 11: Werte von LLDP für Profinet

Das Prozessor- und das Kommunikationsmodul unterstützen LLDP auf den Ports Eth1, Eth2, Eth3 und Eth4.

Die folgenden Parameter legen fest, wie der betreffende Port arbeitet:

Aus	LLDP ist auf diesem Port deaktiviert.
Send	LLDP sendet LLDP Ethernet Frames, empfangene LLDP Ethernet frames werden gelöscht ohne diese zu verarbeiten.
Receive	LLDP sendet keine LLDP Ethernet Frames, aber empfangene LLDP Frames werden verarbeitet.
Send/Receive	LLDP sendet und verarbeitet empfangene LLDP Ethernet Frames.

Standardeinstellung: Aus

3.3.3.6 Register: Mirroring

Konfiguriert, ob das Modul Ethernet-Pakete auf einen Port dupliziert, so dass sie von einem dort angeschlossenen Gerät mitgelesen werden können, z.B. zu Testzwecken.

Die folgenden Parameter legen fest, wie der betreffende Port arbeitet:

- Aus Dieser Port nimmt am Mirroring nicht teil.
- Egress: Ausgehende Daten dieses Ports werden dupliziert.
- Ingress: Eingehende Daten dieses Ports werden dupliziert.
- Egress/Ingress: Ein- und ausgehende Daten dieses Ports werden dupliziert.
- Dest Port: Duplizierte Daten werden auf diesen Port geschickt.

Standardeinstellung: Aus

3.3.4 Verwendete Netzwerk-Ports für Ethernet-Kommunikation

UDP Ports	Verwendung
123	SNTP (Zeitsynchronisation zwischen Steuerung und Remote I/O, sowie externen Geräten).
502	Modbus Slave (vom Anwender änderbar).
6010	safeethernet und OPC.
8000	Programmierung und Bedienung mit SILworX.
8001	Port auf Remote I/O zur Konfiguration der Remote I/O durch die Steuerung.
8004	Port auf Steuerung zur Konfiguration der Remote I/O durch die Steuerung.
34964	PROFINET Endpointmapper (für Verbindungsaufbau notwendig).
49152	PROFINET RPC-Server.
49153	PROFINET RPC-Client.
Xxx	ComUserTask durch Anwender vergeben. Darf nicht von einem anderen Protokoll belegt sein.

Tabelle 12: Verwendete Netzwerk-Ports (UDP-Ports)

TCP Ports	Verwendung
502	Modbus Slave (vom Anwender änderbar).
Xxx	TCP-SR durch Anwender vergeben.
Xxx	ComUserTask durch Anwender vergeben. Darf nicht von einem anderen Protokoll belegt sein.

Tabelle 13: Verwendete Netzwerk-Ports (TCP-Ports)

3.3.5 Switchports durch VLAN trennen

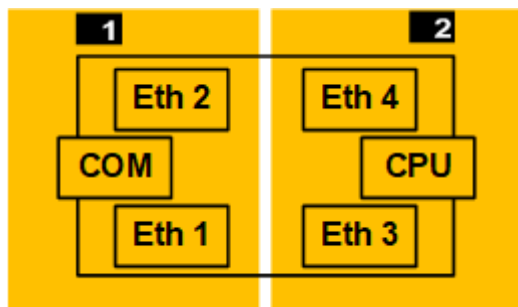
Mit VLAN Einstellungen ist es möglich, die verfügbaren Switchports entsprechend der benötigten Anwendung aufzuteilen. So ist es in der HIMatrix möglich, eine Verbindung mit zwei IP-Adressen aufzubauen und eine sichere Kommunikation über die CPU von der nicht sicherheitsbezogenen Kommunikation über die COM zu trennen.

Die Konfiguration des Switchports erfolgt in SILworX über die Detailansicht des CPU- oder COM-Moduls, siehe Kapitel 3.3.3.

HIMA empfiehlt, bei der HIMatrix CPU und COM zu trennen. Die exemplarische Darstellung unten kann natürlich an die anwendungsspezifischen Bedürfnisse Angepasst werden.

	Eth1	Eth2	Eth3	Eth4	COM
Eth1					
Eth2	aktiv				
Eth3	inaktiv	inaktiv			
Eth4	inaktiv	inaktiv	aktiv		
COM	aktiv	aktiv	inaktiv	inaktiv	
CPU	inaktiv	inaktiv	aktiv	aktiv	inaktiv

Tabelle 14: Register VLAN



- 1** Eth 1 und Eth 2 in den nicht geschützten Bereich über die COM für die nicht sicherheitsbezogenen Protokolle.
- 2** Eth 3 und Eth 4 in den geschützten Bereich über die CPU für die safeethernet Kommunikation zu den Remote I/Os und anderen HIMA PES..

Bild 1: Beispiel zur Aufteilung des Switchports durch VLAN

·
i

Falls alle Ethernet-Port Verbindungen zum Prozessor der Steuerung durch die VLAN-Konfiguration unterbunden wurden, muss für die Steuerung ein Reset durchgeführt werden. Die Steuerung ist danach über die Standard IP-Adresse wieder erreichbar.

·
i

Verbindungsblockaden bei durch VLAN getrennte Netzwerke, wenn diese Netzwerke nicht vollständig getrennt sind, z. B. verbunden durch einen gemeinsamen externen Switch. HIMatrix Steuerungen haben auf dem internen Switch eine **gemeinsame** MAC<->Switchport Zuordnungstabelle für die CPU und die COM. Beim Eintreffen von Ethernet Frames aus einem nicht vollständig getrennten Netzwerk wird die MAC<->Switchport Zuordnungstabelle des internen Switches ständig umgelernt. Dadurch kommt es zu wechselseitigen Blockaden der jeweiligen Ethernet Frames and die CPU und die COM.

3.4 Feldbus-Schnittstellen

Die Feldbus-Submodule ermöglichen die Kommunikation über die Feldbus-Schnittstellen der HIMax X-COM 01, HIQuad X F-COM 01 sowie der HIMatrix Steuerungen F30, F35 und F60 CPU 01.

Für die HIMax und HIMatrix Steuerungen sind die Feldbus-Submodule eine Option und werden werkseitig eingebaut. Die Feldbus-Schnittstelle FB3 der HIMatrix Steuerungen ist werkseitig mit RS485 für Modbus (Master oder Slave) oder ComUserTask belegt.

Für die HIQuad X Steuerungen werden die Übertragungsstandards der Feldbus-Schnittstellen vom Anwender in SILworX konfiguriert. Nach dem Laden dieser Konfiguration in die HIQuad X Steuerung erfolgt automatisch die Pin-Belegung der Schnittstellen FB1/FB2 des F-COM 01 Moduls.

Die Feldbus-Protokolle dürfen in Verantwortung des Anwenders nur für sicherheitstechnische Funktionen verwendet werden, wenn ausreichende Zusatzmaßnahmen ergriffen wurden.

Eine Programmierung über diese Schnittstellen ist im System nicht vorgesehen.

3.4.1 Registrierung und Aktivierung

Abhängig vom Protokoll werden die Kommunikationsoptionen aktiviert, siehe Kapitel 3.2.

3.4.2 Installation der Feldbus-Submodule

Die Feldbus-Submodule sind eine Option und werden werkseitig eingebaut. Die Festlegung erfolgt bei der Bestellung über die Teilenummer. Zusätzlich müssen die verwendeten Protokolle teilweise aktiviert werden.

3.4.2.1 Aufbau der Teilenummer

Die folgenden Abschnitte beschreiben, wie bei der HIMax X-COM 01 oder einer HIMatrix Steuerung sich die Teilenummer mit der Belegung der Feldbus-Schnittstellen ändert.

Für die Teilenummer sind den Feldbus-Submodulen Zahlen zugeordnet, siehe Tabelle 15.

Optionen für FB1 und FB2	Bezeichnung	Beschreibung für Feldbus-Submodul
0	--	kein Feldbus-Submodul eingebaut.
1	RS485-Modul	RS485 für die Verwendung mit Modbus (Master oder Slave) oder ComUserTask.
2	PROFIBUS Master	PROFIBUS DP Master.
3	PROFIBUS Slave	PROFIBUS DP Slave.
5	RS232-Modul	RS232 für die Verwendung mit ComUserTask.
6	RS422-Modul	RS422 für die Verwendung mit ComUserTask.
7	SSI-Modul	SSI für die Verwendung mit ComUserTask.
8	CAN-Modul	CAN für die Verwendung mit ComUserTask. Nur für HIMatrix verfügbar

Tabelle 15: Optionen für Feldbus-Schnittstellen FB1 und FB2

3.4.2.2 Teilenummer des HIMax COM-Moduls

Bei der Ausrüstung der X-COM 01 mit einem oder mehreren Feldbus-Submodulen ändert sich neben der Teilenummer auch die Bezeichnung des Moduls von X-COM 01 nach X-COM 010 XY.

Das COM-Modul bildet mit dem Connector Board X-CB 001 02 eine funktionale Einheit. Das Connector Board muss separat bestellt werden.

Nachfolgende Tabelle enthält die verfügbaren Komponenten:

Bezeichnung	Beschreibung
X-COM 01	Kommunikationsmodul ohne Feldbus-Submodule.
X-COM 010 XY ¹⁾	Kommunikationsmodul mit Feldbus-Submodul.
X-CB 001 02	Connector Board.
¹⁾ X : Option für Feldbus-Schnittstelle FB1 gemäß Tabelle 15. Y : Option für Feldbus-Schnittstelle FB2 gemäß Tabelle 15.	

Tabelle 16: Verfügbare HIMax Komponenten

Bezeichnung und Teilenummer (Part-Nr.) sind auf dem Typenschild des Moduls abgedruckt.

i

HIMA empfiehlt, PROFIBUS DP über die Feldbus-Schnittstelle FB1 (Übertragungsrate maximal 12 MBit) zu betreiben. Über die Feldbus-Schnittstelle FB2 ist eine maximale Übertragungsrate von 1,5 MBit zugelassen.

3.4.2.3 Teilenummern der HIMatrix Steuerungen

Die HIMatrix Steuerungen können gemäß folgender Tabelle mit Feldbus-Submodulen ausgerüstet werden:

Steuerung	FB1 und FB2	FB3
F30 03z XY ¹⁾	Frei bestückbar gemäß Tabelle 15.	Eingebaut RS485
F35 03z XY ¹⁾	Frei bestückbar gemäß Tabelle 15.	Eingebaut RS485
F60 CPU 03z XY ¹⁾	Frei bestückbar gemäß Tabelle 15.	---
¹⁾ X : Option für Feldbus-Schnittstelle FB1 gemäß Tabelle 15. Y : Option für Feldbus-Schnittstelle FB2 gemäß Tabelle 15. z : Hardwarevariante		

Tabelle 17: Ausrüstung von HIMatrix Steuerungen mit Feldbus-Submodulen

Mit der Auswahl des entsprechenden Feldbus-Submoduls ändert sich die Teilenummer:

z.B. „F35 030 XY“ hat die Teilenummer: 98 22**XY**497

X: Option für Feldbus-Schnittstelle FB1 gemäß Tabelle 15

Y: Option für Feldbus-Schnittstelle FB2 gemäß Tabelle 15

3.4.3 HIMax und HIMatrix Feldbus-Schnittstellen

Die Pin-Belegungen der HIMax und HIMatrix Feldbus-Schnittstellen ist abhängig von der gewählten Kommunikationsoption, siehe Kapitel 3.4.

1

Verschaltung und Busabschlüsse!

Beim Anschluss an die Feldbus-Schnittstellen jeweilige Feldbus-Norm beachten.

- Diese erfordern ein passendes Erdungskonzept.
- Die geschirmten Kabel sollten beidseitig großflächig aufgelegt werden. Die Feldbusse an physikalischen Enden mit Busabschlüssen abschließen.

3.4.3.1 RS485 für Modbus Master, Slave oder ComUserTask

Es ist ein RS485 Kabel zu verwenden, siehe Kapitel 3.7.

Anschluss	Signal	Funktion
1	-	Nicht belegt.
2	5V	Feldbus-Versorgung über Diode entkoppelt.
3	RxD/TxD-A	Empfangs-/Sendedaten-A.
4	CNTR-A	Steuersignal A.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	5V	Feldbus-Versorgung.
7	-	Nicht belegt.
8	RxD/TxD-B	Empfangs-/Sendedaten-B.
9	CNTR-B	Steuersignal B.

Tabelle 18: Pin-Belegung der D-Sub-Anschlüsse für RS485

3.4.3.2 PROFIBUS DP Master oder Slave

Es ist ein PROFIBUS DP Kabel zu verwenden, siehe Kapitel 3.7.

Anschluss	Signal	Funktion
1	-	Nicht belegt.
2	-	Nicht belegt.
3	RxD/TxD-A	PROFIBUS DP Empfangs-/Sendedaten-A.
4	RTS	Steuersignal.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	5V	Feldbus-Versorgung.
7	-	Nicht belegt.
8	RxD/TxD-B	PROFIBUS DP Empfangs-/Sendedaten-B.
9	-	Nicht belegt.

Tabelle 19: Pin-Belegung der D-Sub-Anschlüsse für PROFIBUS DP

3.4.3.3 RS232 für ComUserTask

Es ist ein RS485 (RS232) Kabel zu verwenden, siehe Kapitel 3.7.

Anschluss	Signal	Funktion
1	-	Nicht belegt.
2	TxD	Sendedaten.
3	RxD	Empfangsdaten.
4	-	Nicht belegt.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	-	Nicht belegt.
7	RTS	Anforderung zum Senden (Request to Send).
8	-	Nicht belegt.
9	-	Nicht belegt.

Tabelle 20: Pin-Belegung der D-Sub-Anschlüsse für RS232

3.4.3.4 RS422 für ComUserTask

Es ist ein RS485 (RS422) Kabel zu verwenden, siehe Kapitel 3.7.

Anschluss	Signal	Funktion
1	-	Nicht belegt.
2	5V	Feldbus-Versorgung über Diode entkoppelt.
3	RxA	Empfangsdaten-A.
4	TxA	Sendedaten-A.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	5V	Feldbus-Versorgung.
7	-	Nicht belegt.
8	RxB	Empfangsdaten-B.
9	TxB	Sendedaten-B.

Tabelle 21: Pin-Belegung der D-Sub-Anschlüsse für RS422

3.4.3.5 SSI

Es ist ein RS485 (SSI) Kabel zu verwenden, siehe Kapitel 3.7.

Anschluss	Signal	Funktion
1	D2+	Dateneingang Kanal 2+.
2	D1-	Dateneingang Kanal 1-.
3	CL2+/D3+	Schiebetakt-Ausgang Kanal 2+ oder Dateneingang Kanal 3+.
4	CL1+	Schiebetakt-Ausgang Kanal 1+.
5	GND	Bezugspotential.
6	D1+	Dateneingang Kanal 1+.
7	D2-	Dateneingang Kanal 2-.
8	CL2-/D3-	Schiebetakt-Ausgang Kanal 2- oder Dateneingang Kanal 3-.
9	CL1-	Schiebetakt-Ausgang Kanal 1-.

Tabelle 22: Pin-Belegung der D-Sub-Anschlüsse für SSI

3.4.3.6 CAN

Es ist ein CAN Kabel zu verwenden, siehe Kapitel 3.7.

Anschluss	Signal	Funktion
1	-	Nicht belegt.
2	CAN-L	CAN-Low.
3	GND	Bezugspotential.
4	-	Nicht belegt.
5	-	Nicht belegt.
6	-	Nicht belegt.
7	CAN-H	CAN-High.
8	-	Nicht belegt.
9	-	Nicht belegt.

Tabelle 23: Pin-Belegung der D-Sub-Anschlüsse für CAN

3.4.4 HIQuad X F-COM 01 Feldbus-Schnittstellen

Die Pin-Belegungen der F-COM 01 Feldbus-Schnittstellen FB1/FB2 ist abhängig von der gewählten Kommunikationsoption, siehe Kapitel 3.4.

1

Verschaltung und Busabschlüsse!

Beim Anschluss an die Feldbus-Schnittstellen jeweilige Feldbus-Norm beachten.

- Diese erfordern ein passendes Erdungskonzept.
- Die geschirmten Kabel sollten beidseitig großflächig aufgelegt werden. Die Feldbusse an physikalischen Enden mit Busabschlüssen abschließen.

3.4.4.1 RS422

Es ist ein RS485 (RS422) Kabel zu verwenden, siehe Kapitel 3.7.

Pin	Signal	Beschreibung
1	-	Nicht belegt.
2	5V	Feldbus-Versorgung über Diode entkoppelt.
3	RxD-A	Empfangsdaten-A.
4	TxD-A	Sendedaten-A.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	5V	Feldbus-Versorgung.
7	-	Nicht belegt.
8	RxD-B	Empfangsdaten-B.
9	TxD-B	Sendedaten-B.

Tabelle 24: Pin-Belegung der Schnittstelle FB1 mit RS422

3.4.4.2 RS485 mit RTS

Es ist ein RS485 Kabel zu verwenden, siehe Kapitel 3.7.

Pin	Signal	Beschreibung
1	-	Nicht belegt.
2	5V	Feldbus-Versorgung über Diode entkoppelt.
3	RXD/TXD-A	Empfangs-/Sendedaten-A.
4	CNTR-A	Steuersignal A.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	5V	Feldbus-Versorgung.
7	-	Nicht belegt.
8	RXD/TXD-B	Empfangs-/Sendedaten-B.
9	CNTR-B	Steuersignal B.

Tabelle 25: Pin-Belegung der Schnittstelle FB1 mit RS485 (mit RTS)

3.4.4.3 Zweimal RS485 (ohne RTS)

Es ist ein (zwei) RS485 Kabel zu verwenden, siehe Kapitel 3.7.

Die Pin-Belegung entspricht nicht der Norm, da zwei Schnittstellen auf einem Stecker liegen.

Pin	Signal	Beschreibung
1	-	Nicht belegt.
2	5V	Feldbus-Versorgung über Diode entkoppelt.
3	RxD1/TxD1-A	Erste Empfangs-/Sendedaten-A.
4	RxD2/TxD2-A	Zweite Empfangs-/Sendedaten-A.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	5V	Feldbus-Versorgung.
7	-	Nicht belegt.
8	RxD1/TxD1-B	Erste Empfangs-/Sendedaten-B.
9	RxD2/TxD2-B	Zweite Empfangs-/Sendedaten-B.

Tabelle 26: Pin-Belegung der Schnittstelle FB1/2 mit zweimal RS485 (ohne RTS)

i

Nach Reload auf FB1 mit RS485 (mit RTS) ist die Belegung Tabelle 25 aktiv.

Nach Reload auf FB2 mit RS485 (ohne RTS) ist die Belegung Tabelle 27 aktiv.

3.4.4.4 FB2 mit RS485 (ohne RTS)

Es ist ein RS485 Kabel zu verwenden, siehe Kapitel 3.7.

Die Pin-Belegung entspricht nicht der Norm.

Pin	Signal	Beschreibung
1	-	Nicht belegt.
2	5V	Feldbus-Versorgung über Diode entkoppelt.
3	-	-
4	RxD2/TxD2-A	Zweite Empfangs-/Sendedaten-A.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	5V	Feldbus-Versorgung.
7	-	Nicht belegt.
8	-	-
9	RxD2/TxD2-B	Zweite Empfangs-/Sendedaten-B.

Tabelle 27: Pin-Belegung der Schnittstelle FB2 mit RS485 (ohne RTS)

3.4.4.5 PROFIBUS DP Slave

Es ist ein PROFIBUS DP Kabel zu verwenden, siehe Kapitel 3.7.

Pin	Signal	Beschreibung
1	-	Nicht belegt.
2	5V	Feldbus-Versorgung über Diode entkoppelt.
3	RXD/TXD-A	PROFIBUS DP Empfangs-/Sendedaten-A.
4	CNTR-A	Steuersignal A.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	5V	Feldbus-Versorgung.
7	-	Nicht belegt.
8	RXD/TXD-B	PROFIBUS DP Empfangs-/Sendedaten-B.
9	CNTR-B	Steuersignal B.

Tabelle 28: Pin-Belegung der Schnittstelle FB1 mit PROFIBUS DP Slave

3.4.4.6 PROFIBUS DP Slave und RS485

Die Pin-Belegung entspricht nicht der Norm, da zwei Schnittstellen auf einem Stecker liegen.

Für PROFIBUS DP Slave ist ein PROFIBUS DP Kabel zu verwenden. Für RS485 ist ein RS485 Kabel zu verwenden, siehe Kapitel 3.7.

Pin	Signal	Beschreibung
1	-	Nicht belegt.
2	5V	Feldbus-Versorgung über Diode entkoppelt.
3	PROFIBUS DP RXD/TXD-A	PROFIBUS DP Empfangs-/Sendedaten-A.
4	RS485 RxD1/TxD1-A	Empfangs-/Sendedaten-A.
5	DGND	Datenübertragungspotential (Masse zu 5 V).
6	5V	Feldbus-Versorgung.
7	-	Nicht belegt.
8	PROFIBUS DP RXD/TXD-B	PROFIBUS DP Empfangs-/Sendedaten-B.
9	RS485 RxD1/TxD1-B	RS485 Empfangs-/Sendedaten-B.

Tabelle 29: Pin-Belegung der Schnittstelle FB1/2 mit PROFIBUS DP Slave und RS485

3.5 Technische Eigenschaften der RS-485-Übertragung

In der folgenden Tabelle sind die grundlegenden technischen Eigenschaften der RS-485-Übertragung, die auch für den PROFIBUS-DP verwendet wird, dargestellt.

Element	Beschreibung
Netzwerk-Topologie	Linearer Bus, aktiver Busabschluss an beiden Enden.
Medium	Geschirmte, Paarweise verdrehte Zweidrahtleitung.
Steckverbinder	9-pol-SUB-D Steckverbinder, siehe Kapitel 3.4.3 und Kapitel 3.4.4.
Busteilnehmer pro Segment	32 Busteilnehmer in jedem Segment ohne Repeater ¹⁾ .
Busteilnehmer pro Bus insgesamt	1 Modbus Master, 3 Repeater ¹⁾ . 121 Modbus Slaves.
Max. Länge eines Bus Segments	1200 m pro Segment.
Max. Länge des Bus	4800 m, 4 Segmente mit 3 Repeatern ¹⁾ .
Max. Baudrate	115200 Bit/s
¹⁾ Pro eingesetzten Repeater reduziert sich die maximale Zahl der Busteilnehmer in diesem Segment um 1. Das bedeutet, dass in diesem Segment maximal 31 Busteilnehmer betrieben werden können. Nach der Norm sind insgesamt drei Repeater zulässig, so dass maximal 121 Modbus Slaves pro serielle Schnittstelle eines Modbus Masters angeschlossen werden können. Stehen mehrere Schnittstellen zur Verfügung (HIMax und HIMatrix) können an bis zu 3 Schnittstellen Slaves bzw. Repeater angeschlossen werden. Intern verhält sich das System als ein Master. Die Maximalanzahl Slaves ist dann 254.	

Tabelle 30: Eigenschaften der RS485 Übertragung

Die in der Tabelle 31 angegebene Leitungslänge hängt von der gewählten Baudrate ab.

Baudrate	Leitungslänge pro Segment	RS485	PROFIBUS-DP
300 Bit/s	1200 m	X	-
600 Bit/s	1200 m	X	-
1200 Bit/s	1200 m	X	-
2400 Bit/s	1200 m	X	-
4800 Bit/s	1200 m	X	-
9600 Bit/s	1200 m	X	X
19200 Bit/s	1200 m	X	X
38400 Bit/s	1200 m	X	-
45450 Bit/s	1200 m	-	X
57600 Bit/s	1200 m	X	-
62500 Bit/s	1200 m	X	-
76800 Bit/s	1200 m	X	-
93750 Bit/s	1200 m	-	X
115200 Bit/s	1200 m	X	-
187500 Bit/s	1000 m	-	X
500000 Bit/s	400 m	-	X
1,5 MBit/s	200 m	-	X
3 MBit/s	100 m	-	X
6 MBit/s	100 m	-	X
12 MBit/s	100 m	-	X

Tabelle 31: Leitungslänge in Abhängigkeit von der Baudrate für RS 485 und PROFIBUS-DP

i

Eine Vergrößerung der Leitungslänge lässt sich mittels bidirektionaler Repeater erreichen. Maximal dürfen drei Repeater zwischen zwei Teilnehmer geschaltet werden. Somit ist eine Leitungslänge von 4,8 km möglich.

HIMA empfiehlt, bei zeitkritischen Anwendungen nicht mehr als 32 Busteilnehmer anzuschließen. Für nicht zeitkritische Anwendung sind bis zu 126 Teilnehmer (mit Repeater) zulässig.

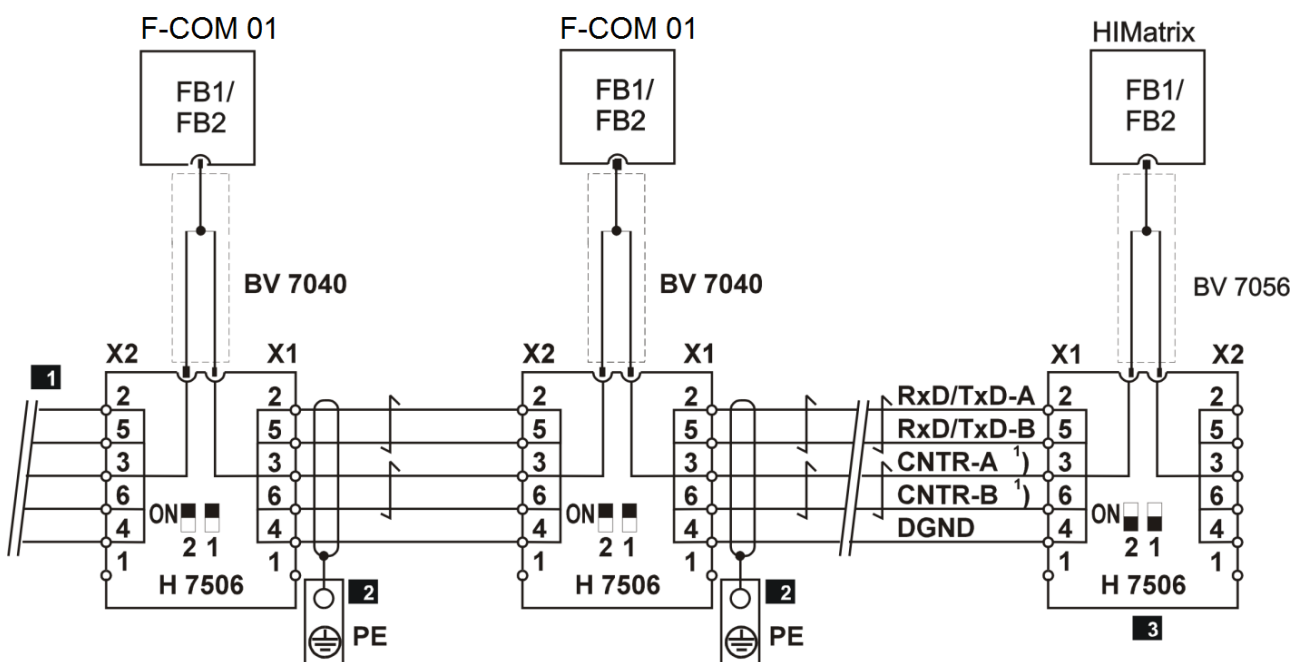
3.6 RS485 Bus-Topologie

Das folgende Bild zeigt exemplarisch den Aufbau einer RS485 Bus-Topologie mit HIMA Komponenten. Als Busklemmen werden H 7506 eingesetzt. Die gesamte Länge des Bus darf maximal 1200 m betragen. Größere Entfernungen erfordern den Einsatz eines Repeaters z. B. H 7505. Insgesamt sind 3 Repeater einsetzbar. Der Bus kann also eine maximale Ausdehnung von 4800 m haben.

i

Werden LWL/RS485 Konvertern im Bus verwendet, darf die H7505 nicht verwendet werden (keine automatische Umschaltung der Datenrichtung).

Die Zeit, bis die Information eines Slaves beim Master verfügbar ist, steigt mit der Anzahl der Slaves am Bus an. Je mehr Slaves am Bus angeschlossen sind, umso schlechter werden die Reaktionszeiten des Systems.



1) Nur erforderlich bei Repeater-Betrieb

- 1** Weitere Steuerungen
- 2** Schutzleiterklemme USLKG4 ge/gn

- 3** H 7506 Bus-Ende mit Abschluß
(Schalterstellung: Beide weiße Schalter auf ON)

Bild 2: RS485 Bus-Topologie

i

Wird der Bus über größeren Distanzen geführt, sollte ein Potentialausgleich erfolgen. Bei Übertragungsraten $\geq 1,5$ MBit/s sind Stichleitungen unbedingt zu vermeiden. Verwenden Sie darum nur geeignete Busanschlussstecker.

3.6.1 Klemmenbelegung H 7506

Die folgende Tabelle zeigt die Klemmenbelegung der HIMA Busklemme H 7506. Das HIMA Kabel BV 7040 verbindet die H 7506 mit der Feldbus-Schnittstelle FBx der Steuerung.

X1/X2	Farbe	Beschreibung
1	-	-
2	WH	RxD/TxD-A, Datenleitung.
3	GN	CNTR-A, Steuerleitung für Repeater.
4	GY	DGND
5	BN	RxD/TxD-B, Datenleitung.
6	YE	CNTR-B, Steuerleitung für Repeater.

Tabelle 32: Klemmenbelegung H 7506



Produktdokumentationen zu dieser und weiteren HIMA RS485 Komponenten stehen für registrierte Kunden unter <https://www.hima.com/de/downloads/> bereit.

3.6.2 Busanschluss und Busabschluss

Das ankommende und das abgehende Datenkabel können direkt im Busanschlusstecker verbunden werden. Dadurch werden Stichleitungen vermieden und der Busanschlusstecker kann jederzeit, ohne Unterbrechung des Datenverkehrs, am Feldgerät auf- und abgesteckt werden.

In der IEC 61158 wird für PROFIBUS-DP ein 9-poliger Sub-D-Stecker empfohlen. Je nach Schutzart des Feldgerätes sind auch andere verfügbare Stecker erlaubt.

Die Steckerbelegung des 9-poligen Sub-D-Steckers ist in Bild 3 dargestellt. Am Feldgerät ist der Busanschluss als Buchse ausgelegt.

Der PROFIBUS-DP Busabschluss besteht aus einer Widerstandskombination, durch die ein definiertes Ruhepotential auf der Busleitung sichergestellt wird. Die Widerstandskombination ist in den PROFIBUS-DP Busanschlussteckern integriert und kann über Brücken oder Schalter aktiviert werden.

Stationen, an denen der Bus endet, sollten zudem eine 5-V-Spannung an Pin 6 anbieten.

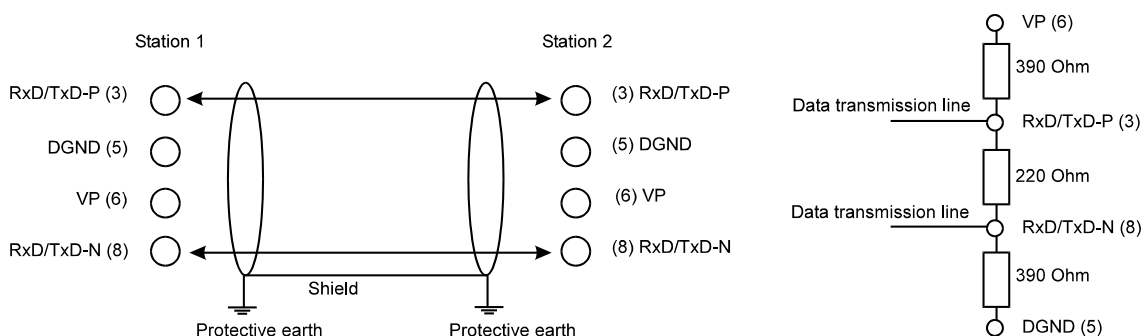


Bild 3: Busanschluss und Busabschluss, Pin-Belegung der Feldbus-Schnittstelle

3.7 Anforderungen an die Kommunikationskabel

Für Kommunikationsverbindungen, die innerhalb eines Schaltschranks verlaufen, muss der Leiterquerschnitt des Kabels mindestens 0,2 mm² betragen.

Für Kommunikationsverbindungen, die außerhalb eines Schaltschranks verlaufen, muss der Leiterquerschnitt des Kabels mindestens 0,5 mm² betragen. Gegebenenfalls muss hierfür Verlegekabel mit starren Adern anstelle von Kabel mit flexiblen Adern verwendet werden.

Für den Anschluss der Ethernet-/Feldbus-Schnittstellen sind Kabel mit folgenden Eigenschaften zugelassen:

- Alle Leitungen für die Ethernet-/Feldbus-Schnittstellen müssen mindestens 500 Biegezyklen standhalten, falls Biegebeanspruchung im bestimmungsgemäßen Betrieb vorgesehen sind.
- Alle Leitungen für die Ethernet-/Feldbus-Schnittstellen müssen mindestens 25 Biegezyklen standhalten, falls Biegebeanspruchung nur bei Wartung vorgesehen sind.
- Alle Leitungen für die Ethernet-/Feldbus-Schnittstellen müssen UL94-V0 genügen.

3.7.1 Patchkabel

HIMA empfiehlt Patchkabel mit den folgenden Minimalanforderungen: Cat.5e, RJ-45.

3.7.2 CAN Kabel

HIMA empfiehlt für CAN nur die dafür zugelassenen CAN Kabel als Übertragungsmedium zu verwenden.

3.7.3 RS485 (RS422, RS232, SSI) Kabel

HIMA empfiehlt für RS485 (gilt auch für RS422, RS232 und SSI) als Buskabel eine geschirmte, paarweise verdrehte Zweidrahtleitung (twisted pair) mit den folgenden Eigenschaften zu verwenden.

Element	Beschreibung
Kabeltyp	LiYCY 3 x 2 x 0,25 mm ² für RS485, RS422, RS232. LiYCY 6 x 2 x 0,25 mm ² für SSI
Adernquerschnitt	> 0,25 mm ²
Wellenwiderstand	100 ... 120 Ω

Tabelle 33: RS485 (RS422, RS232, SSI) Buskabel

3.7.4 PROFINET Kabel

HIMA empfiehlt für PROFINET nur die dafür zugelassenen PROFINET Kabel als Übertragungsmedium zu verwenden.

3.7.5 PROFIBUS DP Kabel

HIMA empfiehlt für PROFIBUS DP nur die dafür zugelassenen PROFIBUS DP Kabel als Übertragungsmedium mit den folgenden Parametern zu verwenden:

Parameter	Kabeltyp A
Wellenwiderstand	135 ... 165 Ω
Kapazitätsbelag	≤ 30 pF / m
Schleifenwiderstand	≤ 110 Ω / km
Aderndurchmesser	> 0,64 mm
Adernquerschnitt	> 0,34 mm ²

Tabelle 34: Parameter des PROFIBUS-DP Kabeltyp A

Der Kabeltyp A kann für alle Übertragungsraten bis 12 MBit/s genutzt werden.

4 safeethernet

Alle HIMA Systeme können über **safeethernet** sicherheitsbezogen kommunizieren.

i

Das **safeethernet** Protokoll erfüllt alle Anforderungen an sicherheitsbezogene Protokolle gemäß IEC 61508-2:2010, IEC 61784-3:2019 und EN 50159:2010. Der TÜV hat diese Eigenschaften geprüft und das **safeethernet** Protokoll als Bestandteil der HIMA Systeme verifiziert.

Bei einer Bitfehlerwahrscheinlichkeit von 0,5 des Übertragungsmediums, z. B. durch ein störungsbehaftetes Netzwerk, beträgt die Restfehlerrate λ_{SCL} einer Sicherheitstechnischen Funktion (SIF) mit 100 **safeethernet** Verbindungen weniger als 1% von SIL 4 gemäß IEC 61508-2:2010, IEC 61784-3:2019 und EN 50159:2010.

Die Restfehlerraten λ_{SCL} ist unabhängig von der Menge speichernder Netzwerkelemente, nicht sicherheitsbezogenen Geräten, dem Einsatz im WLAN sowie mit Kompression und Verschlüsselung anwendbar.

Daraus ergibt sich für die einzelne **safeethernet** Verbindung eine Restfehlerrate λ_{SCL} von kleiner als $10^{-12}/h$.

Die jeweiligen Ethernet-Schnittstellen der HIMA Steuerungen sind simultan auch für andere Protokolle nutzbar.

Die **safeethernet** Kommunikation zwischen den Steuerungen kann über verschiedene Ethernet-Netzwerktopologien erfolgen. Hierzu können in SILworX so genannte **safeethernet** Profile ausgewählt werden, die zum verwendeten Ethernet-Netzwerk passen, um Geschwindigkeit und Effizienz des Datentransfers zu erhöhen.

Mit den **safeethernet** Profilen ist die **safeethernet** Kommunikation sichergestellt, ohne dass sich der Anwender zunächst in alle Details der Netzwerkkonfiguration einarbeiten muss.

⚠️ WARNUNG



Manipulation der sicherheitsbezogenen Datenübertragung!

Personenschaden

Der Anlagenhersteller sowie der Betreiber haben dafür zu sorgen, dass das für safeethernet verwendete Ethernet ausreichend vor Manipulationen (z. B. durch Hacker) geschützt wird.

Art und Umfang der Maßnahmen sind mit der abnehmenden Prüfstelle abzustimmen.

4.1 Allgemeines zu safeethernet

Im Bereich der Prozess- und Automatisierungstechnik sind Anforderungen wie Determinismus, Zuverlässigkeit, Austauschbarkeit, Erweiterbarkeit und vor allem Sicherheit zentrale Themen.

safeethernet ist ein Protokoll zur Übertragung von sicherheitsbezogenen Daten bis SIL 4 gemäß IEC 61508-2:2010, IEC 61784-3:2019 und EN 50159:2010 auf Basis der Ethernet-Technologie.

safeethernet beinhaltet Mechanismen, die Fehler erkennen und darauf sicherheitsbezogen reagieren.

Die Übertragung der sicherheitsrelevanten Daten erfolgt über Standard-Ethernet (IEEE 802.3) und basiert auf UDP/IP.

safeethernet verwendet „unsichere Datenübertragungskanäle“ (Ethernet) nach dem Black Channel Prinzip und überwacht die Korrektheit der Daten durch sicherheitsbezogene Protokollmechanismen. Dadurch sind z. B. Ethernet-Netzwerkkomponenten wie Switches, Router und Wireless LAN Geräte innerhalb eines sicherheitsbezogenen Netzwerkes verwendbar.

safeethernet nutzt die Fähigkeiten von Standard Ethernet in der Form, dass Sicherheit und Echtzeitfähigkeit ermöglicht werden. Ein spezieller Protokollmechanismus garantiert ein

deterministisches Verhalten auch bei Ausfall oder Eintritt von Kommunikationsteilnehmern. Das System bindet neue Komponenten in das laufende System dann automatisch ein. Alle Komponenten eines Netzwerkes sind während des laufenden Betriebs austauschbar. Mit dem Einsatz von Switches lassen sich Übertragungszeiten klar definieren. Somit wird Ethernet bei geeigneter Auslegung echtzeitfähig.

Die mögliche Übertragungsgeschwindigkeit von bis zu 1 Gbit/s, bietet für Anwendungen der Automation genügend Übertragungskapazitäten für sicherheitsbezogene Daten. Als Übertragungsmedien können z. B. Kupferleitungen und LWL verwendet werden.

Die **safeethernet** Daten können über das bestehende firmeninterne Ethernet-Netzwerk neben dem übrigen Datenverkehr auf dem Ethernet-Netzwerk übertragen werden, was jedoch potentiell zur Erhöhung von Security-Risiken wirken könnte.

i

HIMA empfiehlt für die Reduzierung von Security-Risiken den Aufbau eines Safety-Netzwerks über die CPU-Module und ein davon getrenntes Standard-Netzwerk über die COM-Module. Das Standard-Netzwerk dient der Verbindung zu nicht-sicherheitsbezogenen Komponenten wie z. B. X-OPC Server, siehe Bild 4.

safeethernet ermöglicht flexible Systemstrukturen für die dezentrale Automatisierung mit definierten Reaktionszeiten. Je nach Anforderung kann die Intelligenz wahlweise zentral oder dezentral auf die Teilnehmer innerhalb des Netzwerks verteilt werden.

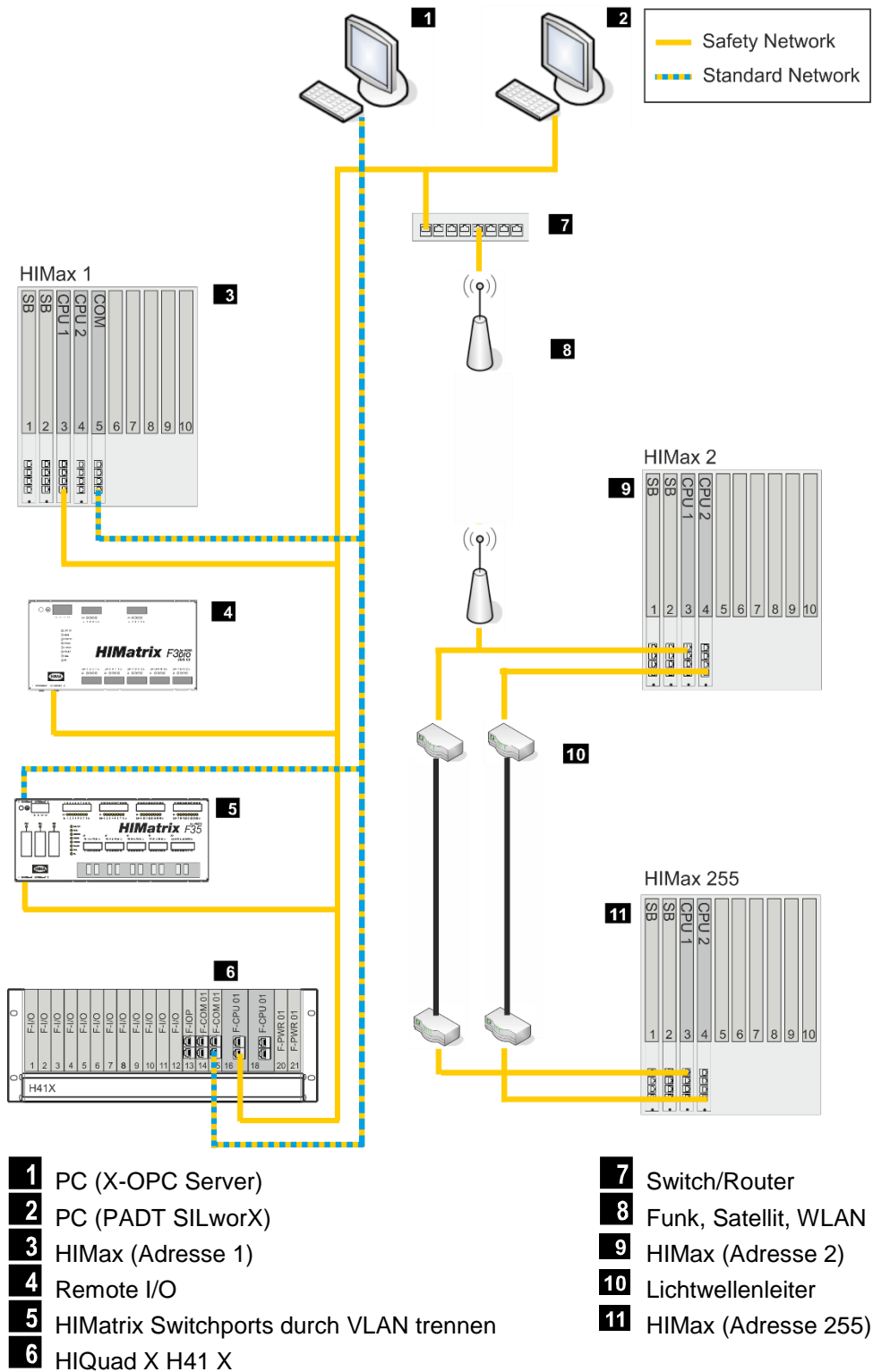


Bild 4: Flexible Systemstruktur mit safeethernet

i

Ein fehlerhafter Aufbau einer Netzstruktur kann dazu führen, dass ein Teil oder das gesamte HIMA System abgeschaltet wird!

Es sind die allgemein gültigen Regeln zur Erstellung von Ethernet-Netzwerken ist zu beachten. Es sollten z. B. keine Netzschleifen entstehen. Datenpakete dürfen nur auf einem Weg zu einer Steuerung gelangen, siehe auch Kapitel 4.7.

4.2 Benutzerauflagen für safeethernet in einem störungsbehafteten Netzwerk

Der Anlagenhersteller sowie der Betreiber müssen in ihre Sicherheitsanalyse die Auswirkungen des störungsbehafteten Netzwerks auf die Anwendung mit einbeziehen.

Damit safe**ethernet** eine für die jeweilige Anwendung hinreichende Verfügbarkeit erreicht, muss der Anwender folgende Auflagen einhalten.

- Der Anwender muss für die sicherheitsbezogene Prozessdatenkommunikation ein geeignetes Übertragungssystem wählen und die safe**ethernet** Parameter dazu derart einstellen, dass für die Anwendung eine hinreichende Verfügbarkeit erreicht wird. Der Anwender muss dazu in seiner Sicherheitsanalyse zum Beispiel die Gefahren einer ungewollten Abschaltung durch safe**ethernet** betrachten. Das Maß der erforderlichen Verfügbarkeit ist im Zweifel mit der zuständigen Abnahmestelle abzustimmen.
- Der Anwender hat dafür Sorge zu tragen, dass sein Kommunikationssystem die parametrisierte Response-Time einhält und diese kleiner gleich der halben Receive-Timeout ist. Falls nicht, muss die Worst-Case-Reaktion-Time für die Sicherheitstechnische Funktion auch dann geeignet sein, wenn die doppelte Receive-Timeout in die Worst-Case-Reaktion-Time-Berechnung eingehen würde.
- Wenn der Anwender nicht immer garantieren kann, dass sein Kommunikationssystem die parametrisierte Response-Time einhält, so muss er diese mit der vom System gemessenen Response-Time (Systemvariable der Verbindung) überwachen. Dabei darf es nur in seltenen Ausnahmefällen zu einer Überschreitung der gemessenen Response-Time über die halbe Receive-Timeout kommen. Alternativ kann der Anwender auch die doppelte Receive-Timeout in die Worst-Case-Reaktion-Time-Berechnung der Sicherheitstechnischen Funktion einfließen lassen.
- Betreibt der Anwender eine safe**ethernet**-Verbindung in einem störungsbehafteten Netzwerk, oder die parametrisierte ResponseTime wird nicht oder häufiger nicht eingehalten und/oder ein Cleanroom Profil verwendet, so wird das Cleanroom Profil von HIMA auf Grund der möglichen reduzierten Verfügbarkeit nicht empfohlen!
Soll safe**ethernet** unter diesen Bedingungen eingesetzt werden, muss die *ReceiveTMO* derart eingestellt werden, dass die Worst-Case-Reaktion-Time für die Sicherheitstechnische Funktion auch dann geeignet ist, wenn die doppelte *ReceiveTMO* in die Worst-Case-Reaktion-Time-Berechnung eingehen würde.
Für die Erhöhung der Verfügbarkeit der safe**ethernet** Verbindung könnte zum Beispiel der Faktor n in $ResponseTime \leq ReceiveTMO / n$, mit $n > 4$ parametrisiert werden. Wie groß n werden muss hängt von der erwünschten/ notwendigen Verfügbarkeit ab. Dabei sind dann die Eigenschaften des Übertragungssystems zu betrachten.

4.3 HIMA System Mengengerüst für safeethernet

Die HIMA Systeme HIMax und HIQuad X unterstützen das safeethernet Protokoll mit den folgenden Eigenschaften.



Element	HIMax	HIQuad X	Beschreibung
Systemansicht			Bilder sind exemplarisch für die jeweilige Systemfamilie. Zu sehen sind eine HIMax und eine HIQuad X H51X
Modul/Steuerung	pro HIMax 1 ... 4 X-CPU 01 1 ... 2 X-CPU 31	pro H41X/H51X: 1 ... 2 F-CPU 01	safeethernet wird auf dem sicherheitsbezogenen CPU-Modul ausgeführt.
Ethernet Schnittstellen:	X-CPU 01: 1 GBit/s X-CPU 31: 100 Mbit/s X-COM 01: 100 Mbit/s	F-CPU 01: 100 Mbit/s F-COM 01: 100 Mbit/s	Die verwendeten Ethernet-Schnittstellen sind simultan auch für andere Protokolle nutzbar.
Verbindungen:	255	128	safeethernet Verbindungen zu anderen Steuerungen und Remote I/Os.
Verbindungen zwischen zwei Steuerungen	1 vor CPU BS V6 64 ab CPU BS V6	64	safeethernet Verbindungen
Redundante Verbindungen	255	128	2 Kanal Betrieb Redundante safeethernet Verbindungen zwischen HIMA Steuerungen sind im safeethernet Editor einstellbar.
Prozessdatenmenge pro Verbindung	1100 Bytes	1100 Bytes	pro safeethernet Verbindung.
n. a: nicht anwendbar			

Tabelle 35: **safeethernet** Protokoll für HIMax und HIQuad X

Die HIMA Systeme HIMatrix unterstützen das **safeethernet** Protokoll mit den folgende Eigenschaften.


Element	HIMatrix	Beschreibung
Systemansicht		Bild ist exemplarisch für die jeweilige Systemfamilie. Zu sehen ist eine F30.
Modul/Steuerung	Integriertes CPU-Modul der Steuerung	safeethernet wird auf dem sicherheitsbezogenen CPU-Modul ausgeführt.
Ethernet Schnittstellen:	100 Mbit/s	Die verwendeten Ethernet-Schnittstellen sind simultan auch für andere Protokolle nutzbar.
Verbindungen:	128 vor CPU BS V12 255 ab CPU BS V12	safeethernet Verbindungen zu anderen Steuerungen und Remote I/Os.
Verbindungen zwischen zwei Steuerungen	1 vor CPU BS V10 64 ab CPU BS V10	safeethernet Verbindungen
Redundante Verbindungen	128 vor CPU BS V12 255 ab CPU BS V12	2 Kanal Betrieb Redundante safeethernet Verbindungen zwischen HIMA Steuerungen sind im safeethernet Editor einstellbar.
Prozessdatenmenge pro Verbindung	1100 Bytes	pro safeethernet Verbindung.
n. a: nicht anwendbar		

Tabelle 36: **safeethernet** Protokoll für HIMatrix

4.4 Konfiguration einer redundanten safeethernet Verbindung

In diesem Beispiel wird eine redundante safeethernet Verbindung zwischen zwei HIMA Steuerungen konfiguriert.

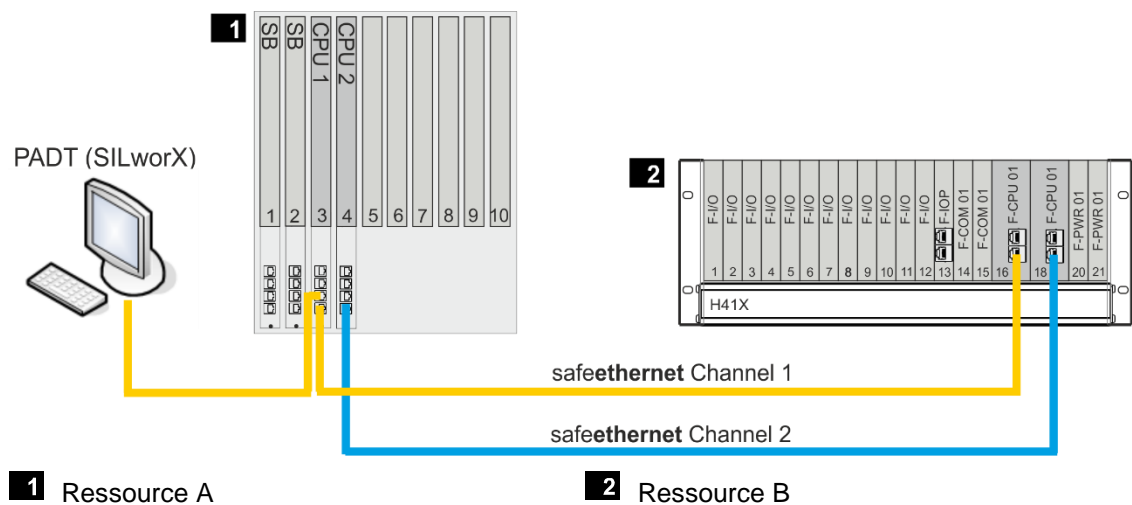


Bild 5: Aufbau zur Konfiguration einer redundanten Verbindung

- i** HIMA empfiehlt, bei einer redundanten safeethernet Verbindung die beiden Transportwege (Kanal 1 und Kanal 2) über zwei vollständig getrennte Ethernet-Netzwerke zu führen. Dabei müssen Bandbreite und Verzögerung auf den jeweiligen Transportwegen annähernd identisch sein.

4.4.1 safeethernet Verbindung erstellen

Im safeethernet Editor eine safeethernet Verbindung zwischen der Ressource A und der Ressource B erstellen.

Den safeethernet Editor der Ressource A öffnen

1. Im Strukturbaum **Konfiguration, Ressource** öffnen.
2. Rechtsklick auf **safeethernet** und im Kontextmenü **Edit** wählen.
 - ☒ In der Objektauswahl befinden sich die *Ressource B*.

Erstellen der safeethernet Verbindung zur Ressource B

1. In der Objektauswahl auf die **Ressource B** klicken und per Drag&Drop auf eine freie Stelle im Arbeitsbereich des safeethernet Editors ziehen.
 - ☒ Es öffnet sich ein Dialogfenster um einen Namen für die safeethernet Verbindung festzulegen. Dieser Name muss eindeutig sein.

- i** Der umgekehrte Kommunikationspfad wird im safeethernet Editor der Ressource B automatisch erstellt.

Konfigurieren der safeethernet Verbindung

1. **Ethernet-Schnittstellen Kanal 1** für Ressource A und Ressource B auswählen.
2. **Ethernet-Schnittstellen Kanal 2** für Ressource A und Ressource B auswählen.
3. **Netzwerk-Profil** (z. B. Fast&Noisy) der safeethernet Verbindung auswählen.
4. **Receive Timeout** und **Response Time** berechnen und eintragen (siehe Kapitel 4.8).

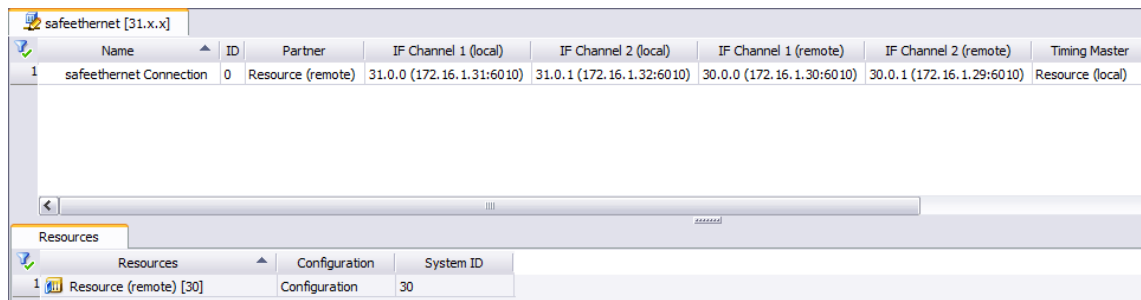


Bild 6: Ansicht im safeethernet Editor

4.4.2 Konfiguration im safeethernet Verbindungseditor

Die Prozessvariablen im safeethernet Verbindungseditor verbinden.

i

Es können nur Globale Variablen aus dem Kontext der Konfiguration verwendet werden, nicht aus dem Kontext des Projekts oder der Ressource!

Öffnen des Verbindungseditors

1. Rechtsklicken auf die erstellte safeethernet Verbindung und Kontextmenü öffnen.
2. Im Kontextmenü **Edit** wählen, um den Verbindungseditor der safeethernet Verbindung zu öffnen.
3. Register **Ressource A<-> Ressource B** wählen.
4. In der Objektauswahl eine **Globale Variable** wählen und per Drag&Drop in den Bereich **Ressource A --> Ressource B** oder in den Bereich **Ressource B --> Ressource A** je nach gewünschter Transportrichtung ziehen.
5. Diesen Schritt für weitere Globale Variablen wiederholen.

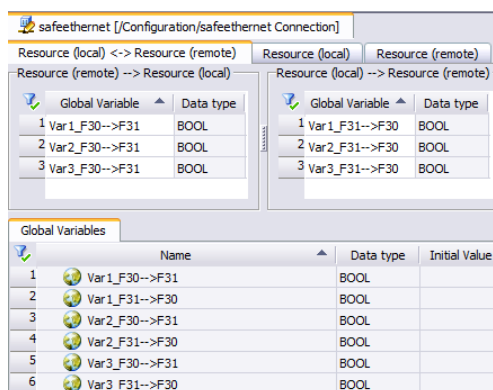


Bild 7: Ansicht im safeethernet Verbindungseditors

i

Die Systemvariablen der safeethernet Verbindung im Anwenderprogramm auswerten!
In den jeweiligen Subregistern der *Ressource A* und *Ressource B* sollten mindestens den Systemvariablen *Verbindungszustand*, *Qualität Kanal 1* und *Qualität Kanal 2* Globale Variablen zuordnet werden, um diese im Anwenderprogramm auszuwerten.

safeethernet Verbindung verifizieren

1. Im Strukturbaum **Konfiguration, Ressource, safeethernet** selektieren.
2. Rechtsklick und im Kontextmenü **Verifikation** wählen.
3. Einträge im Logbuch sorgfältig überprüfen, gegebenenfalls Fehler korrigieren.

i

Die Konfiguration der **safeethernet** Verbindung muss mit dem Anwenderprogramm der Ressource A und der Ressource B neu kompiliert und in die Steuerungen übertragen werden, bevor diese für die Kommunikation der HIMA Steuerung wirksam werden.

4.4.3 Prüfung der safeethernet Kommunikation

Im Control Panel die Anzeigen mit **Reset safeethernet Statistik** auf Null zurücksetzen.

Zur Prüfung der korrekten Einrichtung einer redundanten **safeethernet** Verbindung sollte eine redundante Verbindung getrennt und wieder verbunden werden und danach die andere. Dabei dürfen keine Fehler in der **safeethernet** Kommunikation auftreten. Hierbei die Werte von Qualität Kanal 1 und Qualität Kanal 2 beobachten.

i

Weitere Ursachen für *Fehlerhafte Nachrichten* und *Wiederholungen*!

Den korrekten Netzwerkaufbau prüfen (z. B. Leitungen, Switches, PCs).
Wird das Ethernet-Netzwerk nicht exklusiv für **safeethernet** verwendet, ist zudem die Netzerklastung (Wahrscheinlichkeit von Datenkollisionen) zu prüfen.

4.5 safeethernet-Verbindungsübersicht

In der **safeethernet** Verbindungsübersicht einer Ressource werden alle konfigurierten **safeethernet** Verbindungen gelistet. Zudem können hier neue **safeethernet** Verbindungen erzeugt werden.

Öffnen der safeethernet Verbindungsübersicht

1. Im Strukturbaum **Konfiguration, Ressource** öffnen.
2. Rechtsklick auf **safeethernet** und im Kontextmenü **Edit** wählen.

In der **safeethernet** Verbindungsübersicht werden die folgenden **safeethernet** Protokoll-Parameter angezeigt:

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), siehe auch Kapitel 3.3.
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, siehe auch Kapitel 4.10.
Rsp t	Die <i>ResponseTime</i> ist die Zeit in Millisekunden (ms), die verstreicht, bis der Absender einer Nachricht die Empfangsbestätigung des Empfängers erhält, siehe auch Kapitel 4.8.3. Standardwert: 500 ms
Rcv TMO	Receive Timeout ist die Überwachungszeit auf Steuerung 1, innerhalb der eine korrekte Antwort von Steuerung 2 empfangen werden muss, siehe auch Kapitel 4.8.2. Standardwert: 1000 ms
Rsnd TMO	Resend Timeout ist die Überwachungszeit in ms auf Steuerung 1, innerhalb welcher Steuerung 2 den Empfang eines Datenpaketes bestätigt haben muss, ansonsten wird das Datenpaket wiederholt, siehe auch Kapitel 4.8.5.
Ack TMO	Acknowledge Timeout ist die Zeit in ms, nach der ein empfangenes Datenpaket von der CPU spätestens bestätigt werden muss, siehe auch Kapitel 4.8.6.
Prod Rate	Produktionsrate ist das kleinste Zeitintervall zwischen zwei Datenpaketen, siehe auch Kapitel 4.8.7.
Speicher	Anzahl der Datenpakete, die ohne Empfangsbestätigung versendet werden können, siehe auch Kapitel 4.8.8.


Parameter	Beschreibung
Verhalten	Verhalten der Import Variablen dieser safeethernet Verbindung bei Verbindungsunterbrechung.
	Initialwert verwenden Für die Import Variablen werden die Initialdaten verwendet.
	Prozesswert unbegrenzt einfrieren Die Import Variablen werden auf dem momentanen Wert eingefroren und bis zur erneuten Verbindungsaufnahme verwendet.
	Initialwert nach [ms] Eingabe: Doppelklick auf Feld und die Zeit in Millisekunden eingeben. Die Import Variablen 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.
<div style="text-align: center;">  ⚠ VORSICHT Für sicherheitsbezogene Funktionen, die über safeethernet realisiert werden, darf nur die Einstellung Initialwert verwenden benutzt werden. </div>	
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.	Funktion ist nur für Verbindungen zu X-OPC Server nutzbar und veränderbar.
Codegen	Um safeethernet Verbindungen mit Kommunikationspartnern vor SILworX V6 betreiben zu können, muss die Codegenversion auf vor V6 ausgewählt werden. Ab V6: safeethernet Verbindung reloadbar. Vor V6: safeethernet Verbindung nicht reloadbar. Standardwert: ab V6

Tabelle 37: Parameter **safeethernet** Protokoll

Objektauswahl

Die Objektauswahl stellt alle Ressourcen innerhalb dieses Projektes zur Verfügung, mit denen diese Ressource über **safeethernet** verbunden werden kann.

i

Für **safeethernet** Verbindungen zu Ressourcen außerhalb eines Projektes steht die Funktion Archivieren zur Verfügung (siehe Kapitel 4.13).

4.6 Verbindungs-Editor einer safeethernet Verbindung

Der **safeethernet** Editor hat immer den Bezug auf die lokale Ressource, aus welcher der **safeethernet** Editor gestartet wurde.

Öffnen der safeethernet Verbindungsübersicht

1. Im Strukturbaum **Konfiguration, Ressource** öffnen.
2. Rechtsklick auf **safeethernet** und im Kontextmenü **Edit** wählen.

Öffnen des Verbindungs-Editors einer safeethernet Verbindung

1. Rechtsklick auf die gewünschte **safeethernet** Verbindung und Kontextmenü öffnen.
2. **Edit** wählen.
 - ☒ Die **safeethernet** Editor beinhaltet die drei Register *Peer1<->Peer2*, *Peer1* und *Peer2*.

4.6.1 Register: *Ressource A<->Ressource B*

Das Register *Ressource A<->Ressource B* ist in zwei Bereiche *Ressource B-->Ressource A* und *Ressource A-->Ressource B* für die jeweilige gewünschte Transportrichtung aufgeteilt.

In diese beiden Bereiche können aus der Objektauswahl *Globale Variablen* per Drag&Drop gezogen werden.

4.6.2 Register: *Ressource A*

Das Register *Ressource A* enthält die Register *Systemvariablen* und *Fragment-Definitionen: Ressource B-->Ressource A*, siehe Kapitel 4.6.3.1 und Kapitel 4.6.3.2.

4.6.3 Register: *Ressource B*

Das Register *Ressource B* enthält die Register *Systemvariablen* und *Fragment-Definitionen: Ressource A-->Ressource B*, siehe Kapitel 4.6.3.1 und Kapitel 4.6.3.2.

4.6.3.1 Register: Systemvariablen

Die **safeethernet** Verbindung 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 verführten Nachrichten seit Reset der Statistik. Die verführten Nachrichten werden in der Early Queue gespeichert. Siehe auch Kapitel 4.8.8.
Fehlerhafte Nachrichten	UDINT	R	Anzahl verworfener Nachrichten seit Reset der Statistik.

Name	Datentyp	R/W	Beschreibung																		
Frame-Nr.	UDINT	R	Sendungszähler (Umlaufend).																		
Kanalzustand	USINT	R	<div>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></div>	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	<div>Die Kanal Latenz 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. Letzte Kanal Latenz und Mittlere Kanal Latenz sind dann 0.</div>																		
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).																		
Qualität Kanal 1	BYTE	R	<div>Qualität 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></div>	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	Qualität des redundanten Transportweges, siehe Qualität Kanal 1 (Haupt-Transportweg).																		
Receive Timeout	UDINT	R	Zeit in Millisekunden (ms) auf Steuerung 1, innerhalb der eine gültige Antwort von Steuerung 2 empfangen werden muss, siehe auch Kapitel 4.8.2.																		
Response Time	UDINT	R	Zeit in Millisekunden (ms) bis zur Empfangsbestätigung der letzten Nachricht beim Absender.																		
safe ethernet Statistik zurücksetzen	BYTE	W	<div>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></div>	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	<div>Durch die Änderung der safeethernet Konfiguration entsteht eine Dualkonfiguration. Alte Signatur der safeethernet Konfiguration.</div>																		
Signatur N+1	UDINT	R	Neue Signatur der safe ethernet Konfiguration.																		

Name	Datentyp	R/W	Beschreibung	
Transport-Steuerung Kanal1	BYTE	W	Transportsteuerung von Kanal1.	
			Bit 0	Funktion
			FALSE	Transportweg 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.	
Verbindungssteuerung	WORD	W	Mit dieser Systemvariablen kann die safeethernet Verbindung vom Anwenderprogramm gesteuert werden.	
			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.	
			Status/Wert	Beschreibung
			Closed (0)	Verbindung ist geschlossen und es wird auch nicht versucht sie zu öffnen.
			Try_open (1)	Verbindung wird versucht zu öffnen, sie ist jedoch noch nicht geöffnet. 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).
Reload Zustand	UINT	R	Reload Zustand dieser safeethernet Verbindung, siehe auch Status <i>Reload</i> in Kapitel 4.11.1. unknown: 0x0000 up to date: 0x0001 updated: 0x0002 outdated: 0x0003	

Name	Datentyp	R/W	Beschreibung										
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).										
Zustand des Red.-Kanal	USINT	R	<div>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.</div> <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 38: Register Systemvariablen des safeethernet-Editors

4.6.3.2 Register: Fragment-Definitionen

Das Register *Fragment-Definitionen* enthält die Status und Parameter des versendeten Fragments von der gegenüberliegenden Steuerung.

Hier kann die für diese Steuerung (oder X-OPC-Server) erforderliche Aktualisierungsrate der empfangenen Fragmente aus allen verbundenen Steuerungen eingestellt werden. Die Einstellung der Priorität ist hauptsächlich für X-OPC-Server gedacht, die eine große Datenmenge von verschiedenen Steuerungen verarbeiten.

Name	Datentyp	R/W	Beschreibung
Die folgenden Status und Parameter können globalen Variablen zugewiesen und im Anwenderprogramm verwendet werden			
Fragment-Definition	-	-	<p>In der Spalte Priorität wird eingestellt, wie oft dieses Fragment im Verhältnis zu den anderen Fragmenten empfangen werden soll. Ein Fragment einer HIMax, HIQuad X und HIMatrix ist ein Fragment ≤ 1100 Byte. Standardeinstellung: Priorität 1 Wertebereich: Priorität 1 (höchste) bis 65 535 (niedrigste).</p>
Fragment-Versions-Zustand	UINT	R	<p>Reload-Versionszustand dieses safeethernet Fragments, siehe auch Status <i>Reload</i> in Kapitel 4.11.1.</p> <p>Unknown: 0x0000 up to date: 0x0001 updated: 0x0002 outdated: 0x0003</p>
Fragment-Zeitstempel [ms]	UDINT	R	Millisekunden Anteil des Zeitstempels (aktuelle Systemzeit).
Fragment-Zeitstempel [s]	UDINT	R	Sekunden Anteil des Zeitstempels (aktuelle Systemzeit).

Name	Datentyp	R/W	Beschreibung	
Fragment-Zustand	UINT	R		
			Status	Beschreibung
			0	CLOSED: Verbindung ist geschlossen.
			1	TRY OPEN: Verbindung wird versucht zu öffnen, sie ist jedoch noch nicht geöffnet.
			2	CONNECTED: Die Verbindung steht und aktuelle Fragment-Daten wurden empfangen (vgl. Zeitstempel). Solange keine Fragment-Daten empfangen werden, bleibt der Fragment-Zustand beim Verbindungsaufbau auf TRY_OPEN.
Der Verbindungszustand des safeethernet Editors wird auf CONNECTED gesetzt sobald die Verbindung geöffnet ist. Im Gegensatz zum Fragment-Zustand müssen hier noch keine Daten ausgetauscht worden sein.				

Tabelle 39: Register Fragment-Definitionen

4.7 Netzwerkstrukturen für safeethernet Verschaltungen

In diesem Kapitel werden verschiedene Kombinationen für safeethernet Verschaltungen dargestellt.

i

HIMA empfiehlt für die Reduzierung von Security-Risiken den Aufbau eines Safety-Netzwerks über die CPU-Module und ein davon getrenntes Standard-Netzwerk über die COM-Module. Das Standard-Netzwerk dient der Verbindung zu nicht-sicherheitsbezogenen Komponenten wie z. B. X-OPC Server.

Eine safeethernet Verbindung ist logisch immer eine Verbindung zwischen zwei HIMA Systemen, die einkanalig oder zweikanalig konfiguriert werden kann. Die verfügbaren Ethernet-Schnittstellen für eine safeethernet Verbindung werden immer in Bezug auf die Ressource angezeigt, für die der safeethernet Editor gestartet wurde. Alle verfügbaren Ethernet-Schnittstellen einer Steuerung werden im Dropdown-Menü des jeweiligen Parameters **IF Kanal...** angezeigt.

Element	Beschreibung
IF Kanal1 (lokal)	Ethernet-Schnittstelle der Ressource, deren safeethernet-Editor geöffnet wurde.
IF Kanal2 (lokal)	
IF Kanal1 (fern)	Ethernet-Schnittstelle der Partner-Ressource.
IF Kanal2 (fern)	

Tabelle 40: Verfügbare Ethernet-Schnittstellen

i

HIMA empfiehlt, einen Netzwerkfachmann mit der Auslegung der Netzwerkstrukturen und der Berechnung der maximalen Latenzzeit zu beauftragen. Ein fehlerhafter Aufbau eines Netzwerks kann dazu führen, dass ein Teil oder das gesamte HIMA System abgeschaltet wird!

Gemäß der allgemein gültigen Regeln zur Erstellung von Ethernet-Netzwerken ist zu beachten, dass keine Netzschleifen entstehen. Datenpakete dürfen nur auf einem Weg zu einer Steuerung gelangen.

4.7.1 Mono safeethernet Verbindung (Kanal 1)

Für eine Mono-Verbindung die Ethernet-Schnittstellen *IF Kanal 1 (lokal)* und *IF Kanal 1 (fern)* in der Verbindung konfigurieren. Einen eventuell automatisch eingetragenen *IF Kanal 2* entfernen.

	Name	ID	Partner	IF Channel 1 (local)	IF Channel 2 (local)	IF Channel 1 (remote)	IF Channel 2 (remote)
1	safeethernet Connection	0	Resource (remote)	31.0.0 (172.16.1.31:6010)	None	30.0.0 (172.16.1.30:6010)	None
2	safeethernet Connection_RIO	0	HIMatrix F3 DIO 20/8 02_1	31.0.0 (172.16.1.31:6010)		31.200.0 (172.16.1.200:6010)	

Bild 8: safeethernet Übersicht des Beispiels in Bild 9

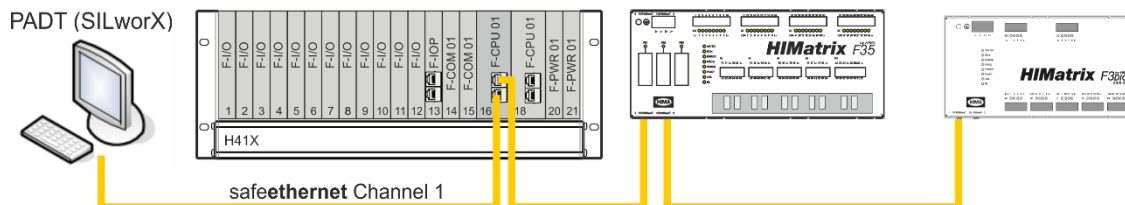


Bild 9: Mono safeethernet Verbindung (Kanal 1)

Alle HIMA Systeme die mit SILworX programmiert werden, sind für die mono safeethernet Verschaltung geeignet.

4.7.2 Redundante safeethernet Verbindung (Kanal 1 und Kanal 2)

Redundante safeethernet Transportwege zwischen zwei HIMA Steuerungen sind möglich. Für eine redundante Verbindung sind die folgenden Ethernet-Schnittstellen benutzbar:

- Die Ethernet-Schnittstellen *IF Kanal1 (lokal)* und *IF Kanal1 (fern)* für Kanal 1.
- Die Ethernet-Schnittstellen *IF Kanal2 (lokal)* und *IF Kanal2 (fern)* für Kanal 2.

i

Die redundanten Transportwege müssen soweit gleichartig sein, dass ihre Bandbreite und ihre Verzögerung annähernd identisch sind.

Sobald auf einem Transportweg der Versatz der empfangenen Messages zu groß wird, oder die Messages um mehr als die Response-Time verzögert ankommen, arbeitet die Transportweg-Diagnose nicht bestimmungsgemäß und interpretiert diese Verzögerungen als Fehler des Transportweges.

Zur Auswertung der Transportweg-Diagnose, siehe Systemvariablen *Zustand des Red.-Kanal* und *Kanalzustand*.

4.7.2.1 Redundante safeethernet Verbindung zu mehreren Systemen

Eine redundante Verbindung mit zwei getrennten logischen und physikalischen Transportwegen (Kanal 1 und Kanal 2) kann mit HIMA Steuerungen aufgebaut werden. Damit alle drei Steuerung gegenseitig safeethernet Daten austauschen können, muss zwischen diesen jeweils mindestens eine safeethernet Verbindung konfiguriert werden. Diese sieht in der safeethernet Übersicht exemplarisch wie in den nachfolgenden Bildern aus.

	Name	ID	Partner	IF Channel 1 (local)	IF Channel 2 (local)	IF Channel 1 (remote)	IF Channel 2 (remote)
1	HIMax <-> HIQuad X	0	HIMatrix	100.0.3 (172.16.1.100:6010)	100.0.4 (172.16.1.101:6010)	35.0.0 (172.16.1.31:6010)	35.0.1 (172.16.1.32:6010)
2	HIMax <-> HIQuad X	0	HIQuad X	100.0.3 (172.16.1.100:6010)	100.0.4 (172.16.1.101:6010)	41.1.16 (172.16.1.40:6010)	41.1.18 (172.16.1.41:6010)

Bild 10: HIMax Ressource: safeethernet Übersicht des Beispiels in Bild 12

	Name	ID	Partner	IF Channel 1 (local)	IF Channel 2 (local)	IF Channel 1 (remote)	IF Channel 2 (remote)
1	HIMax <-> HIQuad X	0	HIMatrix	41.1.16 (172.16.1.40:6010)	41.1.18 (172.16.1.41:6010)	100.0.3 (172.16.1.100:6010)	100.0.4 (172.16.1.101:6010)
2	HIQuad X <-> HIMatrix	0	HIMatrix	41.1.16 (172.16.1.40:6010)	41.1.18 (172.16.1.41:6010)	35.0.0 (172.16.1.31:6010)	35.0.1 (172.16.1.32:6010)
3	HIQuad X <-> Remote IO	0	HIMatrix F3 DIO 20/8 02_1	41.1.16 (172.16.1.40:6010)		41.200.0 (172.16.1.200:6010)	

Bild 11: HIQuad X Ressource: safeethernet Übersicht des Beispiels in Bild 12

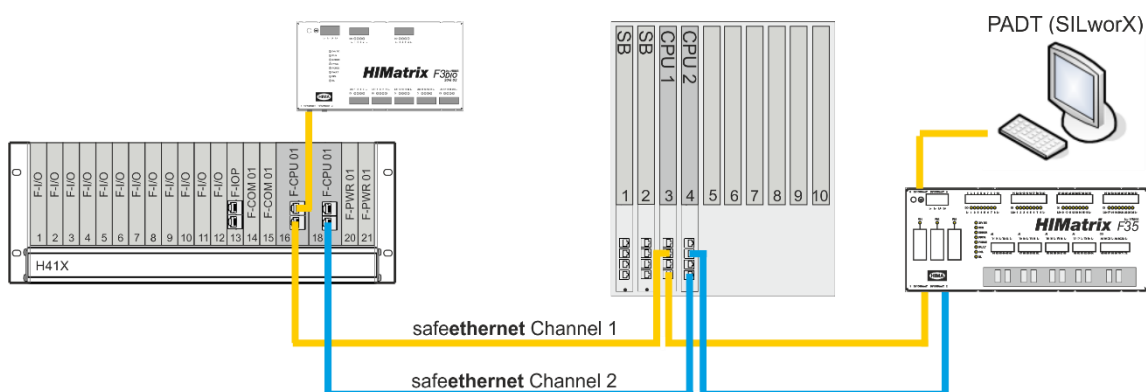


Bild 12: Parallele safeethernet Redundanz

Bei HIMatrix sind die Switchports durch VLAN voneinander zu trennen, siehe Kapitel 4.6.3.4. Remote I/Os sind für die parallele safeethernet **Verschaltung** nicht geeignet.

4.7.2.2 Redundanz über safeethernet Ring

Eine redundante Verbindung ist auch in einer Ring-Verschaltung nach IEC 62439-3 möglich. Die Datenpakete werden im ringförmigen Netzwerk doppelt, d. h. in beide Richtungen übertragen. So wird auch bei der Unterbrechung eines Kommunikationswegs an einer beliebigen Stelle im safeethernet Ring, die Übertragung sichergestellt.

Die safeethernet Verbindung muss in der Ring-Verschaltung über einen Ring-Switch erfolgen. Hierzu ist ein geeigneter Switch mit Ring-Management einzusetzen.

In einen safeethernet Ring können HIMax, HIQuad X und HIMatrix verschaltet werden. Diese Steuerungen benutzen hier jeweils nur eine IP-Adresse für die safeethernet Kommunikation.

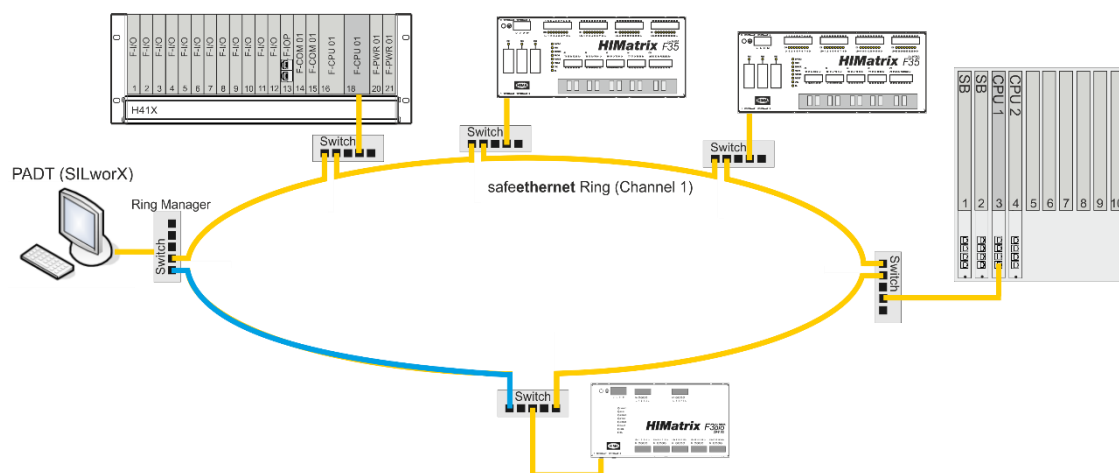


Bild 13: safeethernet Ring-Verschaltung

i

Von HIMA empfohlene Switches und Medienkonverter sind beim Support zu erfragen!

4.8 safeethernet Parameter

Die sicherheitsbezogene Kommunikation wird im **safeethernet** Editor eingerichtet. Dazu müssen die in diesem Kapitel beschriebenen Parameter parametrisiert werden.

Für die Berechnung der **safeethernet** Parameter *Receive Timeout* und *Response Time* gilt folgende Bedingung:

Die Kommunikations-Zeitscheibe muss ausreichend groß sein, um in einem CPU-Zyklus alle **safeethernet** Verbindungen abzuarbeiten, siehe Kapitel 7.1.

4.8.1 Berechnung einer geeigneten Watchdog-Zeit (max. Zykluszeit)

Eine konservative Berechnung der Watchdog-Zeit für das eingesetzte System (HIMax, HIMatrix oder HIQuad X) ist in dem jeweiligen Sicherheitshandbuch beschrieben.

Die maximalen Werte der Zykluszeit bei Reload sind von der eingestellten Watchdog-Zeit abhängig. Soll das System auf eine möglichst niedrige Watchdog-Zeit optimiert werden, ist der Wert der **eingestellten** Watchdog-Zeit in einer Messreihe immer weiter zu verringern.

In folgenden Fällen ist der HIMA Support hinzuzuziehen:

- Falls die Voraussetzungen für die im Sicherheitshandbuch beschriebene Strategie zur Ermittlung der Watchdog-Zeit nicht eingehalten werden können.
- Falls das Ergebnis nicht befriedigend ist.

HIMA Systeme lassen Einstellungen zu, die eine noch bessere Performance ermöglichen. Um diese Einstellungen zu ermitteln, sind tiefergehende Kenntnisse in verschiedenen Bereichen erforderlich.

4.8.2 Receive Timeout

ReceiveTMO ist die Überwachungszeit in Millisekunden (ms), innerhalb der eine korrekte Antwort des Kommunikationspartners empfangen werden muss.

Trifft innerhalb der *ReceiveTMO* keine korrekte Antwort des Kommunikationspartners ein, wird die sicherheitsbezogene Kommunikation geschlossen. Die Import-Variablen dieser **safeethernet** Verbindung verhalten sich gemäß dem eingestellten Parameter *Freeze-Daten bei Verbindungsverlust [ms]*.

Für sicherheitsbezogene Funktionen, die über **safeethernet** realisiert werden, darf nur die Einstellung **Verwende Initialdaten** benutzt werden.

Da die *ReceiveTMO* sicherheitsrelevant und Bestandteil der Worst Case Reaction Time T_R (maximale Reaktionszeit, siehe Kapitel 4.9.1ff) ist, muss die *ReceiveTMO* wie folgt berechnet und im **safeethernet** Editor eingetragen werden.

$$\text{ReceiveTMO} \geq 4 \cdot \text{Delay} + 5 \cdot \text{max. Zykluszeit}$$

Bedingung: Die Kommunikations-Zeitscheibe muss ausreichend groß sein, um in einem CPU-Zyklus alle **safeethernet** Verbindungen abzuarbeiten.

Delay: Verzögerung auf der Übertragungsstrecke, z. B. durch (Switch, Satellit usw.).

Max. Zykluszeit: Maximale Zykluszeit der beiden Steuerungen.

i

Eine Erhöhung der Verfügbarkeit der **safeethernet** Kommunikation kann über eine Erhöhung (z. B. Verdoppelung) der *ReceiveTMO* erreicht werden, sofern diese zum Ausführen der Sicherheitstechnischen Funktion (Worst-Case-Reaktion-Time) dann noch geeignet ist..

Der Anlagenhersteller sowie der Betreiber haben dafür Sorge zu tragen, dass die **safeethernet** Verbindung mindestens $\text{ReceiveTMO} \geq 2 \cdot \text{Response-Time}$ einhält.

4.8.3 ResponseTime

Die *ResponseTime* ist die Zeit in Millisekunden (ms), die verstreicht, bis der Absender einer Nachricht die Empfangsbestätigung des Empfängers erhält.

Für die Parametrierung unter Verwendung eines **safeethernet** Profils muss eine durch die physikalischen Gegebenheiten der Übertragungsstrecke erwartete *ResponseTime* vorgegeben werden.

Die vorgegebene *ResponseTime* hat Einfluss auf die Konfiguration aller Parameter der **safeethernet** Verbindung, die wie folgt berechnet wird:

$$\text{ResponseTime} \leq \text{ReceiveTMO} / n$$

$$n = 2, 3, 4, 5, 6, 7, 8 \dots$$

Das Verhältnis der *ReceiveTMO* und der *ResponseTime* beeinflusst die Fähigkeit zur Fehlertoleranz, z. B. bei Paketverlusten (Wiederholung von verloren gegangenen Datenpaketen) oder Verzögerungen auf dem Übertragungsweg.

In einem Netzwerk, in dem es zu Paketverlusten kommen kann, muss die folgende Bedingung erfüllt sein:

$$[2,5 * \text{max. Zykluszeit} + 2 * \text{Delay}] \leq \text{min. Response Time} \leq [\text{ReceiveTMO} / 2]$$

Ist diese Bedingung erfüllt, kann der Verlust wenigstens eines Datenpaketes abgefangen werden, ohne dass die **safeethernet** Verbindung unterbrochen wird.

i

Ist diese Bedingung nicht erfüllt, kann die Verfügbarkeit einer **safeethernet** Verbindung nur in einem kollisions- und störungsfreien Netzwerk garantiert werden. Dies bedeutet jedoch kein Sicherheitsproblem für das Prozessormodul!

i

Es muss sichergestellt sein, dass die Übertragungsstrecke die parametrisierte *Response-Time* einhält!

Falls dies nicht immer garantiert werden kann, steht zur Überwachung der *Response-Time* eine entsprechende Systemvariable der **safeethernet** Verbindung zur Verfügung. Kommt es öfter zu einer Überschreitung der parametrisierten *Response-Time*, wird dringend empfohlen deren Wert zu erhöhen.

Die *ReceiveTMO* ist der neu parametrisierten *Response Time* anzupassen.

Der Anlagenhersteller sowie der Betreiber haben dafür Sorge zu tragen, dass die **safeethernet** Verbindung mindestens $\text{ReceiveTMO} \geq 2 * \text{Response-Time}$ einhält.

4.8.4 Sync/Async

Sync Wird zur Zeit nicht unterstützt.

Async Ist die Standardeinstellung.

Bei der Einstellung *Async* empfängt die **safeethernet** Protokolleinstanz in der Input-Phase der CPU und sendet gemäß ihren Senderegeln in der Output-Phase der CPU.

4.8.5 ResendTMO

ResendTMO kann nicht manuell eingegeben werden, sondern wird aus dem Profil und der Response-Time berechnet.

Überwachungszeit in Millisekunden (ms) auf Steuerung 1, innerhalb welcher Steuerung 2 den Empfang eines Datenpaketes bestätigt haben muss, ansonsten wird das Datenpaket wiederholt.

**Automatische Berechnung nach folgender Regel:
 $\text{ResendTMO} \leq \text{Receive-Timeout}$**

Bei unterschiedlicher Konfiguration der *Resend-Timeout* bei den Kommunikationspartnern bestimmt der aktive Protokollpartner (kleinere System-ID) den tatsächlichen Wert der *Resend-Timeout* der Protokollverbindung.

4.8.6 Acknowledge Timeout

AckTMO kann nicht manuell eingegeben werden, sondern wird aus dem Profil und der Response-Time berechnet.

AckTMO ist die Zeit, nach der ein empfangenes Datenpaket von der CPU spätestens bestätigt werden muss.

Für ein schnelles Netzwerk ist *AckTMO* null, d. h. der Empfang eines Datenpaketes wird sofort bestätigt. Für ein langsames Netzwerk (z. B. Telefonmodemstrecke) ist *AckTMO* größer null. In diesem Fall wird versucht, die Bestätigungsmeldung zusammen mit Prozessdaten zu übermitteln, um die Netzbelastung durch Vermeidung von Adressierungs- und Sicherungsblöcken zu reduzieren.

Automatische Berechnung nach folgenden Regeln:

- **$\text{AckTMO} \text{ muss } \leq \text{Receive-Timeout} \text{ sein.}$**
- **$\text{AckTMO} \text{ muss } \leq \text{Resend-Timeout} \text{ sein, wenn } \text{Production-Rate} > \text{Resend-Timeout} \text{ ist.}$**

4.8.7 Production Rate

ProdRate kann nicht manuell eingegeben werden, sondern wird aus dem Profil und der Response-Time berechnet.

Kleinstes Zeitintervall in Millisekunden (ms) zwischen zwei Datenpaketen.

Das Ziel von *Prod.-Rate* ist, die Menge an Datenpaketen auf ein Maß zu begrenzen, welches einen (langsamen) Kommunikationskanal nicht überlastet. Dadurch wird eine gleichmäßige Auslastung des Übertragungsmediums erreicht und der Empfang veralteter Daten auf der Empfängerseite vermieden.

Automatische Berechnung nach folgenden Regeln:

- **$\text{ProdRate} \leq \text{Receive-Timeout}$**
- **$\text{ProdRate} \leq \text{Resend-Timeout}$, wenn $\text{Acknowledge-Timeout} > \text{Resend-Timeout}$.**

i

Eine Production Rate von null bedeutet, dass mit jedem Zyklus des Anwenderprogramms Datenpakete übertragen werden können.

4.8.8 Speicher

Speicher kann nicht manuell eingegeben werden, sondern wird aus dem Profil und der Response-Time berechnet.

Speicher (Queue-Tiefe) ist die Anzahl der Datenpakete, die ausgesendet werden können, ohne auf deren Empfangsbestätigung warten zu müssen. Der Wert ist abhängig von der Übertragungskapazität des Netzwerkes und möglichen Verzögerungen durch Netzwerklaufzeiten.

Alle **safeethernet** Verbindungen teilen sich den zur Verfügung stehenden Message-Speicher in der CPU.

4.9 Maximale Reaktionszeit für safeethernet

In den Beispielen ab Kapitel 4.9.3 gelten die Formeln für die Berechnung der maximalen Reaktionszeit im Fall einer Verbindung mit HIMatrix Steuerungen nur dann, wenn auf diesen die Sicherheitszeit = 2 * Watchdog-Zeit eingestellt ist. Für HIMax und HIQuad X Steuerungen gelten diese Formeln immer.

i

Die zulässige maximale Reaktionszeit ist abhängig vom Prozess und ist mit der abnehmenden Prüfstelle abzustimmen.

Die folgende Tabelle beschreibt die in SILworX für die Berechnung der maximalen Reaktionszeit zu berücksichtigenden Parameter und Bedingungen:

Begriffe	Beschreibung
ReceiveTMO	Überwachungszeit in der Steuerung 1 (PES 1), in der eine gültige Antwort von der Steuerung 2 (PES 2) empfangen werden muss. Nach Ablauf der Zeit wird die sicherheitsbezogene Kommunikation andernfalls geschlossen.
Production Rate	Mindestabstand zwischen zwei Datensendungen.
Watchdog-Zeit	Maximal erlaubte Dauer eines RUN-Zyklus in einer Steuerung. Die Dauer des RUN-Zyklus hängt von der Komplexität des Anwenderprogramms und der Anzahl der safeethernet Verbindungen ab. Die Watchdog-Zeit ist in den Eigenschaften der Ressource einzutragen.
Worst Case Reaction Time	Maximale Reaktionszeit für die Übertragung einer Signaländerung am physikalischen Eingang (In) eines PES 1 bis zur Signaländerung am physikalischen Ausgang (Out) eines PES 2.
Delay	Verzögerung einer Übertragungsstrecke z. B. bei Modem- oder Satellitenverbindung. Bei direkter Verbindung kann zunächst eine Verzögerung von 2 ms angenommen werden. Die tatsächliche Verzögerung der Übertragungsstrecke kann von dem zuständigen Netzwerkadministrator ausgemessen werden.

Tabelle 41: Beschreibung safeethernet Parameter und Bedingungen

Für die Berechnungen der zulässigen maximalen Reaktionszeiten gelten folgende Bedingungen:

- Die Signale, die mit safeethernet übertragen werden, müssen in den jeweiligen Steuerungen innerhalb eines CPU-Zyklus verarbeitet werden.
- Die Reaktionszeiten der Sensoren und Aktoren sind zusätzlich zu addieren.

Die Berechnungen gelten auch für Signale in umgekehrter Richtung.

i

HIMA Systeme lassen Einstellungen zu, die eine noch bessere Performance ermöglichen. Um diese Einstellungen zu ermitteln, sind tiefergehende Kenntnisse in verschiedenen Bereichen erforderlich.

4.9.1 Maximale Reaktionszeit zweier HIMax Steuerungen

Maximale Reaktionszeit T_R („Worst Case“) vom Wechsel eines Gebers der Steuerung 1 (In) bis zur Reaktion des Ausgangs (Out) der Steuerung 2 wie folgt berechnen:

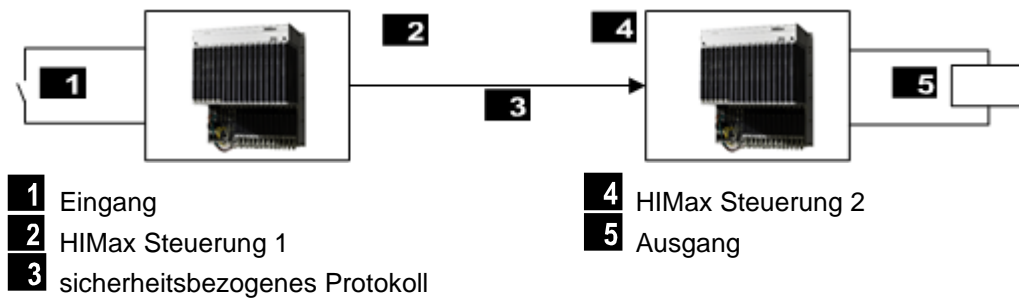


Bild 14: Reaktionszeit bei Verbindung zweier HIMax Steuerungen

$$T_R = t_1 + t_2 + t_3$$

T_R : Worst Case Reaction Time

t_1 : Sicherheitszeit der HIMax Steuerung 1.

t_2 : *ReceiveTMO*

t_3 : Sicherheitszeit der HIMax Steuerung 2.

4.9.2 Maximale Reaktionszeit zweier HIQuad X Steuerungen

Maximale Reaktionszeit T_R („Worst Case“) vom Wechsel eines Gebers der Steuerung 1 (In) bis zur Reaktion des Ausgangs (Out) der Steuerung 2 wie folgt berechnen:

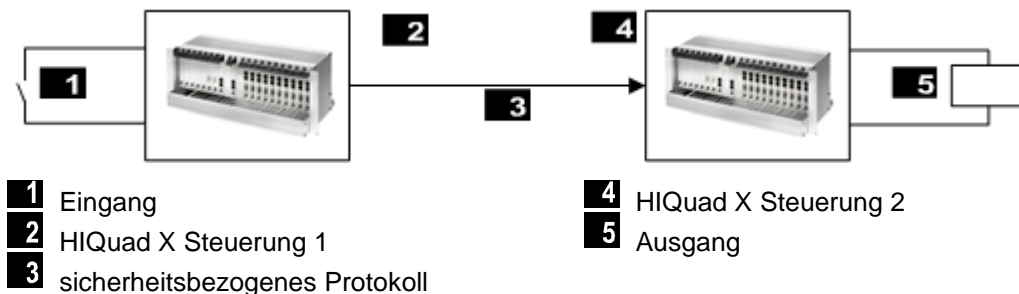


Bild 15: Reaktionszeit bei Verbindung zweier HIQuad X Steuerungen

$$T_R = t_1 + t_2 + t_3$$

T_R : Worst Case Reaction Time

t_1 : Sicherheitszeit der HIQuad X Steuerung 1.

t_2 : *ReceiveTMO*

t_3 : Sicherheitszeit der HIQuad X Steuerung 2.

4.9.3 Maximale Reaktionszeit einer HIMax mit einer HIMatrix Steuerung

Maximale Reaktionszeit T_R („Worst Case“) vom Wechsel eines Gebers (In) der HIMax Steuerung bis zur Reaktion des Ausganges (Out) der HIMatrix Steuerung wie folgt berechnen:

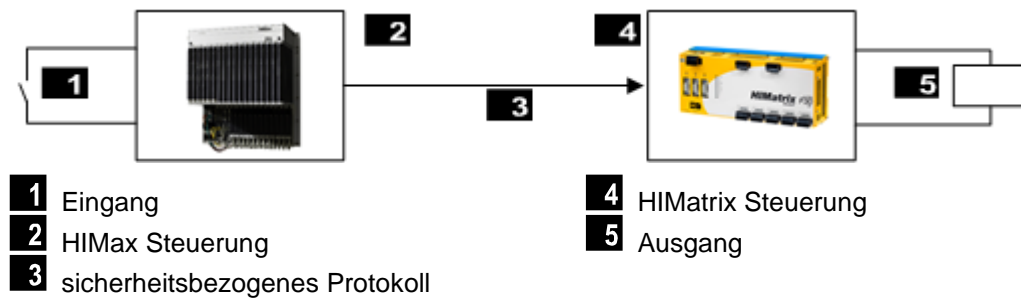


Bild 16: Reaktionszeit bei Verbindung einer HIMax mit einer HIMatrix Steuerung

$$T_R = t_1 + t_2 + t_3$$

T_R : Worst Case Reaction Time

t_1 : Sicherheitszeit der HIMax Steuerung.

t_2 : ReceiveTMO

t_3 : 2 * Watchdog-Zeit der HIMatrix Steuerung.

4.9.4 Maximale Reaktionszeit einer HIQuad X mit einer HIMatrix Steuerung

Maximale Reaktionszeit T_R („Worst Case“) vom Wechsel eines Gebers (In) der HIQuad X Steuerung bis zur Reaktion des Ausganges (Out) der HIMatrix Steuerung wie folgt berechnen:

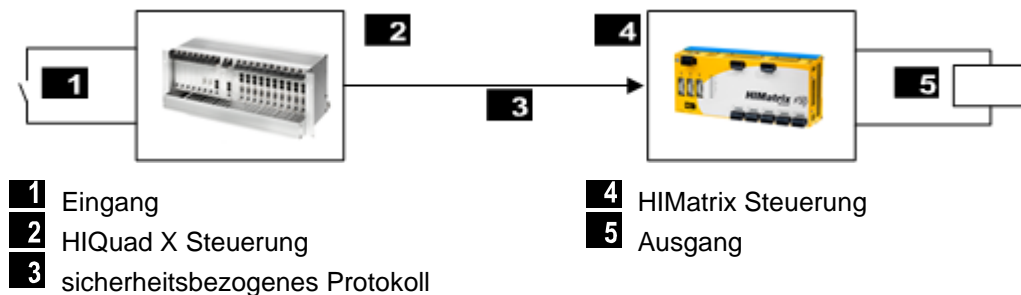


Bild 17: Reaktionszeit bei Verbindung einer HIQuad X mit einer HIMatrix Steuerung

$$T_R = t_1 + t_2 + t_3$$

T_R : Worst Case Reaction Time

t_1 : Sicherheitszeit der HIQuad X Steuerung.

t_2 : ReceiveTMO

t_3 : 2 * Watchdog-Zeit der HIMatrix Steuerung.

4.9.5 Maximale Reaktionszeit einer HIMax mit zwei HIMatrix Steuerungen oder Remote I/Os

Maximale Reaktionszeit T_R („Worst Case“) vom Wechsel eines Gebers (In) in der ersten HIMatrix Steuerung oder in Remote I/O (z. B. F3 DIO 20/8 01) bis zur Reaktion des Ausgangs in der zweiten HIMatrix Steuerung oder in Remote I/O (Out) wie folgt berechnen:

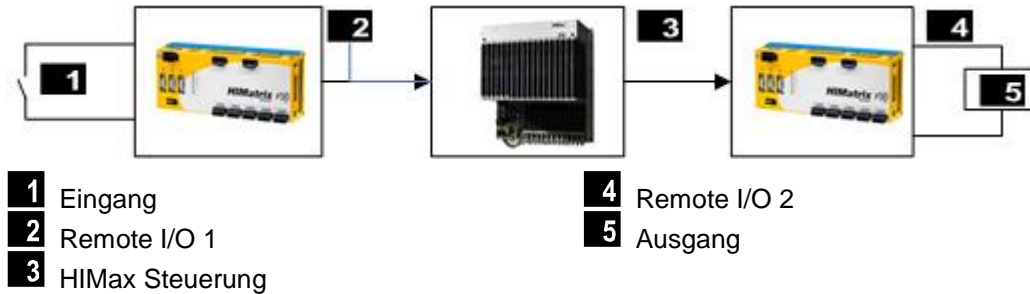


Bild 18: Reaktionszeit mit zwei Remote I/Os und einer HIMax Steuerung

$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

T_R : Worst Case Reaction Time

t_1 : 2 * Watchdog-Zeit der Remote I/O 1.

t_2 : *ReceiveTMO1*

t_3 : 2 * Watchdog-Zeit der HIMax Steuerung.

t_4 : *ReceiveTMO2*

t_5 : 2 * Watchdog-Zeit der Remote I/O 2.

i

Die beiden Remote I/Os 1 und 2 können auch identisch sein. Die Zeiten gelten auch dann, wenn statt einer Remote I/O eine HIMatrix Steuerung eingesetzt wird.

4.9.6 Maximale Reaktionszeit einer HIMatrix mit zwei HIMax Steuerungen

Maximale Reaktionszeit T_R („Worst Case“) vom Wechsel eines Gebers (In) in der ersten HIMax Steuerung bis zur Reaktion des Ausgangs (Out) in der zweiten HIMax Steuerung wie folgt berechnen:

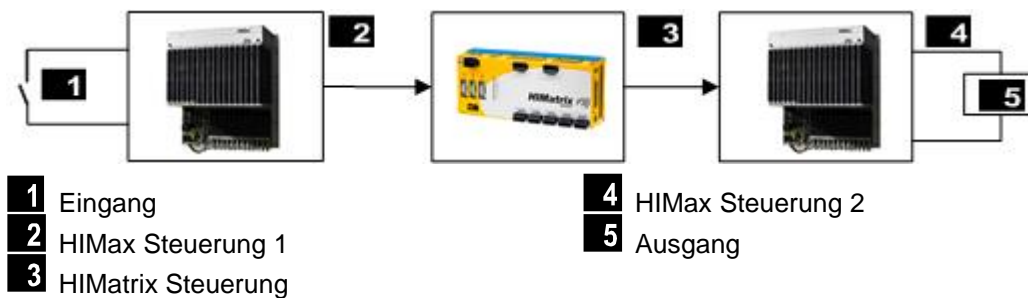


Bild 19: Reaktionszeit mit zwei HIMax Steuerungen und einer HIMatrix Steuerung

$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

T_R : Worst Case Reaction Time

t_1 : Sicherheitszeit des HIMax Steuerung 1.

t_2 : *ReceiveTMO1*

t_3 : 2 * Watchdog-Zeit des HIMatrix Steuerung.

t_4 : *ReceiveTMO2*

t_5 : Sicherheitszeit der HIMax Steuerung 2.

i

Die beiden HIMax Steuerungen 1 und 2 können auch identisch sein.

Die HIMatrix Steuerung kann auch eine HIMax Steuerung sein.

4.9.7 Maximale Reaktionszeit zweier HIMatrix Steuerungen

Die maximale Reaktionszeit T_R („Worst Case“) vom Wechsel eines Gebers der Steuerung 1 bis zur Reaktion des Ausgangs der Steuerung 2 kann wie folgt berechnet werden:

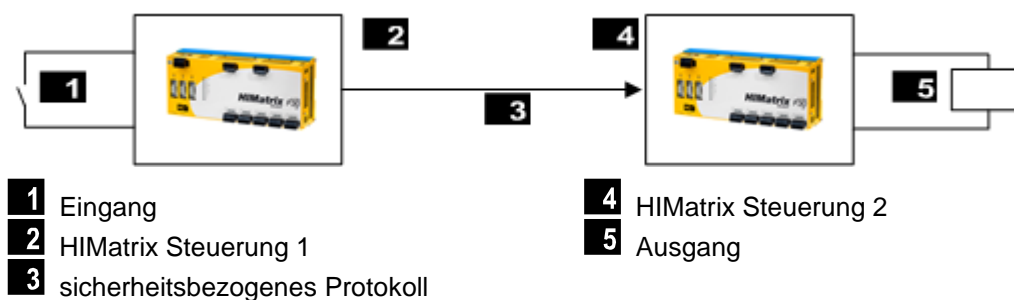


Bild 20: Reaktionszeit bei Verbindung zweier HIMatrix Steuerungen

$$T_R = t_1 + t_2 + t_3$$

T_R : Worst Case Reaction Time

t_1 : 2 * Watchdog-Zeit der HIMatrix Steuerung 1.

t_2 : *ReceiveTMO*

t_3 : 2 * Watchdog-Zeit der HIMatrix Steuerung 2.

4.9.8 Maximale Reaktionszeit einer HIMatrix Steuerung mit zwei Remote I/Os

Die maximale Reaktionszeit T_R vom Wechsel eines Gebers (In) der ersten HIMatrix- Steuerung oder Remote I/O (z. B. F3 DIO 20/8 01) bis zur Reaktion des Ausgangs der zweiten HIMatrix Steuerung oder Remote I/O (Out) kann wie folgt berechnet werden:

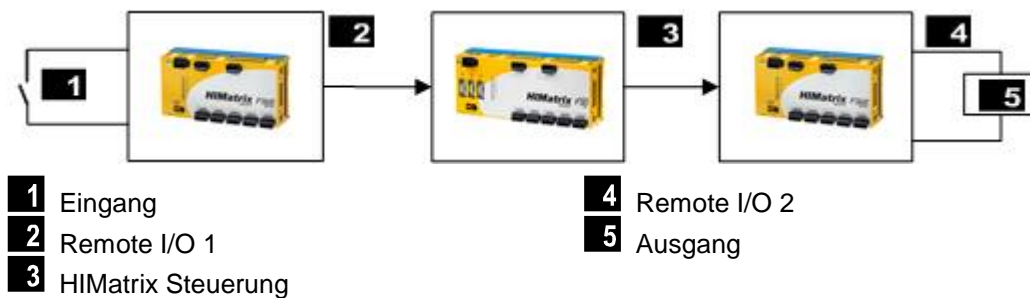


Bild 21: Reaktionszeit mit Remote I/Os

$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

T_R : Worst Case Reaction Time

t_1 : 2 * Watchdog-Zeit der Remote I/O 1.

t_2 : ReceiveTMO1

t_3 : 2 * Watchdog-Zeit der HIMatrix Steuerung.

t_4 : ReceiveTMO2

t_5 : 2 * Watchdog-Zeit der Remote I/O 2.

Anmerkung: Die beiden Remote I/Os 1 und 2 können auch identisch sein. Die Zeiten gelten auch dann, wenn statt eines Remote I/O eine HIMatrix Steuerung eingesetzt wird.

4.10 safeethernet Profile

safe**ethernet** Profile sind Kombinationen zueinander passender Parameter, die automatisch bei Auswahl eines der safe**ethernet** Profile eingestellt werden.

Für die Parametrierung muss nur die Receive-Timeout und die erwartete Response-Time einzeln konfiguriert werden.

Das Ziel eines safe**ethernet** Profils besteht darin, den Datendurchsatz im Netzwerk unter Berücksichtigung der physikalischen Gegebenheiten zu optimieren.

Voraussetzung für die Wirksamkeit der Optimierung sind die nachfolgenden Bedingungen:

- Kommunikations-Zeitscheibe muss ausreichend groß sein, damit in einem CPU-Zyklus alle safe**ethernet** Verbindungen abgearbeitet werden.
- Mittlere CPU Zykluszeit < Response-Time.
- Mittlere CPU Zykluszeit < ProdRate oder ProdRate = 0.

i

Unpassende Kombinationen von CPU-Zyklus, Kommunikations-Zeitscheibe, Response-Time und Production Rate werden bei der Codegenerierung und beim Download/Reload nicht abgelehnt. Diese Kombinationen können aber zu Störungen bis hin zum Ausfall der safe**ethernet** Kommunikation führen.

In den Control Panels der beiden Steuerungen die Anzeigen *Fehlerhafte Nachrichten* und *Wiederholungen* überprüfen.

Sechs safe**ethernet** Profile stehen zur Verfügung, aus denen das für die Übertragungsstrecke geeignete safe**ethernet** Profil ausgewählt werden kann.

HIMA empfiehlt, für eine safe**ethernet** Verbindung mit hoher Verfügbarkeit, die Profile *Fast&Noisy*, *Medium&Noisy* oder *Slow&Noisy* zu verwenden.

Fast & Cleanroom	Nur für störungsfreies Netzwerk empfohlen.
Fast & Noisy	Empfohlen, für eine hohe Verfügbarkeit der safe ethernet Verbindung.
Medium & Cleanroom	Nur für störungsfreies Netzwerk empfohlen.
Medium & Noisy	Empfohlen, für eine hohe Verfügbarkeit der safe ethernet Verbindung.
Slow & Cleanroom	Nur für störungsfreies Netzwerk empfohlen.
Slow & Noisy	Empfohlen, für eine hohe Verfügbarkeit der safe ethernet Verbindung.
Fixed	Alle Cleanroom-Profile haben ab V4 eine geänderte Berechnung. Soll ein Projekt von kleiner SILworX V4 konvertiert werden, muss der Parameter Profil auf <i>Fixed</i> gesetzt sein, um den CRC nicht zu ändern.

4.10.1 Profil I (Fast & Cleanroom)

1

HIMA empfiehlt, für eine safe**ethernet** Verbindung mit hoher Verfügbarkeit, die Profile *Fast&Noisy*, *Medium&Noisy* oder *Slow&Noisy* zu verwenden.

Verwendung des Cleanroom Profils nur für störungsfreie Netzwerke empfohlen, siehe Kapitel 4.2.

Verwendung

Das Profil *Fast & Cleanroom* ist geeignet für Anwendungen, in idealer Umgebung z. B. Labor!

- Für schnellsten Datendurchsatz.
- Für Anwendungen, die eine schnelle Datenübermittlung erfordern.
- Für Anwendungen, die eine möglichst geringe Worst Case ReactionTime erfordern.

Netzwerkanforderungen

- Fast: 100-Mbit-Technologie (100BASE-Tx), 1-Gbit-Technologie.
- Clean: Störungsfreies Netzwerk.
Datenverlust durch Netzüberlastung, Einflüsse von außen oder Netzwerkmanipulationen müssen vermieden werden.
- LAN-Switches erforderlich!

Charakteristiken des Kommunikationspfads

- Minimale Verzögerungen.
- Erwartete ResponseTime \leq ReceiveTMO
(anderenfalls FEHLER bei Parametrierung).

4.10.2 Profil II (Fast & Noisy)

Verwendung

Das Profil *Fast & Noisy* ist das SILworX Standardprofil für die Kommunikation über safe**ethernet**.

- Für schnellen Datendurchsatz.
- Für Anwendungen, die eine schnelle Datenübermittlung erfordern.
- Für Anwendungen, die eine möglichst geringe Worst Case Reaction Time erfordern.

Netzwerkanforderungen

- Fast: 100-Mbit-Technologie (100BASE-Tx), 1-Gbit-Technologie.
- Noisy: Netzwerk ist nicht störungsfrei.
Geringe Wahrscheinlichkeit für Verlust von Datenpaketen, Zeit für ≥ 1 Wiederholung.
- LAN-Switches erforderlich!

Charakteristiken des Kommunikationspfads

- Minimale Verzögerungen.
- Erwartete ResponseTime \leq ReceiveTMO / 2
(anderenfalls FEHLER bei Parametrierung).

4.10.3 Profil III (Medium & Cleanroom)

i

HIMA empfiehlt, für eine **safeethernet** Verbindung mit hoher Verfügbarkeit, die Profile *Fast&Noisy*, *Medium&Noisy* oder *Slow&Noisy* zu verwenden.
Verwendung des Cleanroom Profils nur für störungsfreie Netzwerke empfohlen, siehe Kapitel 4.2.

Verwendung

Das Profil *Medium & Cleanroom* ist für Anwendungen in einem störungsfreien Netzwerk, die eine nur mäßig schnelle Datenübermittlung erfordern.

- Für mittleren Datendurchsatz.
- Geeignet für Virtual Private Networks (VPN), in denen der Datenaustausch durch zwischengeschaltete Sicherheitseinrichtungen (Firewalls, Verschlüsselung) langsam, aber fehlerfrei ist.
- Geeignet für Anwendungen, in denen die Worst Case ReactionTime kein kritischer Faktor ist.

Netzwerkanforderungen

- Medium: 10-Mbit- (10BASE-T), 100-Mbit- (100BASE-Tx), 1-Gbit-Technologie.
- LAN-Switches erforderlich!
- Clean: Störungsfreies Netzwerk.
Datenverlust durch Netzüberlastung, Einflüsse von außen oder Netzwerkmanipulationen müssen vermieden werden, Zeit für ≥ 0 Wiederholungen.

Charakteristiken des Kommunikationspfads

- Moderate Verzögerungen.
- Erwartete ResponseTime \leq ReceiveTMO (anderenfalls FEHLER bei Parametrierung).

4.10.4 Profil IV (Medium & Noisy)

Verwendung

Das Profil *Medium & Noisy* ist für Anwendungen, die eine nur mäßig schnelle Datenübermittlung erfordern.

- Für mittleren Datendurchsatz.
- Für Anwendungen, die nur eine mäßig schnelle Datenübermittlung erfordern.
- Geeignet für Anwendungen, in denen die Worst Case ReactionTime kein kritischer Faktor ist.

Netzwerkanforderungen

- Medium: 10-Mbit- (10BASE-T), 100-Mbit- (100BASE-Tx), 1-Gbit-Technologie.
- LAN-Switches erforderlich!
- Noisy: Netzwerk ist nicht störungsfrei.
Geringe Wahrscheinlichkeit für Verlust von Datenpaketen, Zeit für ≥ 1 Wiederholung.

Charakteristiken des Kommunikationspfads

- Moderate Verzögerungen.
- Erwartete ResponseTime \leq ReceiveTMO / 2 (anderenfalls FEHLER bei Parametrierung).

4.10.5 Profil V (Slow & Cleanroom)

1

HIMA empfiehlt, für eine safe**ethernet** Verbindung mit hoher Verfügbarkeit, die Profile *Fast&Noisy*, *Medium&Noisy* oder *Slow&Noisy* zu verwenden.

Verwendung des Cleanroom Profils nur für störungsfreie Netzwerke empfohlen, siehe Kapitel 4.2.

Verwendung

Das Profil *Slow & Cleanroom* ist für Anwendungen in einem störungsfreien Netzwerk, die nur eine langsame Datenübermittlung erfordern.

- Für langsamen Datendurchsatz.
- Für Anwendungen, die nur eine langsame Datenübermittlung zu (möglicherweise weit entfernten) Steuerungen erfordern, und dort, wo die Bedingungen der Kommunikationsstrecke nicht Vorhersagbar sind.

Netzwerkanforderungen

- Slow: Datentransfer über ISDN, Standleitung oder Richtfunkverbindung.
- Clean: Störungsfreies Netz.
Datenverlust durch Netzüberlastung, Einflüsse von außen oder Netzwerkmanipulationen müssen vermieden werden, Zeit für ≥ 0 Wiederholungen.

Charakteristiken des Kommunikationspfads

- Moderate Verzögerungen.
- Erwartete ResponseTime = ReceiveTMO (anderenfalls FEHLER bei Parametrierung).

4.10.6 Profil VI (Slow & Noisy)

Verwendung

Das Profil *Slow & Noisy* ist für Anwendungen, die nur eine langsame Datenübermittlung zu (möglicherweise weit entfernten) Steuerungen erfordern.

- Für langsamen Datendurchsatz.
- Für Anwendungen, hauptsächlich für Datentransfer über schlechte Telefonleitungen oder gestörte Richtfunkstrecken.

Netzwerkanforderungen

- Slow: Datentransfer über Telefon, Satellit, Funk usw.
- Noisy: Netzwerk ist nicht störungsfrei.
Geringe Wahrscheinlichkeit für Verlust von Datenpaketen, Zeit für ≥ 1 Wiederholung.

Charakteristiken des Kommunikationspfads

- Moderate bis lange Verzögerungen.
- Erwartete ResponseTime \leq ReceiveTMO / 2 (anderenfalls FEHLER bei Parametrierung).

4.11 Control Panel (safeethernet)

Im Control Panel kann die Einstellungen der **safeethernet** Verbindung überprüft werden. Zudem werden aktuelle Statusinformationen (z. B. Zykluszeit, Bus-Zustand usw.) der **safeethernet** Verbindung angezeigt.

Öffnen des Control Panels zur Überwachung der safeethernet Verbindung

1. Im Strukturbaum **Ressource** selektieren.
2. Im Kontextmenü der Ressource **Online** wählen.
3. Im **System-Login**, Zugangsdaten eingeben um das Control Panel der Ressource zu öffnen.
4. Im Strukturbaum des Control Panels **safeethernet** wählen.

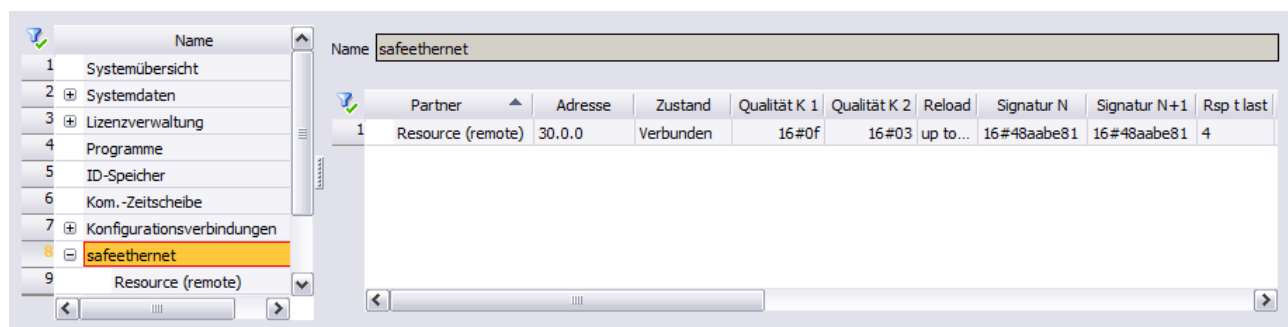


Bild 22: Control Panel zur safeethernet Verbindungsübersicht

Zurücksetzen der statistischen Daten der safeethernet Verbindung

Mit der Kontextmenüfunktion können die statistischen Daten (Zykluszeit min, max usw.) auf null zurückgesetzt werden.

1. Im Strukturbaum **safeethernet** Verbindung selektieren.
2. Aus dem Kontextmenü der **safeethernet** Verbindung, **safeethernet Statistik zurücksetzen** wählen.

4.11.1 Anzeigefeld (safeethernet Verbindung)

In dem Anzeigefeld werden die folgenden Werte der selektierten **safeethernet** Verbindung angezeigt:

Element	Beschreibung
Partner	Ressource-Name des Kommunikationspartners.
Adresse	System-ID
Zustand	Zustand der safeethernet Verbindung. (Siehe auch Kapitel 4.6).
Qualität K 1	Qualität von Transportweg Kanal 1. (Siehe auch Kapitel 4.6).
Qualität K 2	Qualität von Transportweg Kanal 2. (Siehe auch Kapitel 4.6).

Element	Beschreibung		
Reload	safeethernet Reload Status unknown: Zustand der geladenen Signaturen des Partners ist unbekannt: -es besteht keine Verbindung. -Partner hat ein altes Betriebssystem ohne die Funktion safeethernet Reload. updated: In diese Steuerung wurde der aktuelle Code geladen, beim Partner muss er noch geladen werden. outdated: Der Partner wurde bereits mit einem neueren Code geladen, diese Steuerung muss noch geladen werden. up to date: Beide Partner haben die identische N+1 Signatur.		
Signatur N	Durch die Änderung der safeethernet Konfiguration entsteht eine Dualkonfiguration. Alte Signatur der safeethernet Konfiguration.		
Signatur N+1	Neue Signatur der safeethernet Konfiguration.		
Rsp t last	Tatsächliche Response-Time als Minimal-, Maximal-, Letzte- und Durchschnittswert. Siehe auch Kapitel 4.8.3.		
Rsp t avg			
Rsp t min			
Rsp t max			
Fehler	Fehlerhafte Nachrichten Anzahl verworfener Nachrichten seit Reset der Statistik.		
Wdh	Anzahl der Wiederholungen seit Reset der Statistik.		
Erfolge	Anzahl der Verbindungserfolge seit Reset der Statistik.		
Früh	Early Queue Usage Anzahl der verfrühten Nachrichten seit Reset der Statistik. Die verfrühten Nachrichten werden in der Early Queue gespeichert.		
Frame	Frame-Nr. Umlaufender Sendungszähler		
Ack Frame	Ack-Frame-Nr. Umlaufender Empfangszähler		
Monotonie	Umlaufender Nutzdatensendungszähler		
Rcv TMO	Receive-Timeout [ms] (Siehe auch Kapitel 4.8.2)		
Rsnd TMO	Resend-Timeout [ms] (Siehe auch Kapitel 4.8.5)		
Ack TMO	Acknowledge Timeout [ms] (Siehe auch Kapitel 4.8.6)		
Verb.Strg	Verbindungssteuerung		
Strg K 1	Transport-Steuerung Kanal 1 (Siehe auch Kapitel 4.6).		
Strg K 2	Transport-Steuerung Kanal 2 (Siehe auch Kapitel 4.6).		
Protokoll	0-1	Protokollversion für ELOP II Factory Ressourcen.	
	2	Protokollversion für SILworX Ressourcen.	

Tabelle 42: Anzeigefeld der **safeethernet** Verbindung

4.12 safeethernet Reload

Diese Funktionalität ermöglicht, Änderungen einer **safeethernet** Konfiguration im laufenden Betrieb per Reload auf die Steuerungen zu laden, und dabei die **safeethernet** Verbindung kontinuierlich aufrecht zu erhalten.

4.12.1 Voraussetzungen

safeethernet Reload ist für HIMax, HIMatrix und HIQuad X möglich. Es gelten die folgenden Systemanforderungen für alle an der **safeethernet** Verbindung beteiligten Steuerungen:

- HIMax ab CPU BS V6 und COM BS V6.
- HIQuad X ab CPU BS V10 und COM BS V10.
- HIMatrix ab CPU BS V10 und COM BS V15.

Die oben genannten COM-BS-Versionen oder höher sind erforderlich, wenn **safeethernet** Verbindungen über das COM-Modul transportiert werden, siehe Kapitel 4.12.7.

In den Eigenschaften der **safeethernet** Verbindung den Parameter *Codegen* auf **ab V6** einstellen.

i

Betriebssysteme der HIMax Module können während des Betriebs aktualisiert werden, wenn ein redundantes Modul vorhanden ist. Damit ist die Umstellung auf **safeethernet** Reload unterbrechungsfrei auch in HIMax Anlagen mit alten Betriebssystemen möglich.

4.12.2 Technisches Konzept

Die **safeethernet** Signatur ist ein CRC Code, welcher der eindeutigen Identifikation der **safeethernet** Konfiguration dient. Die **safeethernet** Signatur wird bei der Codegenerierung erstellt und ist Teil der geladenen Konfiguration.

safeethernet Kommunikation zwischen zwei Kommunikations-Partnern ist nur möglich, wenn beide die gleiche **safeethernet** Konfiguration mit derselben Signatur besitzen.

Um Änderungen einer **safeethernet** Verbindung mit einem Reload durchführen zu können, müssen der Steuerung zwei **safeethernet** Konfigurationen mit den zugehörigen Signaturen (N und N+1) zur Verfügung stehen. Dies ist ab SILworX V6 möglich.

In den beiden Steuerungen wird die Konfiguration E1 mit einer **safeethernet** Signatur gehalten



Nach Änderung der Verbindung und Reload der Steuerung 1 stehen dort die Konfigurationen E1 und E2 zur Verfügung. In der Steuerung1 ist weiterhin die alte **safeethernet** Konfiguration E1 mit der Signatur N aktiv.

Durch die Änderung der **safeethernet** Konfiguration entsteht eine Dualkonfiguration (hier E1+E2). Der **safeethernet** Reload-Zustand von Steuerung 1 ist jetzt **updated** und der von Steuerung 2 **outdated** und signalisiert so, dass ein Reload auf Steuerung 2 durchgeführt werden muss.



¹⁾ **safeethernet** Versionszustand, siehe Kapitel 4.12.5

Nach dem Reload der Steuerung2 ist die neue **safeethernet** Konfiguration E2 mit der Signatur N+1 aktiv. Die Dualkonfiguration (E1+E2) besteht jetzt in beiden Steuerungen und sollte wie empfohlen durch einen weiteren Reload auf beiden Steuerungen entfernt werden, siehe Kapitel 4.12.3.1.



¹⁾ **safeethernet** Versionszustand, siehe Kapitel 4.12.5

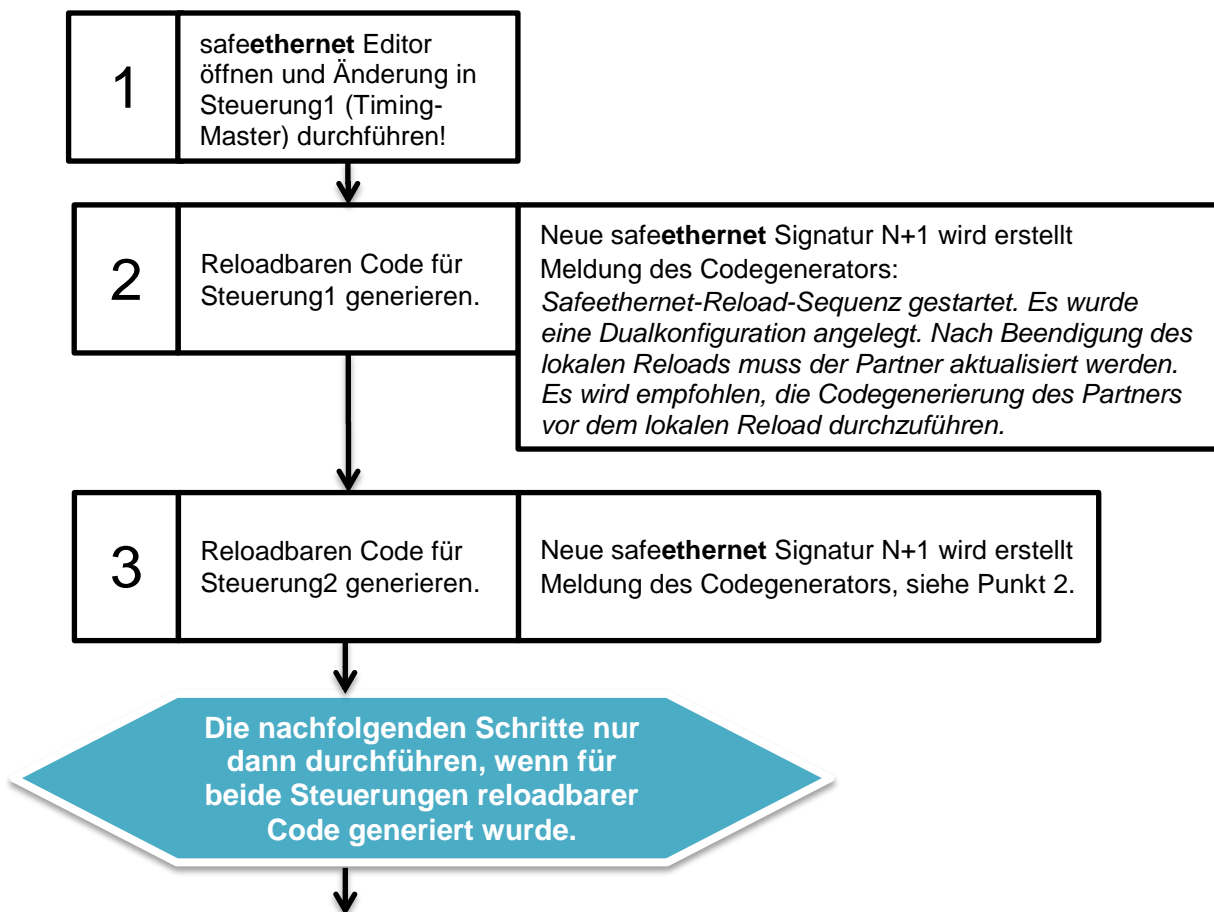
i

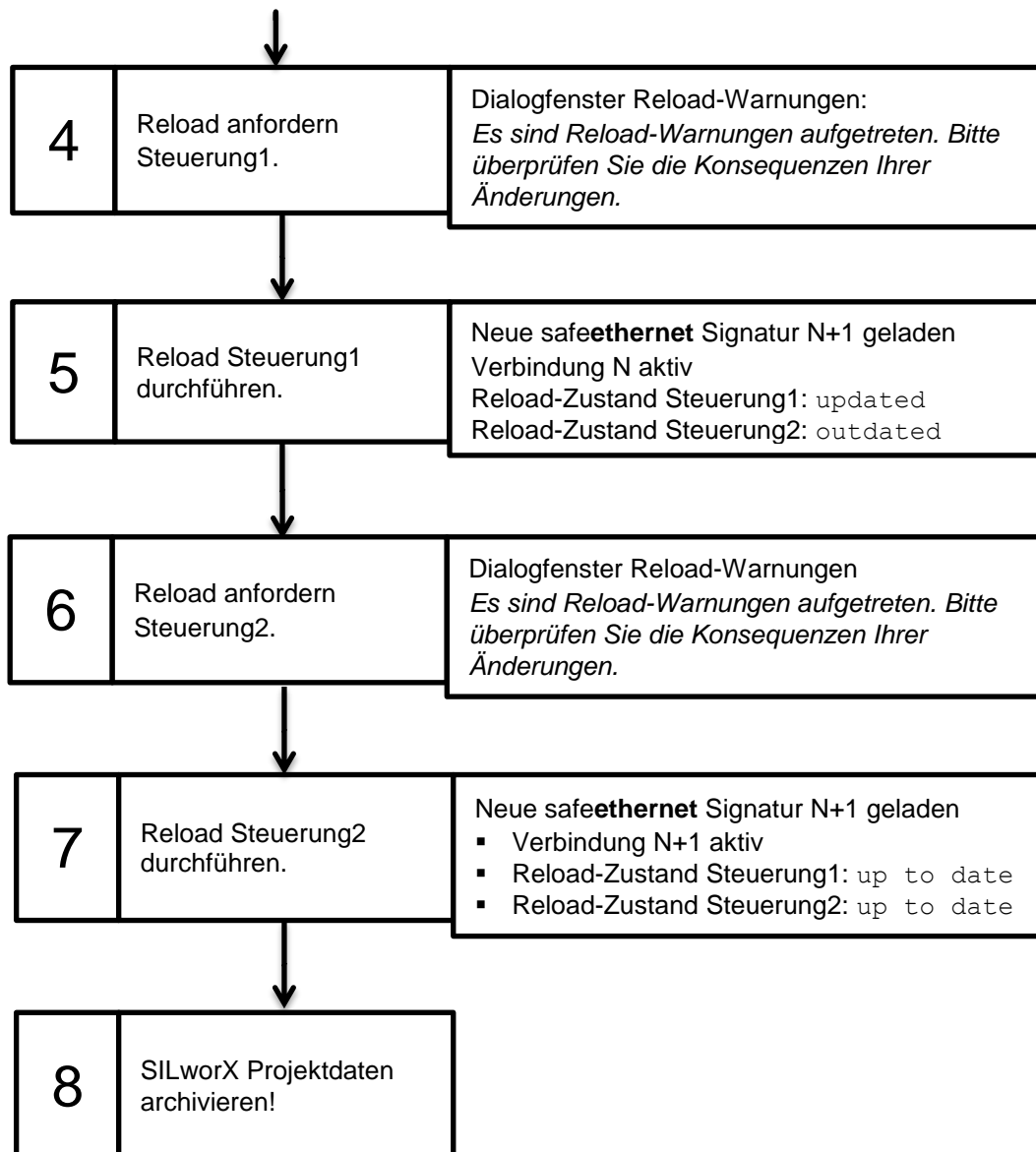
HIMA empfiehlt beim Reload immer zuerst mit der Steuerung zu beginnen, die als *Timing-Master* der **safeethernet** Verbindung konfiguriert ist. Die neue **safeethernet** Verbindung wird erst aktiviert, wenn beide Steuerungen geladen wurden.

4.12.3 Einzuhaltende Vorgehensweise

safeethernet Verbindungen sind ganzheitlich zu betrachten und Änderungen immer auf beiden Seiten direkt nacheinander vorzunehmen, um inkonsistente **safeethernet** Konfigurationen zu vermeiden.

Bis zu Schritt 5 ist die alte **safeethernet** Konfiguration noch aktiv. Nach dem erfolgreichen Reload in Schritt 5 ist die neue **safeethernet** Konfiguration aktiv.





4.12.3.1 Signatur N und N+1 angleichen

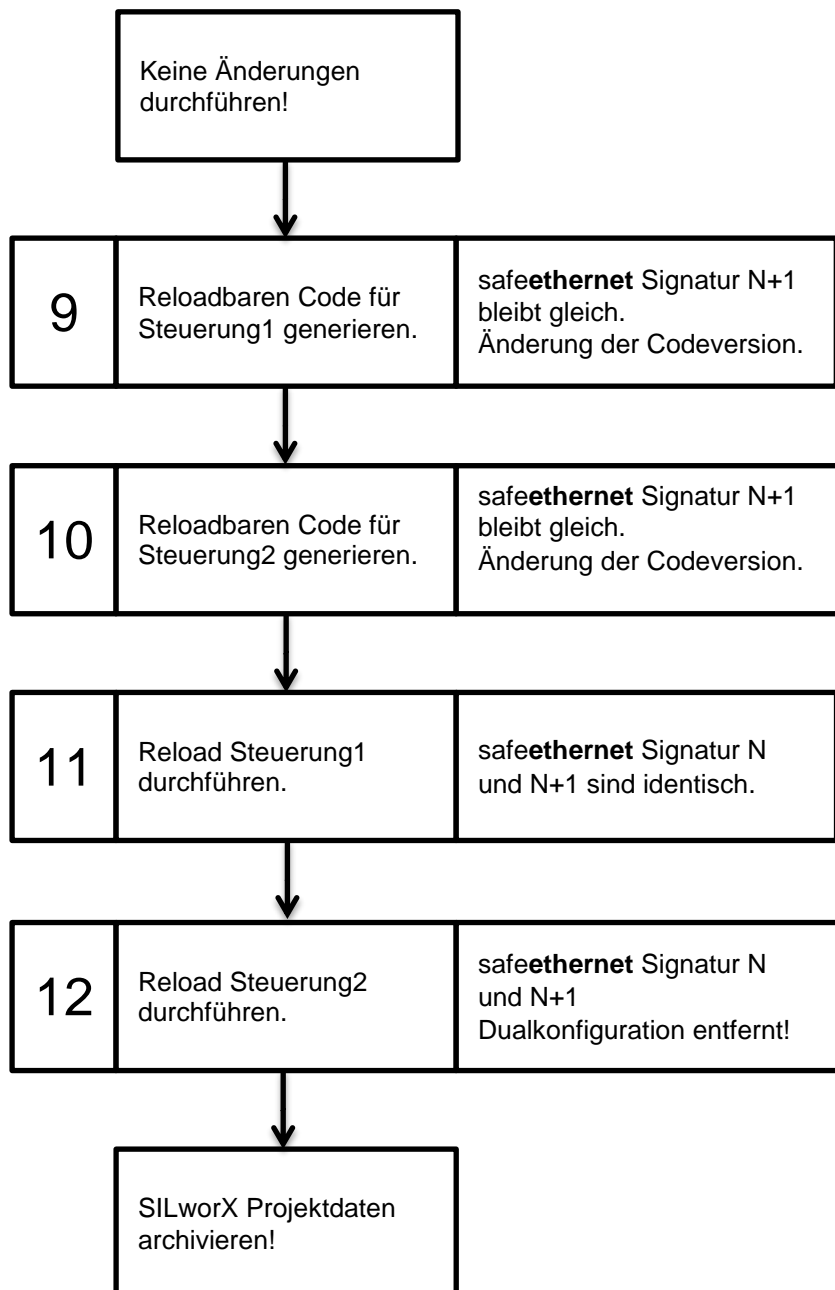
Änderungen der **safeethernet** Konfiguration wie im Kapitel 4.12.3 beschrieben führen zu einer Dualkonfiguration. Die Steuerungen beinhalten dann die folgenden zwei Konfigurationen:

- Die alte Konfiguration mit der **safeethernet** Signatur N, über welche die **safeethernet** Kommunikation läuft, solange noch nicht beide Steuerungen aktualisiert sind.
- Die neue Konfiguration mit der **safeethernet** Signatur N+1, über welche die **safeethernet** Kommunikation läuft, nachdem beide Steuerungen aktualisiert wurden.

i

Nach einer weiteren Codegenerierung ohne **safeethernet** Änderung wird die Dualkonfiguration entfernt. Das bedeutet, dass in den Systemvariablen *Signatur N* und *Signatur N+1* der gleiche CRC Code steht. HIMA empfiehlt, eine Dualkonfiguration immer zu entfernen. Dies muss für beide Ressourcen durchgeführt werden.

Zum Entfernen einer Dualkonfiguration die folgenden Schritte 9 bis 12 ausführen!



4.12.4 Integrierte Schutzmechanismen

In SILworX und im Betriebssystem der Steuerung sind Schutzmechanismen integriert, die eine versehentliche Unterbrechung oder Wiederaufnahme einer **safeethernet** Verbindung vorab erkennen und eine Warnung generieren.

4.12.4.1 Automatische Prüfung bei der Codegenerierung

Die folgende Tabelle enthält die Meldungen, die während einer Codegenerierung in Bezug auf **safeethernet** Reload auftreten und den Anwender über den aktuellen **safeethernet** Reload Zustand informieren.

Info im Codegenerator Dialog	Beschreibung
<i>Reload Warnung</i> <i>Safeethernet-Reload-Sequenz gestartet. Es wurde eine Dualkonfiguration angelegt. Nach Beendigung des lokalen Reloads muss der Partner aktualisiert werden. Es wird empfohlen, die Codegenerierung des Partners vor dem lokalen Reload durchzuführen.</i>	Vorgang OK! Nach einer Änderung der safeethernet Verbindung und Codegenerierung erfolgt diese Information! Empfohlene Vorgehensweise ausführen, siehe Kapitel 4.12.2.
<i>Reload Info</i> <i>safeethernet Reload Dualkonfiguration für Verbindung „safeethernet V1“ zu „Steuerung2“ wurde entfernt.</i>	Vorgang OK! Reload nach einer weiteren Codegenerierung ohne safeethernet Änderung wurde durchgeführt. Die Dualkonfiguration wurde entfernt, d. h. es gibt jetzt wieder nur eine Konfiguration mit einer safeethernet Signatur, siehe Kapitel 4.12.3.1.
<i>Es kann zu einer safeethernet Verbindungsunterbrechung für Verbindung „safeethernet V1 zu „Steuerung2“ kommen. Bitte aktualisieren sie diesen Partner. In der Download-Konfiguration des Partners kann keine Verbindungsversion gefunden werden, welche zur gerade erzeugten passt.</i>	Achtung! Keinen Reload durchführen, wenn eine Verbindungsunterbrechung vermieden werden soll! Setzen Sie sich mit dem HIMA Support in Verbindung! Mit der Partnersteuerung gibt es keine gemeinsame Konfiguration mit der gleichen Signatur mehr um einen safeethernet Reload durchzuführen.

Tabelle 43: Meldungen des Codegenerators

4.12.4.2 Automatische Prüfung bei Reload der Steuerung

Voraussetzung für die Erzeugung von Warnmeldungen vor einem **safeethernet** Reload sind die geeigneten CPU Betriebssysteme auf den Steuerungen.

- HIMax CPU BS ab V6.
- HIQuad X ab CPU BS V10.
- HIMatrix ab CPU BS V10.

Vor der Ausführung eines Reloads prüft das Betriebssystem, ob der **safeethernet** Reload Zustand für einen Reload geeignet ist. Erkennt eine Steuerung, dass ein Reload zur Unterbrechung der **safeethernet** Verbindung führen kann, erzeugt diese eine entsprechende Warnmeldung die in SILworX angezeigt wird. Der Reload kann in dieser Situation manuell abgebrochen werden. Die Steuerungen laufen danach mit der letzten passenden **safeethernet** Konfiguration weiter.

Info im Dialogfenster	Beschreibung
<i>Ein Reload soll ausgeführt werden, obwohl eine SE-Verbindung den safeethernet Reload Zustand updated meldet, SE-Adresse des Partners: x/x/x. Die Verbindung kann bei Aktivierung der Konfiguration verloren gehen. Prüfen sie die Konsequenzen.</i>	Achtung! Keinen Reload durchführen! Setzen Sie sich mit dem HIMA Support in Verbindung! Wird der Reload dennoch durchgeführt, kann die safeethernet Verbindung unterbrochen werden!
<i>Ein Reload soll ausgeführt werden, während eine SE-Verbindung den safeethernet Reload Zustand unknown meldet (d.h. dass keine Verbindung zum Partner besteht), SE-Adresse des Partners: x/x/x. Sollte vor der Aktivierung der Konfiguration eine Verbindung zustande kommen, könnte diese durch die Aktivierung wieder verloren gehen. Prüfen sie die Konsequenzen.</i>	Achtung! Der safeethernet Reload Zustand unknown wird gemeldet, wenn eine safeethernet Verbindung unterbrochen ist, siehe Kapitel 4.12.5. Vor einem erneuten Reload physikalische Verbindung prüfen, z. B. ob alle Ethernet-Kabel richtig gesteckt sind.

Tabelle 44: Meldungen des Betriebssystems

4.12.5 safeethernet Reload Zustand

Der Reload Zustand informiert über den aktuellen Zustand der safeethernet Verbindung und ob die passenden safeethernet Konfigurationen geladen sind oder geladen werden müssen. Voraussetzung für die korrekte Anzeige des Reload Status ist die konsequente vorgehensweise beim safeethernet Reload, siehe Kapitel 4.12.3.

Der folgende safeethernet Reload Zustand wird angezeigt:

unknown:	Zustand der geladenen Signaturen des Partners ist unbekannt: <ul style="list-style-type: none"> ▪ Es besteht keine Verbindung. ▪ Partner hat ein altes Betriebssystem ohne die Funktion safeethernet Reload.
updated:	In diese Steuerung wurde der aktuelle Code geladen, beim Partner muss er noch geladen werden.
outdated:	Der Partner wurde bereits mit einem neueren Code geladen, diese Steuerung muss noch geladen werden.
up to date:	Beide Partner haben die identische N+1 Signatur.

Sollte nach einem Reload keine passende Konfiguration mehr zur Verfügung stehen, erhält der Anwender eine Warnung und hat die Möglichkeit, diesen Reload abzubrechen.

Wird der Reload dennoch unter Missachtung der in Kapitel 4.12.4 beschriebenen Warnmeldungen durchgeführt, steht in der Partnersteuerung ggf. keine passende Konfiguration mehr zur Verfügung. Die safeethernet Verbindung zur Partnersteuerung wird eventuell unterbrochen (CLOSED)!

Der safeethernet Versionszustand wird in der SILworX Online-Ansicht der safeethernet Verbindung als *Reload* angezeigt. Die gleiche Information enthält die Systemvariable *Versions Zustand*, die durch Zuweisung einer Globalen Variablen im Anwenderprogramm verwendet werden kann.

4.12.6 Maximale Anzahl safeethernet Verbindungen während des Reloads

Die Anzahl der in der Steuerung gehaltenen safeethernet Verbindungen kann während des Reloads größer sein als konfiguriert. Zusätzlich zu den hinzugefügten safeethernet Verbindungen werden auch die gelöschten safeethernet Verbindungen gehalten, da diese noch bis zum Ende des Reloads aktiv bleiben müssen.

Die maximale Anzahl der gleichzeitig gehaltenen safeethernet Verbindungen während des Reloads ist wie folgt:

- $HIMax = 300$ (max. 255 safeethernet Verbindungen + 45 (Reload-Buffer)).

- HIMatrix = 277 (max. 255 safeethernet Verbindungen + 22 (Reload-Buffer)).
- HIQuad X = 150 (max. 128 safeethernet Verbindungen + 22 (Reload-Buffer)).

Diese Limits bestehen, um den maximal benötigten Speicherplatz beim Reload zu begrenzen.

i

Wird bei der Reload-Codegenerierung die maximale Anzahl der safeethernet Verbindungen für Reload überschritten, wird die Reload-Codegenerierung mit einer Fehlermeldung abgebrochen. Max. Anzahl safeethernet Verbindungen zwischen zwei Steuerungen, siehe Kapitel 4.3.

Sind mehr Änderungen erforderlich, müssen diese über mehrere Reloads hinweg durchgeführt werden.

4.12.7 safeethernet Verbindung über Kommunikationsmodul

HIMA empfiehlt den Parameter *Codegenerierung* des Kommunikationsmoduls auf den Wert *ab V6* einzustellen, um bei einem Reload der Steuerung einen Cold Reload des Kommunikationsmoduls möglichst zu vermeiden. Damit bleiben safeethernet Verbindungen die über dieses Kommunikationsmodul geleitet werden unterbrechungsfrei, auch wenn Änderungen der Variablen oder Parameter (z. B. Profil) durchgeführt wurden.

Zum safeethernet Reload Verhalten des Kommunikationsmoduls bei weiteren Änderungen, siehe nachfolgendes Kapitel 4.12.8.

4.12.8 Änderungen der safeethernet Konfiguration

Die folgende Tabelle gibt eine Übersicht über Änderungen der safeethernet Konfiguration und welche Auswirkungen diese auf den safeethernet Reload haben.

Änderungen bei	CPU	COM
Hinzufügen oder Löschen globaler Variablen zu		
safeethernet	•	•
X-OPC (DA)	•	•
X-OPC (Events)	•	•
Ändern der Anzahl Views (X-OPC).	•	•
Hinzufügen oder Löschen einer neuen safeethernet Verbindung.	•	• ¹⁾
safeethernet Parameter (z. B. <i>Timing Master</i> , <i>Receive Timeout</i>).	•	•
IP-Adressen (Änderung des Transportwegs).	•	• ¹⁾
safeethernet Parameter (<i>Profile</i>).	-	n. a.
safeethernet Parameter (<i>Verhalten bei Verbindungsverlust</i>).	-	n. a.
<ul style="list-style-type: none"> • safeethernet Reload möglich. - safeethernet Reload nicht möglich. 		
n. a. nicht anwendbar		
¹⁾ Nur mit <i>Cold Reload</i> , d. h. bei gestopptem Kommunikationsmodul.		

Tabelle 45: safeethernet Reload nach Änderungen

4.13 Projektübergreifende Kommunikation

Die projektübergreifende sicherheitsbezogene Kommunikation wird verwendet, um Ressourcen aus verschiedenen Projekten miteinander zu verbinden.

Die Verbindung zwischen den beiden Projekten erfolgt über Proxy Ressourcen. Eine Proxy Ressource ist ein Stellvertreter für eine Ressource aus dem anderen Projekt.

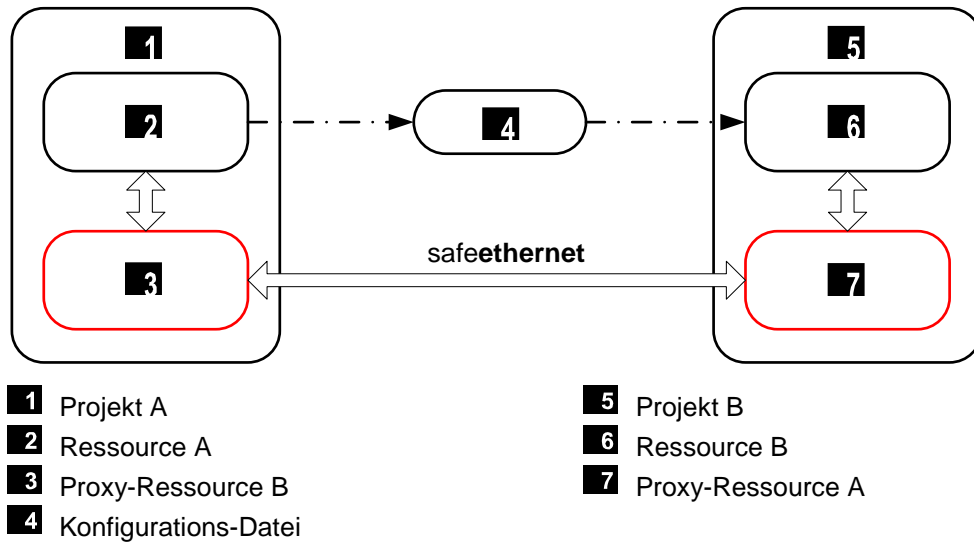


Bild 23: **safeethernet** Verbindung zwischen Ressource A im Projekt A und der Ressource B im Projekt B

Im Projekt A wird die Konfiguration der **safeethernet** Verbindung durchgeführt und die Konfigurationsdatei erstellt und archiviert.

Im Projekt B wird die Konfigurationsdatei wiederhergestellt. Es entsteht automatisch eine Proxy Ressource A mit den Daten der Ressource A aus dem Projekt A.

4.13.1 Konfiguration in SILworX

Anhand eines Beispiels soll die prinzipielle Vorgehensweise aufgezeigt werden. Die verwendeten Namen für die Projekte, Konfigurationen und Ressourcen sind nur beispielhaft gewählt.

Zur Übersichtlichkeit werden die Konfiguration A und die Konfiguration B in beiden SILworX Projekten angelegt.

Projekt A

- └ Konfiguration A
 - | └ Ressource A
- └ Konfiguration B
 - | └ Ressource B (als Proxy)
- └ Globale Variablen

Projekt B

- └ Konfiguration B
 - | └ Ressource B
- └ Konfiguration A
 - | └ Ressource A (als Proxy)
- └ Globale Variablen
(Die Globalen Variablen können durch Wiederherstellen eines Archivs oder als Import einer Excel-Liste erstellt werden.)

4.13.1.1 Konfiguration B im Projekt A erstellen

Separate Konfiguration B für Proxy Ressource B im Projekt A erstellen.

Erstellen der Konfiguration B

1. Projekt A öffnen, in dem die Konfiguration B erstellt werden soll.
2. Rechtsklick auf **Projekt A** und **Neu, Konfiguration** wählen.
 - ☒ Eine neue Konfiguration (Konfiguration B) wird angelegt.

4.13.1.2 Erstellen der Proxy-Ressource B im Projekt A

Die Proxy-Ressource B dient als Platzhalter für die Ressource aus dem externen Projekt B und wird für die Konfiguration des Prozessdaten-Austauschs über **safeethernet** genutzt.

Erstellen der Proxy-Ressource B

1. Rechtsklicken auf **Konfiguration B** und **Neu, Proxy-Ressource** SILworX wählen.
 - ☒ Eine neue Proxy-Ressource (Proxy-Ressource B) wird hinzugefügt.

Konfiguration der Proxy-Ressource B

1. Im Kontextmenü der Proxy-Ressource B **Eigenschaften** wählen.
2. Im Feld **Name** eindeutigen Namen eintragen.
Für die Proxy-Ressource B im Projekt A den Namen der Ressource B im Projekt B verwenden.
3. Die im Projekt B ausgelesene **System-ID** für diese Proxy-Ressource B eintragen.
4. Mit **OK** bestätigen.

Struktur der Proxy-Ressource B öffnen

1. Rechtsklick auf **Hardware** und **Edit** wählen.
2. Den im Projekt B verwendeten Ressource-Typ auswählen:
 - **HIMatrix 03 Proxy**
 - HIMatrix Proxy
 - HIMax System-Proxy
 - H41X System-Proxy
 - H51X System-Proxy
3. Mit **OK** bestätigen, um den Hardware-Editor der Proxy-Ressource B zu öffnen.

4. Für HIMatrix 03 Proxy, nacheinander **CPU-** und **COM-Modul** doppelklicken, über welche die redundante Verbindung auf der Proxy-Ressource B hergestellt wird.

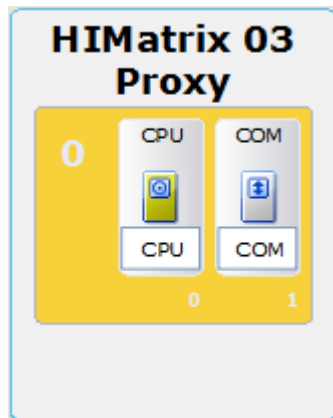


Bild 24: HIMatrix Proxy-Ressource

5. Die *IP-Adressen* eintragen und auf **Speichern** klicken.
6. Diese Schritte für jede weitere Proxy-Ressource im Projekt A wiederholen.

4.13.1.3 Globale Variablen für safeethernet Verbindung erstellen und archivieren

Erstellen der Globalen Variablen für die safeethernet Verbindung

1. Rechtsklick auf **Projekt A** und **Neu, Globale Variablen** wählen.
☒ Objekt Globale Variable wird auf Projektebene angelegt.
2. Rechtsklick auf **Globale Variablen** und im Kontextmenü **Edit** wählen, um den Variableneditor zu öffnen.
3. Rechtsklick auf eine freie Stelle im Arbeitsbereich des Variableneditors und im Kontextmenü **Neue Globale Variable** wählen, um eine neue Globale Variable anzulegen.
4. Diese Schritte für jede weitere neue Globale Variable für die safeethernet Verbindung wiederholen.
5. Zusätzlich Globale Variablen *Verbindungszustand*, *Qualität Kanal 1* (eventuell *Qualität Kanal 2* bei redundanter Verbindung) erstellen. Die Systemvariablen je doppelt erstellen. Einmal aus Sicht der Ressource A und einmal aus Sicht der Ressource B.

Archivieren der Globalen Variablen

TIPP

Ist auf der Projektebene im Projekt B bereits das Objekt *Globale Variablen* vorhanden, kann alternativ die SILworX Funktion zum CSV-Import/-Export verwendet werden. Mit den entsprechenden Filtereinstellungen können die benötigten Globalen Variablen selektiv exportiert werden, siehe Online Hilfe.
 Auch bei mehreren Proxy-Verbindungen zu unterschiedlichen Projekten ist Export sinnvoller als Archivieren. Dann z. B. im Feld Zusatzkommentar je Variable eine Identifikation für die Verbindung eintragen.

1. Im Strukturbaum **Projekt A, Globale Variable** selektieren.
2. Im Kontextmenü **Archivieren** wählen. Das SILworX-Dialogfenster zum Archivieren eines Objekts wird geöffnet.
3. Im Dialogfenster Archivname für das Globale Variablen Objekt eingeben. Archiv wird mit der Datei-Erweiterung ***.A3** im gewählten Archivverzeichnis gespeichert.
☒ Das archivierte Globale Variablen Objekt enthält alle Globalen Variablen die im Projekt A auf Projektebene angelegt wurden.

4.13.1.4 Verbindung erstellen zwischen Ressource A und Proxy-Ressource B

Im **safeethernet** Editor eine **safeethernet** Verbindung zwischen der Ressource A und der Proxy-Ressource B erstellen.

Öffnen des **safeethernet** Editors der Ressource A

1. Im Strukturbaum **Konfiguration A, Ressource A, safeethernet** selektieren.
2. Rechtsklicken auf **safeethernet** und im Kontextmenü **Edit** wählen.
☒ In der Objektauswahl befindet sich die zuvor angelegte Proxy-Ressource B.

Erstellen der **safeethernet** Verbindung zur Proxy-Ressource:

1. In der Objektauswahl auf die **Proxy-Ressource B** klicken und per Drag&Drop auf eine freie Stelle im Arbeitsbereich des **safeethernet** Editors ziehen.
Sofort passenden Namen für diese Verbindung vergeben.
2. Passende Ethernet-Schnittstellen **IF Kanalx** der Ressource und der Proxy-Ressource auswählen.

4.13.1.5 Prozessvariablen verbinden

Die Prozessvariablen im Editor der **safeethernet** Verbindung hinzufügen.

Öffnen des Verbindungseditors

Der **safeethernet**-Editor der Ressource A ist geöffnet.

1. Rechtsklicken auf Zeile **Ressource B (Proxy)** und Kontextmenü öffnen.
2. Im Kontextmenü **Edit** wählen, um den Verbindungseditor der **safeethernet** Verbindung zu öffnen.
3. Register **Ressource A<->Ressource B (Proxy)** wählen.
4. In der Objektauswahl eine **Globale Variable** wählen und per Drag&Drop in den Bereich **Ressource A --> Ressource B (Proxy)** oder in den Bereich **Ressource B (Proxy) --> Ressource A** je nach gewünschter Transportrichtung ziehen.
5. Diesen Schritt für weitere Variablen wiederholen.

4.13.1.6 Systemvariablen verbinden

Die Systemvariablen *Verbindungszustand*, *Qualität Kanal 1* und (eventuell *Qualität Kanal 2* bei redundanter Verbindung) mit Globalen Variablen verbinden. Weitere Informationen zu den Systemvariablen, siehe Kapitel 4.6.3.1.

Öffnen des Verbindungseditors

Der **safeethernet**-Editor der Ressource A ist geöffnet.

1. Rechtsklicken auf Zeile **Proxy-Ressource** und Kontextmenü öffnen.
2. Im Kontextmenü **Edit** wählen, um den Verbindungseditor der **safeethernet** Verbindung zu öffnen.
3. Sub-Register **Systemvariablen** im Register **Ressource A** wählen.
4. In der Objektauswahl eine passende **Globale Variable** für diese Systemvariable wählen und per Drag&Drop in die Spalte **Globale Variable** ziehen.
5. Diesen Schritt für weitere Systemvariablen wiederholen.
6. Sub-Register **Systemvariablen** im Register **Ressource B** wählen.
7. In der Objektauswahl eine passende **Globale Variable** für diese Systemvariable wählen und per Drag&Drop in die Spalte **Globale Variable** ziehen.
8. Diesen Schritt für weitere Systemvariablen wiederholen.

4.13.1.7 Archivieren der safeethernet Verbindung im Projekt A

Die im Projekt A konfigurierte safeethernet Verbindung wird archiviert und im Projekt B wiederhergestellt.

Verifikation der safeethernet Verbindung

1. Im Strukturbaum **Projekt A**, safeethernet wählen und Kontextmenü öffnen.
2. Im Kontextmenü **Verifikation** wählen und mit **OK** bestätigen.
3. Einträge in der Statusanzeige sorgfältig überprüfen und gegebenenfalls korrigieren.

Archivieren der safeethernet Verbindung

1. Im Strukturbaum **Projekt A**, safeethernet wählen und Kontextmenü öffnen.
2. Im Kontextmenü **Archivieren** wählen. Das SILworX-Dialogfenster zum Archivieren eines Objekts wird geöffnet.
3. Im Dialogfenster Archivname für safeethernet Objekt eingeben. Archiv wird mit der Datei-Erweiterung *.A3 im gewählten Archivverzeichnis gespeichert.
 - ☒ Alle im safeethernet Objekt enthaltenen safeethernet Verbindungen sind nun archiviert. safeethernet Verbindungen können auch einzeln archiviert werden.
4. Projekt A schließen.



Die Konfiguration der safeethernet Verbindung muss mit dem Anwenderprogramm der Ressource neu kompiliert und in die Steuerung übertragen werden, bevor sie für die Kommunikation der Steuerung wirksam werden.

4.13.2 Konfiguration A im Projekt B

Separate Konfiguration A für Proxy Ressource A im Projekt B erstellen.

Das Projekt B stellt sich in SILworX nun wie das erste Projekt dar. Die Ressource aus dem ersten Projekt ist hier die Proxy-Ressource.

4.13.2.1 Erstellen Proxy-Ressource A im Projekt B

Die Proxy-Ressource A dient als Platzhalter für die Ressource A aus dem externen Projekt A und wird für den Prozessdaten-Austausch über safeethernet genutzt.

Erstellen einer Proxy-Ressource

1. Projekt B öffnen, in dem die Proxy-Ressource A erstellt werden soll.
2. Rechtsklick auf **Projekt B** und **Neu, Konfiguration** wählen.
 - ☒ Eine neue Konfiguration (Konfiguration A benennen) wird angelegt.
3. Rechtsklicken auf **Konfiguration A** und **Neu, Proxy-Ressource** SILworX wählen.
 - ☒ Eine neue Proxy-Ressource (Proxy-Ressource A benennen) wird hinzugefügt.

Konfiguration einer Proxy-Ressource

1. Kontextmenü der Proxy-Ressource A öffnen und **Eigenschaften** wählen.
2. Im Feld **Name** eindeutigen Namen eintragen.
Für die Proxy-Ressource A im Projekt B den Namen der Ressource A im Projekt A verwenden.
3. Die im Projekt A ausgelesene **System-ID** für diese Proxy-Ressource A eintragen.
4. Mit **OK** bestätigen.

Struktur der Proxy-Ressource öffnen

1. Rechtsklick auf **Hardware** und **Edit** wählen.
2. Den im ersten Projekt verwendeten Ressource-Typ auswählen:
 - H41X System-Proxy
 - H51X System-Proxy
 - HIMatrix 03 Proxy
 - HIMatrix Proxy
 - **HIMax System-Proxy**
3. Mit **OK** bestätigen, um den Hardware-Editor der Proxy-Ressource zu öffnen.
4. Für HIMax System-Proxy, das **Generic-Modul** wählen und per Drag&Drop auf den Steckplatz im Basisträger ziehen, der dem Steckplatz des CPU-/COM-Modul der Ressource A im Projekt A entspricht.

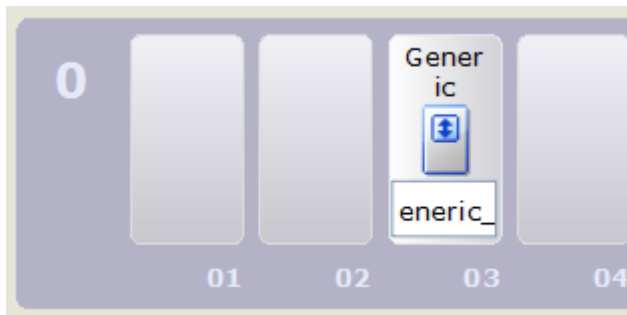


Bild 25: HIMax Proxy-Ressource

5. Auf das **Generic-Modul** doppelklicken und die *IP-Adresse* der CPU- und/oder COM-Module eintragen.
6. Auf **Speichern** klicken.
7. Diese Schritte für jede weitere Proxy-Ressource im Projekt B wiederholen.

4.13.2.2 Globale Variablen für safeethernet Verbindung erstellen

Im Projekt B müssen die gleichen Globalen Variablen wie im ersten Projekt angelegt werden.

TIPP Ist auf der Projektebene bereits das Objekt Globale Variablen vorhanden, kann alternativ die SILworX Funktion zum CSV-Import/-Export verwendet werden, siehe Online Hilfe.

Die Globalen Variablen im Projekt B wiederherstellen

1. Rechtsklick auf **Projekt** und im Kontextmenü **Wiederherstellen** wählen.
 - ☒ Das SILworX-Dialogfenster zum Wiederherstellen eines Objekts wird geöffnet.
2. Im Archivverzeichnis das archivierte *Globale Variable* Objekt mit der Datei-Erweiterung ***.A3** wählen, dass im Projekt A erstellt wurde.
 - ☒ Das wiederhergestellte Globale Variablen Objekt enthält alle Globalen Variablen die im Projekt A archiviert wurden.

4.13.2.3 Wiederherstellen der safeethernet Verbindung im Projekt B

Die safeethernet Verbindung im Projekt B wiederherstellen

1. Rechtsklick auf **Projekt** und im Kontextmenü **Wiederherstellen** wählen.
 - ☒ Das SILworX-Dialogfenster zum Wiederherstellen eines Objekts wird geöffnet.
2. Im Archivverzeichnis das archivierte **safeethernet** Objekt mit der Datei-Erweiterung ***.A3** wählen, dass im Projekt A erstellt wurde.
 - ☒ Das wiederhergestellte **safeethernet** Objekt enthält alle Verbindungen der Ressource A mit Proxy-Ressource B im Projekt B. Inklusive aller zugewiesener Variablen, Prozessvariablen und Systemvariablen.

5 SNTP-Protokoll

Das Simple Network Time Protocol (Simple Network Time Protocol) ist eine vereinfachte Version des NTP (Network Time Protocol).

Mit dem SNTP-Protokoll wird über Ethernet die Uhrzeit der SNTP-Clients durch den SNTP-Server synchronisiert.

HIMA Systeme können als **SNTP-Server** und/oder als **SNTP-Client** konfiguriert und eingesetzt werden. Es gilt der SNTP Standard nach RFC 2030 (SNTP-Version 4) mit der Einschränkung, dass nur der Unicast-Modus unterstützt wird.

5.1 Benötigte Ausstattung und Systemanforderung

Element	Beschreibung
Steuerung	HIMax HIQuad X HIMatrix
Aktivierung	Diese Funktion ist bei allen HIMA Systemen standardmäßig freigeschaltet.
Schnittstelle	Ethernet 10/100/1000BaseT

Tabelle 46: Systemanforderung und Ausstattung SNTP-Protokoll

5.2 SNTP-Client

Der SNTP-Client benutzt zu seiner Zeitsynchronisation immer nur den erreichbaren SNTP-Server mit der höchsten Priorität. Bei gleicher Priorität wird der SNTP-Server ausgewählt der (zufällig) als erstes Daten an den SNTP-Client vermittelt hat. Dieser SNTP-Server wird so lange beibehalten bis er nicht mehr zur Verfügung steht. Erst dann wird gewechselt.

Ist die Zeitdifferenz < 128 ms so wird die Uhr entsprechend 0,5 ms pro Zyklus schneller oder langsamer laufen gelassen bis die Zeitdifferenz ausgeglichen ist. Ist die Zeitdifferenz ≥ 128 s wird die Uhr sofort/schlagartig umgestellt.

In jeder HIMA Steuerung kann ein SNTP-Client zur Zeitsynchronisation konfiguriert werden.

Einen neuen SNTP-Client anlegen

1. Im Strukturbaum **Konfiguration, Ressource, Protokolle** öffnen.
2. Rechtsklick auf **Protokolle** und im Kontextmenü **Neu, SNTP-Client** wählen.
☒ Eine SNTP-Server Info wird standardmäßig unterhalb des SNTP-Clients hinzugefügt.
3. Im Kontextmenü vom SNTP-Client **Eigenschaften** das **COM-Modul** auswählen.

Das Dialogfenster des SNTP-Client enthält die folgenden Parameter.

Element	Beschreibung
Typ	SNTP-Client
Name	Name für den SNTP-Client.
Modul	Auswahl des CPU- oder COM-Moduls, auf dem dieses Protokoll abgearbeitet wird.
Max. μ P-Budget aktivieren	Wird vom Betriebssystem des Moduls nicht berücksichtigt. Parameter wurde wegen der CRC- und Reload-Stabilität erhalten.
Max. μ P-Budget in [%]	Wird vom Betriebssystem des Moduls nicht berücksichtigt. Parameter wurde wegen der CRC- und Reload-Stabilität erhalten.
Beschreibung	Beliebige eindeutige Beschreibung für den SNTP.
Aktuelle SNTP-Version	Anzeige der aktuellen SNTP Version.

Element	Beschreibung
Referenz Stratum	<p>Das Stratum eines SNTP-Clients gibt die Genauigkeit seiner lokalen Zeit wieder. Je niedriger das Stratum, desto genauer ist seine lokale Zeit. Null bedeutet ein unspezifiziertes oder nicht verfügbares Stratum (nicht gültig). Der aktuell verwendete SNTP-Server eines SNTP-Clients ist der, welcher erreichbar ist und die höchste Priorität besitzt.</p> <p>Ist das Stratum des aktuellen SNTP-Servers kleiner als das des SNTP-Clients, so übernimmt die Ressource die Zeit des aktuellen SNTP-Servers.</p> <p>Ist das Stratum des aktuellen SNTP-Servers größer als das des SNTP-Clients, so übernimmt die Ressource die Zeit des aktuellen SNTP-Servers nicht.</p> <p>Ist das Stratum des aktuellen SNTP-Servers gleich dem des SNTP-Clients, so sind zwei Fälle zu unterscheiden:</p> <ul style="list-style-type: none"> ▪ Wenn der SNTP-Client (Ressource) ausschließlich als SNTP-Client arbeitet, so übernimmt die Ressource die Zeit des aktuellen SNTP-Servers. ▪ Wenn der SNTP-Client (Ressource) gleichzeitig auch als SNTP-Server arbeitet, wird pro Anfrage des SNTP-Clients die Hälfte der Zeitdifferenz zum aktuellen-SNTP-Server auf der Ressource übernommen (Zeit nähert sich langsam an). <p>Wertebereich: 2 ... 15 Standardwert: 15</p>
Client Zeitanfrage Intervall [s]	<p>Zeitintervall, in dem die Zeitsynchronisation durch den aktuellen SNTP-Server erfolgt.</p> <p>Das Client Zeitanfrage Intervall im SNTP-Client muss größer sein, als das Timeout im SNTP-Server.</p> <p>Wertebereich: 16 ... 16384 s Standardwert: 16 s</p>

Tabelle 47: Eigenschaften des SNTP-Client

5.2.1 SNTP-Server Info

In der SNTP-Server Info wird die Verbindung zu einem SNTP-Server (Zeitserver) konfiguriert.

Eine SNTP-Server Info ist standardmäßig unterhalb des SNTP-Clients enthalten. Maximal können 4 SNTP-Server Infos unterhalb eines SNTP-Clients konfiguriert werden.

i

Sind in einem HIMA System mehrere SNTP-Clients konfiguriert, so darf zu jedem Zeitpunkt immer nur der (eine) SNTP-Client zur Zeitsynchronisierung verwendet werden, dessen aktiver Remote-SNTP-Server die höchste Priorität besitzt.

Eine neue SNTP-Server Info anlegen

1. Im Strukturbaum **Konfiguration, Ressource, Protokolle, SNTP Client** öffnen.
2. Rechtsklick auf **Protokolle** und im Kontextmenü **Neu, SNTP-Server Info** wählen.
 - ☒ Eine neue SNTP-Server Info wird hinzugefügt.

Das Dialogfenster der SNTP-Server Info enthält die folgenden Parameter.

Element	Beschreibung
Typ	SNTP-Server-Info
Name	Name für die SNTP-Server-Info.
Beschreibung	Beschreibung für den SNTP-Server.
IP-Adresse	IP-Adresse der Ressource oder des PC's, auf dem der SNTP-Server konfiguriert ist. Standardwert: 0.0.0.0
SNTP-Server Priorität	Priorität mit welcher der SNTP-Client diesen SNTP-Server behandelt. Die für einen SNTP-Client konfigurierten SNTP-Server sollten unterschiedliche Prioritäten besitzen. Wertebereich: 0 (geringste Priorität) bis 4294967295 (höchste Priorität.) Standardwert: 1
SNTP-Server Timeout [s]	Das Timeout im SNTP-Server muss kleiner eingestellt sein als das <i>Zeitanfragen Intervall</i> im SNTP-Client. Wertebereich: 1 ... 16384 s Standardwert: 1 s

Tabelle 48: Eigenschaften SNTP-Server-Info

5.3 SNTP-Server

Der SNTP-Server auf einem HIMA System ermöglicht externen Systemen ihr Datum und ihre Uhrzeit auf das Datum und die Uhrzeit des HIMA Systems zu synchronisieren.

Der SNTP-Server beantwortet SNTP-Anfragen, wenn die Systemzeit synchronisiert ist. Andernfalls werden SNTP-Anfragen verworfen.

Der SNTP-Server eines HIMA Systems nimmt die Anforderung von einem SNTP-Client (z. B. Remote I/O) entgegen und sendet seine aktuelle Zeit an diesen SNTP-Client zurück.

Einen neuen SNTP-Server anlegen

1. Im Strukturbaum **Konfiguration, Ressource, Protokolle** öffnen.
2. Rechtsklick auf **Protokolle** und im Kontextmenü **Neu, SNTP-Server** wählen.
☒ Ein neuer SNTP Server wird hinzugefügt.
3. Im Kontextmenü vom SNTP Server **Eigenschaften** das **Modul** auswählen, worüber der SNTP-Client gekoppelt ist.

Das Dialogfenster des SNTP Servers enthält die folgenden Parameter.

Element	Beschreibung
Typ	SNTP-Server
Name	Name für den SNTP-Server.
Modul	Auswahl des CPU- oder COM-Moduls, auf dem dieses Protokoll abgearbeitet wird.
Max. μ P-Budget aktivieren	Aktiviert : Limit des μ P-Budget aus dem Feld Max. μ P-Budget in [%] übernehmen. Deaktiviert: Kein Limit des μ P-Budget für dieses Protokoll verwenden. Standardwert: Aktiviert
Max. μ P-Budget in [%]	Maximale μ P-Last das Modul, welche bei der Abarbeitung des Protokolls produziert werden darf. Wertebereich: 1 ... 100% Standardwert: 10%
Beschreibung	Beschreibung für den SNTP.
Aktuelle SNTP-Version	Anzeige der aktuellen SNTP.
Stratum des Zeitervers	Das Stratum eines SNTP-Servers gibt die Genauigkeit seiner lokalen Zeit wieder. Je niedriger das Stratum, desto genauer die lokale Zeit. Null bedeutet ein unspezifiziertes oder nicht verfügbares Stratum (nicht gültig). Das Stratum des SNTP-Servers muss niedriger oder gleich dem Stratum des anfragenden SNTP-Clients sein. Ansonsten wird die Zeit des SNTP-Servers vom SNTP-Client nicht übernommen. Wertebereich: 1 ... 15 Standardwert: 14

Tabelle 49: Eigenschaften SNTP-Server

5.4 Konfiguration der Zeitsynchronisation über SNTP

In der dargestellten Netzwerkstruktur wird eine HIMatrix als SNTP-Server für die Zeitsynchronisation der untergeordneten Remote I/O konfiguriert. Die HIMatrix ist zusätzlich als SNTP-Client konfiguriert und holt sich die Zeitsynchronisation vom Netzwerk-Zeitserver.

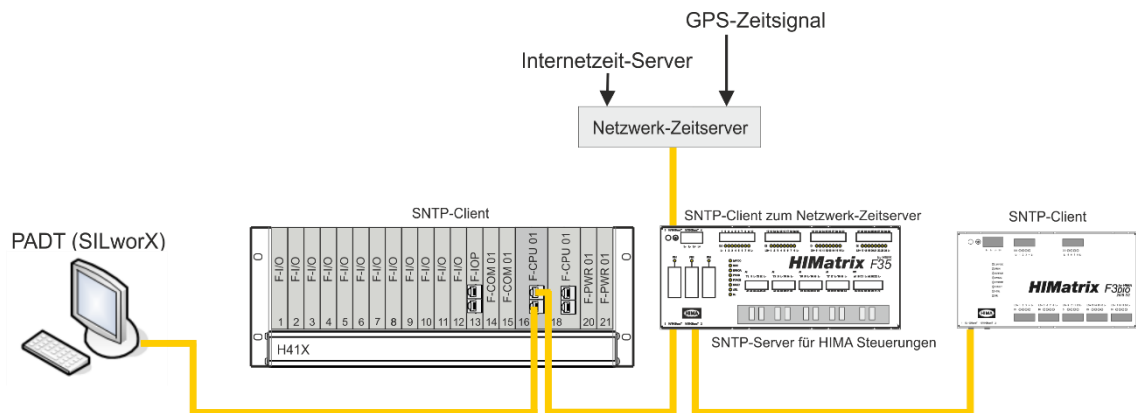


Bild 26: Zeitsynchronisation der HIMA Systeme durch den SNTP Zeitserver

5.4.1 Anlegen einer IP-Verbindung zu einem Netzwerkzeitserver

In jeder Ressource kann ein SNTP-Client zur Zeitsynchronisation konfiguriert werden.

Einen neuen SNTP-Client anlegen

1. Im Strukturbaum **Konfiguration, Ressource, Protokolle** öffnen.
2. Rechtsklick auf **Protokolle** und im Kontextmenü **Neu, SNTP-Client** wählen.
3. Im Kontextmenü vom SNTP-Client **Eigenschaften** das **COM-Modul** auswählen, das mit dem PC verbunden ist.
 - ☒ Standard Referenz Stratum '15' kann beibehalten werden, wenn das COM-Modul nicht zusätzlich auch als SNTP-Server arbeitet.

Regel: Stratum des SNTP-Servers ≤ Stratum des anfragenden SNTP-Clients. Ansonsten wird die Zeit des SNTP-Servers vom SNTP-Client nicht übernommen.

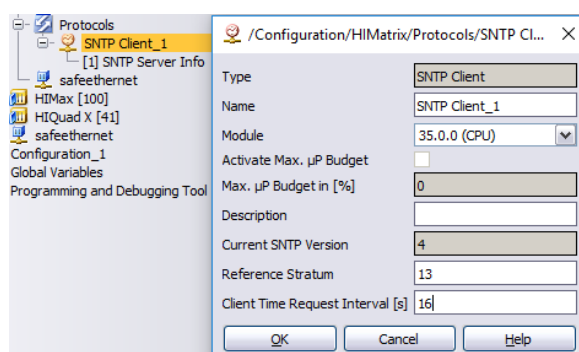


Bild 27: SNTP-Client zur Zeitsynchronisation konfigurieren

Unterhalb des SNTP-Clients den SNTP- Server Info konfigurieren

1. Im Strukturbaum **Konfiguration, Ressource, Protokolle, SNTP Client** öffnen.
2. Rechtsklick auf **SNTP-Server Info** und **Eigenschaften** wählen.
3. Im Kontextmenü von SNTP-Server Info **Eigenschaften** die **IP-Adresse** des SNTP-Server (PCs) auswählen.

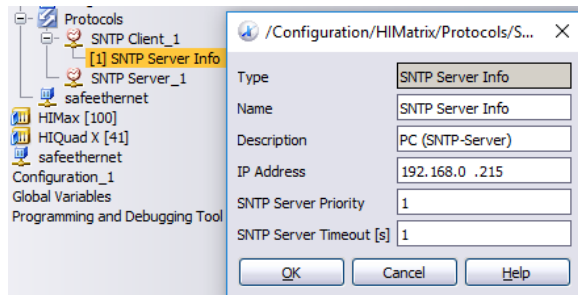


Bild 28: IP-Verbindung zum SNTP-Server (PC) konfigurieren

5.4.2 SNTP Zeitsynchronisation einer Remote I/O durch eine HIMA Ressource

Die Remote I/O wird über SNTP synchronisiert. Bei der übergeordneten HIMA Ressource muss hierzu ein SNTP Server angelegt werden, der durch einen Internet-Zeitserver oder einer GPS-Uhr zeitsynchronisiert wird.

Einen SNTP-Server für die SNTP Zeitsynchronisation anlegen

1. Im Strukturbaum **Konfiguration, Ressource, Protokolle** öffnen.
2. Rechtsklick auf **Protokolle** und im Kontextmenü **Neu, SNTP-Server** wählen.
☒ Ein neuer SNTP Server wird hinzugefügt.
3. Im Kontextmenü vom SNTP Server **Eigenschaften** das **Modul** auswählen, mit dem die Remote I/O verbunden wird. Es muss das identische Modul sein worüber die safeethernet-Anbindung zur Remote I/O läuft. Das Stratum darf maximal 14 sein.

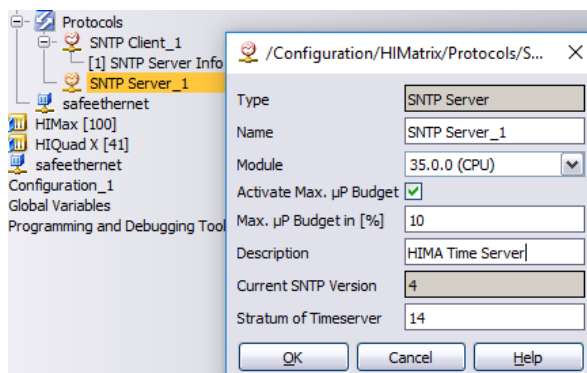


Bild 29: Einen SNTP-Server für die SNTP Zeitsynchronisation anlegen

6 HART

Das HART Protokoll (Highway Addressable Remote Transducer) ist eine digitale Feldbus-Kommunikation bei welchem dem analogen Stromsignal (4 ... 20 mA) das HART Signal aufmoduliert wird. Die Datenübertragungsrate des HART Protokolls beträgt 1200 Bit/s. Über das HART Signal werden Mess- und Gerätedaten angeschlossener HART-fähiger Sensoren oder Aktoren übertragen.

Das X-HART 32 01 Modul stellt die digitale HART-Feldbus-Kommunikation zwischen maximal 32 HART-fähigen Feldgeräten und dem HIMax System her.

Über das HART-Signal werden Mess- und Gerätedaten angeschlossener HART-fähiger Sensoren oder Aktoren übertragen. Die Mess- und Gerätedaten werden vom X-HART 32 01 Modul zu dem zugeordneten Kommunikationsmodul X-COM 01 systemintern übertragen. Vom X-COM 01 werden die Mess- und Gerätedaten über das HART-IP Protokoll an ein Asset-Management-System oder einen HART OPC Server übertragen.



HIMA empfiehlt, für die Reduzierung von Security-Risiken unautorisierte Änderungen an den HART-Feldgeräten per Schreibschutz zu verhindern.

6.1 Systemanforderung

Benötigte Ausstattung und Systemanforderung für HART-Protokoll:

Element	Beschreibung
Steuerung	HIMax mit X-COM-Modul und X-HART-Modul
X-CPU-Modul	Die Ethernet-Schnittstellen werden für HART-IP nicht verwendet. Für modulweise Parametrierung: CPU Betriebssystem ab V5 Für kanalweise Parametrierung: CPU Betriebssystem ab V11.x
X-COM-Modul	Ethernet 10/100BaseT werden für HART-IP verwendet. COM-Betriebssystem ab 7.24.
X-HART 32 01	Für modulweise Parametrierung: IO-Betriebssystem ab V5. Für kanalweise Parametrierung: IO-Betriebssystem ab V7.48.
Analoges Modul	Analoges Eingangs- oder Ausgangsmodul.
Aktivierung	Das HART-IP Protokoll ist für HIMax Systeme standardmäßig freigeschaltet.

Tabelle 50: Systemanforderung und Ausstattung für HART-Protokoll

6.1.1 Eigenschaften HART-Protokoll

Das HART-Protokoll hat die in der folgenden Tabelle aufgeführten Eigenschaften.

Eigenschaften	Beschreibung	
Sicherheitsbezogen	Nein	
Übertragungsrate	HART-Feldbus-Kommunikation: 1200 Bit/s HART-IP über Ethernet: 100 Mbit/s voll duplex	
Transportweg	HART-Feldbus-Kommunikation	
	32 kanalige HART-Schnittstelle des X-HART-Moduls.	
	HART-IP über Ethernet	
	Ethernet-Schnittstellen der X-COM-Module Verwendete Ethernet-Schnittstellen simultan auch für andere Protokolle nutzbar.	
Max. Anzahl X-HART-Module	100 pro HIMax System. Resultiert aus Dimensionierung, siehe Systemhandbuch HI 801 000 D.	
Max. Anzahl E/A Punkte	3200 pro HIMax System. Abhängig vom Modultyp, hier für 100 analoge Module mit	

Eigenschaften	Beschreibung
	jeweils 32 Eingängen.
Max. Anzahl HART-IP Protokollinstanzen	1 pro X-COM-Modul. 2 pro HIMax System (mit 2 X-COM-Modulen).
Max. Anzahl HART-IP Sessions über UDP	2 auf jedem X-COM-Modul.
Max. Anzahl HART-IP Sessions über TCP	2 auf jedem X-COM-Modul.

Tabelle 51: Eigenschaften HART-Protokoll

6.2 HART-Kommunikation für sicherheitsbezogene Anwendungen

Die HART-Kommunikation bietet die Möglichkeit, lesend und schreibend auf die Transmitter zuzugreifen und dadurch gegebenenfalls auch die Konfiguration des Transmitters zu ändern.

Da das HART-IP-Protokoll nicht nach den Anforderungen der IEC 61508 entwickelt worden ist, dürfen die über HART gelieferten Daten auch nicht als verlässliche Quelle für sicherheitsbezogene Funktionen genutzt werden.

Die über das HART-Protokoll gelieferten Informationen können innerhalb von Asset-Management-Systemen, z. B. für Diagnose, genutzt werden.

Die sicherheitsbezogenen Analogwerte werden in der sicherheitsbezogenen HIMA Steuerung und die HART-Daten im Asset-Management-System verarbeitet (Schutzebenen nach IEC 61511).

6.2.1 Sicherheitsfunktion

Die Sicherheitsfunktion der HART-Kommunikation über das HIMax System umfasst die folgenden Punkte:

- HART-Deaktivierung: Im abgeschalteten Fall werden HART-Kanäle gemäß SIL 3 sicher deaktiviert.
- HART-Filterung: HART-Zugriffe auf Transmitter oder Sensoren werden gemäß SIL 3 gesperrt.
- Die HART-Kommunikation beeinflusst die Genauigkeit der analogen Messung um 1 %. Weitere Rückwirkungen auf die analogen HIMax Module sind ausgeschlossen.
- HART-Parametrierung: Die Parametrierung des X-HART-Moduls kann modulweise für alle 32 Kanäle oder kanalweise für jeden einzelnen Kanal durchgeführt werden.

WARNUNG



Manipulation der analogen Sensoren und Aktoren!

Wird die HART-Filterung auf dem X-HART-Modul deaktiviert, ist ein Umprogrammieren des zugehörigen analogen Sensors oder Aktors möglich.

Der Betreiber hat dafür zu sorgen, dass die für das HART Protokoll verwendeten HART-Feldgeräte ausreichend vor Manipulationen (z. B. durch Hacker) geschützt sind. Art und Umfang der Maßnahmen sind mit der abnehmenden Prüfstelle abzustimmen, siehe auch Kapitel 2.5.

6.3 Konfiguration einer HART-IP-Protokollinstanz

Dieses Kapitel gibt einen Überblick zur Konfiguration der HART-IP-Protokollinstanz und dem Zusammenwirken von HART-Feldgerät, HIMax-Steuerung, Engineering-Tool und eines HART OPC Server oder FDT/DTM Asset-Management-Systems.

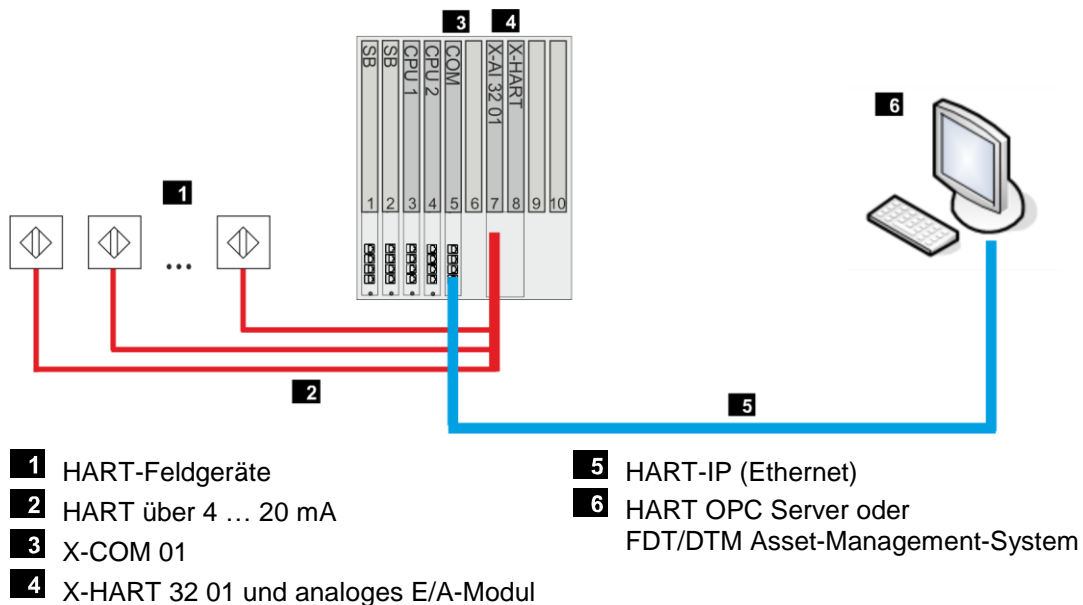


Bild 30: Aufbau der HART-IP Installation

6.3.1 HART OPC Server oder FDT/DTM Asset-Management-System

Zur Parametrierung und Überwachung der HART-Feldgeräte kann ein HART OPC Server oder ein FDT/DTM Asset-Management-System eingesetzt werden.

Unterstützte Asset-Management-Systeme z. B.

- PACTWARE.
- FIELD CARE.
- Honeywell FDM.
- Yokogawa FieldMate.
- Weitere auf Anfrage.

Ein geeigneter HART OPC Server kann von der HART-Foundation bezogen werden.

i

Die beiden Gerätetreiber *CommDTM* und *DeviceDTM* für das HIMax System können von HIMA bezogen werden.

6.3.2 HART-Feldgeräte

Die HART-Feldgeräte müssen an die analogen Eingangs- oder Ausgangsmodule (z. B. X-AI 32 01, X-AO 16 01) angeschlossen sein. Bei Leitungsbruch oder Leitungsschluss ist keine HART-Kommunikation möglich.

i

HIMA empfiehlt, an allen angeschlossenen HART-Feldgeräten die Polling Adresse *Null* einzustellen.

Die gleiche Sub-Device Adresse für jedes angeschlossene Gerät ist möglich, da das HIMax System nur ein Feldgerät pro HART-Kanal vorsieht (kein Multidrop-Betrieb). Das *Suchen* nach angeschlossenen Feldgeräten wird mit Polling Adresse *Null* gestartet. Ein Gerät mit Adresse *Null* wird nach dem Power-On am schnellsten "gefunden".

6.3.3 X-HART-Modul, X-COM-Modul und analoge E/A-Module konfigurieren

Das Kommunikationsmodul X-COM und das zugeordnete X-HART-Modul bilden zusammen ein E/A-System im Sinne der HART-Spezifikation.

Das X-HART-Modul ist ein Kommunikationsmodul mit 32 Kanälen und wird mit einem analogen Eingangs- oder Ausgangsmodul kombiniert und über ein Connector-Board verbunden. Das jeweils geeignete Connector-Board belegt für Mono-Anwendung 2 Steckplätze und für Redundante-Anwendung 3 Steckplätze.

Die HIMax Module werden im Hardware-Editor des Programmierwerkzeugs SILworX konfiguriert.

So fügen Sie im Hardware-Editor die benötigten Module hinzu

1. Im Strukturbaum **Konfiguration, Ressource, Hardware** selektieren.
2. Im Kontextmenü von Hardware **Edit** wählen, um den Hardware-Editor zu öffnen.
3. Aus der Objektauswahl die Module **X-COM 01**, **X-AI 32 01** und **X-HART 32 01** per Drag&Drop auf eine geeignete Position im Bais-Rack ziehen.

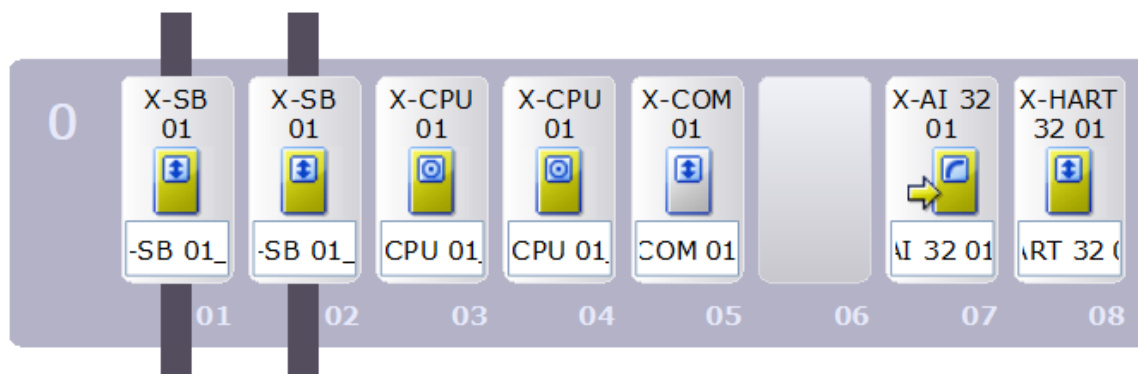


Bild 31: HART-IP Konfiguration im SILworX Hardware-Editor

6.3.3.1 Analoges Eingangsmodul X-AI 32 01

Die X-AI 32 01 wird in der Detailansicht des Hardware-Editors konfiguriert.

So öffnen Sie die Detailansicht der X-AI 32 01 im Hardware-Editor

1. Rechtsklick auf **X-AI 32 01** und im Kontextmenü, **Detailansicht** wählen.
 - ☒ Die Detailansicht enthält einen eigenen Arbeitsbereich, teilweise mit weiteren Registern für die Parametrierung der Objekte und analogen Eingänge.



Für weitere Informationen zur Konfiguration der X-AI 32 01, siehe Handbuch HI 801 020 D.

6.3.3.2 X-HART-Modul

Das X-HART-Modul wird in der Detailansicht des Hardware-Editors konfiguriert.

So öffnen Sie die Detailansicht des X-HART-Moduls im Hardware-Editor

1. Rechtsklick auf **X-HART** und im Kontextmenü, **Detailansicht** wählen.
 - ☒ Die Detailansicht enthält einen eigenen Arbeitsbereich, teilweise mit weiteren Registern für die Parametrierung der Objekte.

Bei der Konfiguration sind folgende Punkte zu beachten:

- Zugehöriges analoges Eingangs- oder Ausgangsmodul (z. B. X-AI 32 01) konfigurieren.
- Zur Diagnose des X-HART-Moduls und der HART-Kanäle können die Systemparameter mit Globalen Variablen verbunden und im Anwenderprogramm ausgewertet werden.
- Bei analogen Ausgangsmodulen in redundanter Verschaltung ist zusätzlich der Parameter *Modul-Status* mit zu berücksichtigen, siehe X-AO 16 01 Modulhandbuch HI 801 110 D.



Für weitere Informationen zur Konfiguration des X-HART-Moduls, siehe Handbuch HI 801 306 D.

6.3.3.3 Konfiguration des X-COM-Moduls in der Detailansicht

Die X-COM 01 wird in der Detailansicht des Hardware-Editors konfiguriert.

So öffnen Sie die Detailansicht der X-COM 01 im Hardware-Editor

1. Rechtsklick auf **X COM 01** und im Kontextmenü, **Detailansicht** wählen.
 - ☒ Die Detailansicht enthält einen eigenen Arbeitsbereich, teilweise mit weiteren Registern für die Parametrierung der Objekte.
2. **IP-Adresse** zur Verbindung mit dem HART OPC Server oder FDT/DTM Asset-Management-System eintragen.



Für weitere Informationen zur Konfiguration der X-COM 01, siehe Handbuch HI 801 010 D.

6.3.4 Konfiguration der HART-IP Protokollinstanz

Das Protokoll und die benötigten HIMax Module werden im Programmierwerkzeug SILworX konfiguriert.

So legen Sie eine HART-IP Protokollinstanz an

1. Im Strukturbaum **Konfiguration, Ressource, Protokolle** selektieren.
2. Im Kontextmenü von Protokolle **Neu, HART-IP-Protokoll** wählen, um ein neues HART-IP-Protokoll hinzuzufügen.
3. Im Kontextmenü des HART-Protokolls, **Eigenschaften des X-COM-Moduls** auswählen.
Die Standardeinstellungen können für die erste Konfiguration beibehalten werden.

6.3.4.1 Eigenschaften

Das Dialogfenster Eigenschaften des HART-IP Protokolls enthält die folgenden Parameter.

Element	Beschreibung
Name	Name für HART-IP-Protokoll.
Modul	Auswahl des COM-Moduls, auf dem das HART-IP Protokoll abgearbeitet wird.
Max. μ P-Budget aktivieren	Aktiviert: Limit des μ P-Budget aus dem Feld <i>Max. μP-Budget in [%]</i> übernehmen. Deaktiviert: Kein Limit des μ P-Budget, für dieses Protokoll verwenden. Standardwert: Aktiviert
Max. μ P-Budget in [%]	Maximales μ P-Budget des Moduls, welches bei der Abarbeitung des Protokolls produziert werden darf. Wertebereich: 1 ... 100% Standardwert: 30%
Polling-Adresse	Polling-Adresse der X-COM Wertebereich: 0 ... 63 Standardwert: 0
Standard HART TCP Port (5094) verwenden	Aktiviert TCP-Verbindung aktiviert. Deaktiviert TCP-Verbindung deaktiviert. Standardwert: Aktiviert, es wird TCP Port 5094 verwendet.
Zweiten HART TCP Port verwenden	Aktiviert TCP-Verbindung aktiviert Deaktiviert TCP-Verbindung deaktiviert Standardwert: Deaktiviert
Zweiter HART TCP Port	Die zweite Portnummer kann alternativ oder zusätzlich zum Standard Port verwendet werden. Wertebereich: 1 ... 65535 Standardwert: 20004
Standard HART UDP Port (5094) verwenden	Aktiviert UDP-Verbindung aktiviert. Deaktiviert UDP-Verbindung deaktiviert. Standardwert: Aktiviert, es wird UDP Port 5094 verwendet.
Zweiten HART UDP Port verwenden	Aktiviert UDP-Verbindung aktiviert. Deaktiviert UDP-Verbindung deaktiviert. Standardwert: Deaktiviert
Zweiter HART UDP Port	Die zweite Portnummer kann alternativ oder zusätzlich zum Standard Port verwendet werden. Wertebereich: 1 ... 65535 Standardwert: 20004

Tabelle 52: Eigenschaften des HART-IP Protokolls

6.4 Online-Ansicht des X-COM-Moduls

In der Online-Ansicht des X-COM-Moduls kann der Anwender die Einstellungen des HART-Protokolls überprüfen und steuern. Zudem werden aktuelle Statusinformationen der Feldgeräte und des X-COM-Moduls angezeigt.

So öffnen Sie die Online-Ansicht des Hardware-Editors des HART-Protokolls

1. Im Strukturbaum **Hardware** selektieren und im Kontextmeü **Online** wählen.
2. Im **System-Login**, Zugangsdaten eingeben um die Online Ansicht der Hardware zu öffnen.
3. Doppelklick auf **X-COM-Modul** und im Strukturbaum **HART-Protokoll** wählen.

6.4.1 Anzeigefeld (HART-Protokoll)

Im Anzeigefeld werden die folgenden Werte des selektierten HART-Protokolls angezeigt.

Element	Beschreibung
Name	Name für HART-Protokoll.
Projektiertes μ P-Budget [%]	Anzeige des projektierten maximalen μ P-Budget des X-COM-Moduls, welches bei der Abarbeitung des Protokolls produziert werden darf.
Aktuelles μ P-Budget [%]	Anzeige des aktuellen μ P-Budget des X-COM-Moduls, welches bei der Abarbeitung des Protokolls momentan produziert wird.
Polling-Adresse	Anzeige der X-COM Polling-Adresse. Wertebereich: 0 ... 63
Eindeutige Adresse der X-COM	Die 5 Byte Adresse der X-COM (Unique Adresse) wird angezeigt.
Standard HART TCP Port Nummer	Der für HART-IP genutzte Standard TCP Port wird online angezeigt.
Zweiten HART TCP Port Nummer	Der für HART-IP genutzte zusätzliche oder alternative TCP Port wird online angezeigt.
Standard HART UDP Port Nummer	Der für HART-IP genutzte Standard UDP Port wird online angezeigt.
Zweite HART UDP Port Nummer	Der für HART-IP genutzte zusätzliche oder alternative UDP Port wird online angezeigt.
Anzahl HART-Geräte	Es wird die Anzahl HART-Geräte angezeigt, die aktuell als angeschlossen erkannt werden. Die X-COM 01, die Teil auch der HART-Konfiguration ist, ist hierbei nicht enthalten.
Anzahl X-HART-Module	Es wird die Anzahl X-HART 32 01 Module (IO-Cards) angezeigt, die zu diesem X-COM 01 Modul gehören und erkannt wurden.
Status Gerätesperre	Es wird der Status der Gerätesperre angezeigt. Die Gerätesperre (Sperre des HART-IO-Subsystems) wird vom Host über das HART-Kommando 71 ausgeführt. Wertebereich: Siehe HCF_SPEC-183 (Common Tables) Table 25 Null - Gerät nicht gesperrt Ungleich Null - Lock Device Status Code Standardwert: 0
Gerätesperre durch Host mit IP	Bei aktiver Gerätesperre (Status Gerätesperre nicht Null) wird hier die IP-Adresse des Hosts angezeigt, der die Gerätesperre ausgeführt hat (d.h. das HART-Kommando 71 gesendet hat). Wertebereich: IP-Adresse Standardwert: 0

Tabelle 53: Online-Ansicht des HART-Protokolls

6.4.2 Online-Ansicht der Geräteliste

So wird die Geräteliste aktualisiert

1. Im Strukturbaum **HART-Protokoll, Geräteliste** wählen.
2. Rechter Mausklick und **Geräteliste aktualisieren** wählen.

In dem Anzeigefeld Geräteliste werden die folgenden Werte angezeigt.

Element	Beschreibung
Geräteindex	Der Index des Geräts wird online angezeigt. Wertebereich: 0 ... 65535 (dezimal, 2 Bytes)
IO-Card-Nummer	Die IO-Card Nummer an der das Gerät angeschlossen ist wird online angezeigt. Wertebereich: 0 ... 249 (dezimal, 1 Byte) für angeschlossene Geräte. Wert: 251 ("None") für die X-COM selbst.
Kanal-Nummer	Die Nummer des Kanals an der das Gerät angeschlossen ist wird online angezeigt. Wertebereich: 1 ... 31 (dezimal, 1 Byte) für angeschlossene Geräte, siehe Kapitel 6.4.2.1. Wertebereich: 251 ("None") für die X-COM selbst.
Hersteller-ID	Die Hersteller ID des Geräts wird online angezeigt. Wertebereich: 0x00 ... 0xFFFF (hexadezimal, 2 Bytes)
Expanded Device Type Code	Der Expanded Device Type Code des Geräts wird online angezeigt. Wertebereich: 0x00 ... 0xFFFF (hexadezimal 2 Bytes)
Device ID	Die Device ID des Geräts wird online angezeigt. Wertebereich: 0x00 0x00 0x00 ... 0xFF 0xFF 0xFF (hexadezimal 3 Bytes)
HART-Version	Die HART-Version (Universal Command Revision Level) des Geräts wird online angezeigt. Wertebereich 0 ... 255 (dezimal 1 Byte)
Long Tag	Das Long Tag des Geräts wird online angezeigt. Wertebereich 32 Zeichen (Latin-1)
Rack.Slot IO-Card	Der Steckplatz (Rack.Slot) der IO-Card wird online angezeigt. Format: Rack.Slot Wertebereich Rack: 0 ... 15 Wertebereich Slot: 0 ... 15
Telegrammzähler STX	Der Telegrammzähler für Kommandos (Stx) des Geräts wird online angezeigt. Wertebereich 0 ... 65535 (dezimal 2 Bytes umlaufend)
Telegrammzähler ACK	Der Telegrammzähler für Antworten (Ack) des Geräts wird online angezeigt. Wertebereich 0 ... 65535 (dezimal 2 Bytes umlaufend)
Telegrammzähler BACK	Der Telegrammzähler für Burst-Antworten (Back) des Geräts wird online angezeigt. Wertebereich 0 ... 65535 (dezimal 2 Bytes umlaufend)

Tabelle 54: Online-Ansicht der Geräteliste

6.4.2.1 Adressierung der HART-Feldgeräte

Kanal-Nummer (X-HART 32 01 Frontplatte)	Kanal-Adresse (dezimal)	Kanal-Adresse (hexadezimal)
1 ... 32	0 ... 31	0x00 ... 0x1f

Tabelle 55: Adressierung der HART-Feldgeräte

Die in der Online Ansicht der X-COM 01 angezeigten Kanal-Nummern entsprechen den Kanal-Nummern auf der Frontplatte des X-HART 32 01 Moduls (Kanalzählweise beginnend mit 1).

Bei der Adressierung eines angeschlossenen HART-Feldgerätes gilt:

Kanal-Adresse (channel number bei Kommando 77) = Kanal-Nummer - 1

Beispiel:

Kanal Nummer = 15

Das Feldgerät wird mit der Kanal-Adresse = 14 (0x0e) adressiert

7 Allgemein

In diesem Kapitel sind Parameter gesammelt, die für alle Kommunikationsprotokolle relevant sind.

7.1 Maximale Kommunikationszeitscheibe

Die maximale Kommunikationszeitscheibe ist die zugeteilte Zeit in Millisekunden (ms) pro CPU-Zyklus, innerhalb der das Prozessormodul die Kommunikationsaufgaben abarbeitet. Wenn die Protokollverarbeitung innerhalb der Dauer einer Kommunikationszeitscheibe nicht beendet werden konnte, führt die CPU dennoch die sicherheitsrelevanten Überwachungen für alle Protokolle in einem CPU-Zyklus aus.

i

Wenn nicht alle in einem CPU-Zyklus anstehenden Kommunikationsaufgaben ausgeführt werden können, erfolgt die komplette Übertragung der Kommunikationsdaten über mehrere CPU-Zyklen. Die Anzahl der Kommunikationszeitscheiben ist dann größer 1.

Für die Berechnungen der zulässigen maximalen Reaktionszeiten gilt die Bedingung, dass die Anzahl der Kommunikationszeitscheiben genau 1 ist.

7.1.1 Ermitteln der maximalen Dauer der Kommunikationszeitscheibe

Für eine erste Abschätzung der maximalen Dauer der Kommunikationszeitscheibe müssen die folgenden Zeiten aufsummiert und das Ergebnis in den Systemparameter *Max. Kom.-Zeitscheibe [ms]* in den Eigenschaften der Ressource eingetragen werden:

- Pro COM-Modul 3 ms.
- Pro redundante **safeethernet** Verbindung 1 ms.
- Pro nicht redundante **safeethernet** Verbindung 0,5 ms.
- Pro KByte Nutzdaten bei nichtsicheren Protokollen (z. B. Modbus) 1 ms.

HIMA empfiehlt, den abgeschätzten Wert *Max. Kom.-Zeitscheibe [ms]* mit dem im Control Panel angezeigten Wert zu vergleichen und gegebenenfalls in den Eigenschaften der Ressource zu korrigieren. Dies kann z. B. in einem FAT (Factory Acceptance Test) oder SAT (Site Acceptance Test) durchgeführt werden.

Ermitteln der tatsächlichen Dauer der maximalen Kommunikationszeitscheibe

1. Das HIMA System unter voller Last betreiben (FAT, SAT):
Alle Kommunikationsprotokolle sind in Betrieb (**safeethernet** und Standardprotokolle).
2. Das **Control Panel** öffnen und im Strukturbaum das Verzeichnis **Kom.-Zeitscheibe** wählen.
3. Anzeige *Maximale Kom.-Zeitscheibe Dauer pro Zyklus [ms]* auszulesen.
4. Anzeige *Maximale Anzahl benötigter Kom.-Zeitscheibe Zyklen* auszulesen.

Die Dauer der Kommunikationszeitscheibe ist so hoch einzustellen, dass der CPU-Zyklus die vom Prozess vorgegebene Watchdog-Zeit nicht überschreiten kann, wenn er die eingestellte Kommunikationszeitscheibe ausnutzt.

7.2 Lastbegrenzung

Für jedes Kommunikationsprotokoll kann ein Rechenzeitbudget in % (*μP-Budget*) vorgegeben werden. So kann die verfügbare Rechenzeit zwischen den konfigurierten Protokollen verteilt werden. Die Summe der Rechenzeitbudgets aller parametrisierten Kommunikationsprotokolle eines CPU- oder COM-Moduls darf nicht größer als 100 % sein.

Die festgelegten Rechenzeitbudgets der einzelnen Kommunikationsprotokolle werden überwacht. Hat ein Kommunikationsprotokoll sein Rechenzeitbudget erreicht oder überschritten und es steht keine zusätzliche Rechenzeit als Reserve zur Verfügung, so wird das Kommunikationsprotokoll nicht komplett abgearbeitet.

Wenn noch genügend zusätzliche Rechenzeit vorhanden ist, wird diese verwendet, um ein Kommunikationsprotokoll, das sein Rechenzeitbudget erreicht oder überschritten hat noch abzuarbeiten. Dadurch kann es vorkommen, dass ein Kommunikationsprotokoll tatsächlich ein höheres Rechenzeitbudget verwendet als ihm zugeteilt wurde.

Eventuell werden über 100 % Rechenzeitbudget online angezeigt. Dies ist kein Fehler, das Rechenzeitbudget über 100 % ist die zusätzlich verwendete Rechenzeit.

i

Das zusätzliche Rechenzeitbudget ist keinesfalls eine Zusicherung für ein bestimmtes Kommunikationsprotokoll und kann jederzeit vom System zurückgenommen werden.

7.3 Konfiguration der Funktionsbausteine

Die Feldbus-Protokolle und die zugehörigen Funktionsbausteine laufen auf dem COM-Modul des HIMA Systems. Daher müssen diese Funktionsbausteine im SILworX Strukturbaum unter **Konfiguration, Ressource, Protokolle...** angelegt werden.

Um diese Funktionsbausteine auf dem COM-Modul zu steuern, können im Anwenderprogramm von SILworX Funktionsbausteine angelegt werden (siehe Kapitel 7.3.1), die wie Standard-Funktionsbausteine verwendet werden können.

Die Verbindung der Funktionsbausteine im Anwenderprogramm von SILworX mit den entsprechenden Funktionsbausteinen im Strukturbaum von SILworX erfolgt über gemeinsame Variablen. Diese müssen zuvor vom Anwender im Variablen-Editor erstellt werden.

7.3.1 Beschaffung der Funktionsbausteinbibliotheken

Die Funktionsbausteinbibliotheken für PROFIBUS DP und TCP Send/Receive müssen über die Funktion *Wiederherstellen...* (Kontextmenü des Projekts) dem Projekt hinzugefügt werden.

Die Funktionsbausteinbibliothek ist auf Anfrage über den HIMA Support erhältlich.

7.3.2 Konfiguration der Funktionsbausteine im Anwenderprogramm

Die benötigten Funktionsbausteine können per Drag&Drop in das Anwenderprogramm kopiert werden. Die Eingänge und Ausgänge sind nach der Beschreibung des jeweiligen Funktionsbausteins zu konfigurieren.

Oberer Teil des Funktionsbausteins

Der obere Teil des Funktionsbausteins entspricht der Benutzerschnittstelle, über die der Funktionsbaustein vom Anwenderprogramm gesteuert wird.

Hier werden die Variablen verbunden, die im Anwenderprogramm verwendet werden. Das Präfix "A" steht für "Applikation".

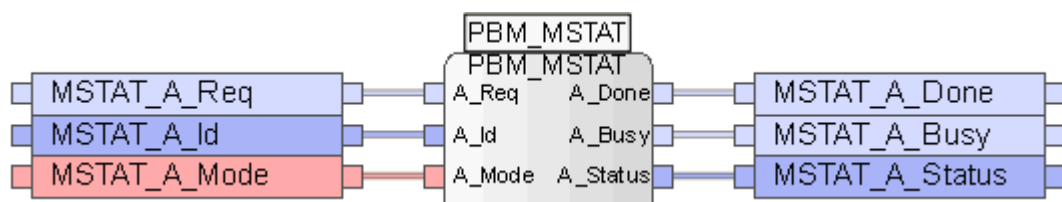


Bild 32: Funktionsbaustein PNM_MSTST (oberer Teil)

Unterer Teil des Funktionsbausteins

Der untere Teil des Funktionsbausteins stellt die Verbindung zum Funktionsbaustein (im Strukturbaum von SILworX) dar.

Hier werden die Variablen verbunden, die mit dem Funktionsbaustein im Strukturbaum von SILworX verbunden werden müssen. Das Präfix "F" steht für "Field".

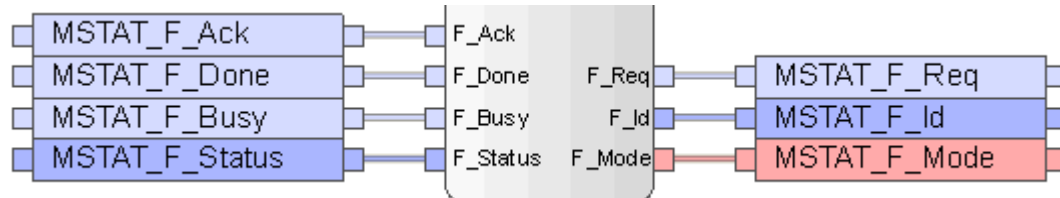


Bild 33: Funktionsbaustein PNM_MSTST (unterer Teil)

7.3.3 Konfiguration der Funktionsbausteine im Strukturbaum von SILworX

Den Funktionsbaustein im Strukturbaum von SILworX anlegen:

1. Im Strukturbaum **Konfiguration, Ressource, Protokolle**, z. B. **PROFIBUS Master** wählen.
2. Rechtsklick auf **Funktionsbausteine** und **Neu** wählen.
3. Den passenden Funktionsbaustein (im Strukturbaum von SILworX) auswählen.

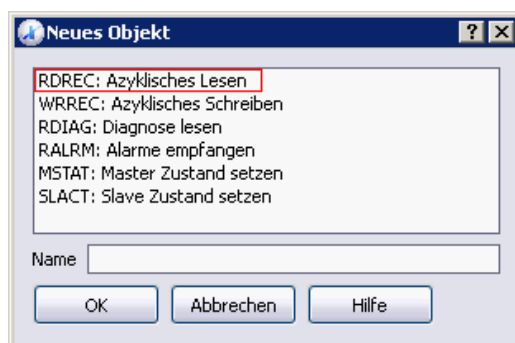


Bild 34: Auswahl Funktionsbausteine

Die Eingänge des Funktionsbausteins (Häkchen in Spalte Eingangsvariable) müssen mit den gleichen Variablen verbunden werden, die mit den *F-Ausgängen* des Funktionsbausteins im Anwenderprogramm verbunden sind.

Die Ausgänge des Funktionsbausteins (kein Häkchen in Spalte Eingangsvariable) müssen mit den gleichen Variablen verbunden werden, die mit den *F-Eingängen* des Funktionsbausteins im Anwenderprogramm verbunden sind.

Systemvariablen					
F	Name	Datentyp	Transfer-Operation	Eingangsvariable	Globale Variable
1	ACK	BOOL		5 <input checked="" type="checkbox"/>	MSTAT_F_Ack
2	BUSY	BOOL		5 <input checked="" type="checkbox"/>	MSTAT_F_Busy
3	DONE	BOOL		5 <input checked="" type="checkbox"/>	MSTAT_F_Done
4	REQ	BOOL		5 <input type="checkbox"/>	MSTAT_F_Req
5	M_ID	DWORD		5 <input type="checkbox"/>	MSTAT_F_Id
6	STATUS	DWORD		5 <input checked="" type="checkbox"/>	MSTAT_F_Status
7	MODE	INT		5 <input type="checkbox"/>	MSTAT_F_Mode

Bild 35: Systemvariablen des Funktionsbausteins MSTAT

Anhang

Glossar

Begriff	Beschreibung
ARP	Address Resolution Protocol: Netzwerkprotokoll zur Zuordnung von Netzwerkadressen zu Hardwareadressen.
Bit-Variable	Variable, die bitweise adressiert wird.
CENELEC	Comité Européen de Normalisation Électrotechnique (Europäisches Komitee für elektrotechnische Normung)
Connector Board	Anschlusskarte für HIMax Modul.
COM	Kommunikationsmodul
CPU	Prozessormodul
CRC	Cyclic Redundancy Check, Prüfsumme
Dataview	Einer Dataview sind die Globalen Variablen für Eingangs- und Ausgangsdaten für den Zugriff durch Modbus-Quellen zugeordnet.
EN	Europäische Normen
Exportbereich	Als Exportbereich wird die Prozessdatenmenge bezeichnet, die vom System (aus einem Anwenderprogramm, HW-Eingang oder einem anderen Protokoll) geschrieben und vom Modbus Master gelesen werden kann.
FB	Feldbus
FBS	Funktionsbausteinsprache
ICMP	Internet Control Message Protocol: Netzwerkprotokoll für Status- und Fehlermeldungen.
IEC	Internationale Normen für die Elektrotechnik.
Importbereich	Als Importbereich wird die Prozessdatenmenge bezeichnet, die vom Modbus-Master geschrieben wird und als Eingangsdaten für das System (in einem Anwenderprogramm, HW-Ausgang oder einem anderen Protokoll) verwendet werden kann.
KE	Kommunikationsendpunkt
MAC-Adresse	Hardware-Adresse eines Netzwerkanschlusses (Media Access Control).
NSIP	Nicht-sicherheitsbezogenes Protokoll.
PADT	Programming and Debugging Tool (nach IEC 61131-3), PC mit SILworX.
PE	Schutzerde
PELV	Protective Extra Low Voltage: Funktionskleinspannung mit sicherer Trennung.
PES	Programmierbares Elektronisches System
R	Read
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.
R/W	Read/Write
Register-Variable	Variable, die wortweise adressiert wird.
SB	Systembusmodul
SFF	Safe Failure Fraction, Anteil der sicher beherrschbaren Fehler.
SIF	Sicherheitstechnische Funktion
SIL	Safety Integrity Level (nach IEC 61508)
SILworX	Programmiersoftware für HIMax, HIQuad X und HIMatrix.
SIP	Sicherheitsbezogenes Protokoll
SNTP	Simple Network Time Protocol (RFC 1769)
SRS	System.Rack.Slot
SW	Software

Begriff	Beschreibung
TMO	Timeout
W	Write
WD	Watchdog
WDZ	Watchdog-Zeit

Abbildungsverzeichnis

Bild 1:	Beispiel zur Aufteilung des Switchports durch VLAN	25
Bild 2:	RS485 Bus-Topologie	35
Bild 3:	Busanschluss und Busabschluss, Pin-Belegung der Feldbus-Schnittstelle	36
Bild 4:	Flexible Systemstruktur mit safeethernet	40
Bild 5:	Aufbau zur Konfiguration einer redundanten Verbindung	44
Bild 6:	Ansicht im safeethernet Editor	45
Bild 7:	Ansicht im safeethernet Verbindungseditors	45
Bild 8:	safeethernet Übersicht des Beispiels in Bild 9	54
Bild 9:	Mono safeethernet Verbindung (Kanal 1)	54
Bild 12:	Parallele safeethernet Redundanz	55
Bild 13:	safeethernet Ring-Verschaltung	56
Bild 14:	Reaktionszeit bei Verbindung zweier HIMax Steuerungen	62
Bild 15:	Reaktionszeit bei Verbindung zweier HIQuad X Steuerungen	62
Bild 16:	Reaktionszeit bei Verbindung einer HIMax mit einer HIMatrix Steuerung	63
Bild 17:	Reaktionszeit bei Verbindung einer HIQuad X mit einer HIMatrix Steuerung	63
Bild 18:	Reaktionszeit mit zwei Remote I/Os und einer HIMax Steuerung	64
Bild 19:	Reaktionszeit mit zwei HIMax Steuerungen und einer HIMatrix Steuerung	65
Bild 20:	Reaktionszeit bei Verbindung zweier HIMatrix Steuerungen	65
Bild 21:	Reaktionszeit mit Remote I/Os	66
Bild 22:	Control Panel zur safeethernet Verbindungsübersicht	71
Bild 23:	safeethernet Verbindung zwischen Ressource A im Projekt A und der Ressource B im Projekt B	80
Bild 24:	HIMatrix Proxy-Ressource	82
Bild 25:	HIMax Proxy-Ressource	85
Bild 26:	Zeitsynchronisation der HIMA Systeme durch den SNTP Zeitserver	91
Bild 27:	SNTP-Client zur Zeitsynchronisation konfigurieren	91
Bild 28:	IP-Verbindung zum SNTP-Server (PC) konfigurieren	92
Bild 29:	Einen SNTP-Server für die SNTP Zeitsynchronisation anlegen	92
Bild 30:	Aufbau der HART-IP Installation	95
Bild 31:	HART-IP Konfiguration im SILworX Hardware-Editor	96
Bild 32:	Funktionsbaustein PNM_MSTST (oberer Teil)	103
Bild 33:	Funktionsbaustein PNM_MSTST (unterer Teil)	104
Bild 34:	Auswahl Funktionsbausteine	104

Bild 35:	Systemvariablen des Funktionsbausteins MSTAT	104
-----------------	---	------------

Tabellenverzeichnis

Tabelle 1:	Zusätzlich geltende Handbücher	7
Tabelle 2:	Verfügbare Protokolle für die HIMA Systeme	13
Tabelle 3:	HIMA System Mengengerüst für nicht-sicherheitsbezogene Protokolle	15
Tabelle 4:	Registrierung und Aktivierung der Protokolle	16
Tabelle 5:	HIMax Ethernet Schnittstellen	18
Tabelle 6:	HIQuad X und HIMatrix Ethernet Schnittstellen	19
Tabelle 7:	Konfigurationsparameter	21
Tabelle 8:	Routing Parameter	22
Tabelle 9:	Ethernet-Switch-Parameter	22
Tabelle 10:	Register VLAN	23
Tabelle 11:	Werte von LLDP für Profinet	23
Tabelle 12:	Verwendete Netzwerk-Ports (UDP-Ports)	24
Tabelle 13:	Verwendete Netzwerk-Ports (TCP-Ports)	24
Tabelle 14:	Register VLAN	25
Tabelle 15:	Optionen für Feldbus-Schnittstellen FB1 und FB2	26
Tabelle 16:	Verfügbare HIMax Komponenten	27
Tabelle 17:	Ausrüstung von HIMatrix Steuerungen mit Feldbus-Submodulen	27
Tabelle 18:	Pin-Belegung der D-Sub-Anschlüsse für RS485	28
Tabelle 19:	Pin-Belegung der D-Sub-Anschlüsse für PROFIBUS DP	28
Tabelle 20:	Pin-Belegung der D-Sub-Anschlüsse für RS232	29
Tabelle 21:	Pin-Belegung der D-Sub-Anschlüsse für RS422	29
Tabelle 22:	Pin-Belegung der D-Sub-Anschlüsse für SSI	29
Tabelle 23:	Pin-Belegung der D-Sub-Anschlüsse für CAN	30
Tabelle 24:	Pin-Belegung der Schnittstelle FB1 mit RS422	31
Tabelle 25:	Pin-Belegung der Schnittstelle FB1 mit RS485 (mit RTS)	31
Tabelle 26:	Pin-Belegung der Schnittstelle FB1/2 mit zweimal RS485 (ohne RTS)	32
Tabelle 27:	Pin-Belegung der Schnittstelle FB2 mit RS485 (ohne RTS)	32
Tabelle 28:	Pin-Belegung der Schnittstelle FB1 mit PROFIBUS DP Slave	32
Tabelle 29:	Pin-Belegung der Schnittstelle FB1/2 mit PROFIBUS DP Slave und RS485	33
Tabelle 30:	Eigenschaften der RS485 Übertragung	34
Tabelle 31:	Leitungslänge in Abhängigkeit von der Baudrate für RS 485 und PROFIBUS-DP	34
Tabelle 32:	Klemmenbelegung H 7506	36
Tabelle 33:	RS485 (RS422, RS232, SSI) Buskabel	37
Tabelle 34:	Parameter des PROFIBUS-DP Kabeltyp A	37
Tabelle 35:	safeethernet Protokoll für HIMax und HIQuad X	42
Tabelle 36:	safeethernet Protokoll für HIMatrix	43
Tabelle 37:	Parameter safeethernet Protokoll	48

Tabelle 38: Register Systemvariablen des safeethernet-Editors	52
Tabelle 39: Register Fragment-Definitionen	53
Tabelle 40: Verfügbare Ethernet-Schnittstellen	54
Tabelle 41: Beschreibung safeethernet Parameter und Bedingungen	61
Tabelle 42: Anzeigefeld der safeethernet Verbindung	72
Tabelle 43: Meldungen des Codegenerators	77
Tabelle 44: Meldungen des Betriebssystems	78
Tabelle 45: safeethernet Reload nach Änderungen	79
Tabelle 46: Systemanforderung und Ausstattung SNTP-Protokoll	87
Tabelle 47: Eigenschaften des SNTP-Client	88
Tabelle 48: Eigenschaften SNTP-Server-Info	89
Tabelle 49: Eigenschaften SNTP-Server	90
Tabelle 50: Systemanforderung und Ausstattung für HART-Protokoll	93
Tabelle 51: Eigenschaften HART-Protokoll	94
Tabelle 52: Eigenschaften des HART-IP Protokolls	98
Tabelle 53: Online-Ansicht des HART-Protokolls	99
Tabelle 54: Online-Ansicht der Geräteliste	100
Tabelle 55: Adressierung der HART-Feldgeräte	101

Index

Aktivierung	26	Signatur	73
Funktionsbausteine	103	Sicherheitsbezogenes Protokoll	38
Kommunikationszeitscheibe	102	Prozessdatenmenge	42, 43
Lastbegrenzung	102	Redundanz	42, 43
NSIP		Sicherheitsfunktion	94
Prozessdatenmenge	15	Teilenummer	
Pin-Belegungen	28, 31	HIMatrix	27
Registrierung	26	HIMax	27
safeethernet		Verbindungsverlust	
Dualkonfiguration	73	safeethernet	48
Reload	73	Wireless LAN	38
Reload Zustand	78		

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/