



Handbuch

HIMax[®]

Sicherheitshandbuch



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
8.02	Geändert: Redaktionelle Änderungen		X
10.00	Aktualisierte Ausgabe zu SILworX V10 Geändert: Kapitel Überdrehzahl-Schutzmodul X-MIO 7/6 01	X	X
11.00	Aktualisierte Ausgabe zu SILworX V11 Neu: Kapitel MultiForcen	X	X
12.00	Aktualisierte Ausgabe zu SILworX V12 Neu: Kapitel API-Sicherheitsmaßnahmen	X	X

Inhaltsverzeichnis

1	Einleitung	7
1.1	Gültigkeit und Aktualität	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	Einsatz des Systems HIMax	11
2.1	Bestimmungsgemäße Verwendung	11
2.1.1	Anwendung im Ruhestromprinzip	11
2.1.2	Anwendung im Arbeitsstromprinzip	11
2.1.3	Einsatz in Brandmelderzentralen	11
2.1.4	Explosionsschutz	11
2.2	Aufgaben der Maschinen- und Anlagenhersteller sowie des Betreibers	12
2.2.1	Anschluss von Kommunikationspartnern	12
2.2.2	Verwendung der sicherheitsbezogenen Kommunikation	12
2.3	ESD-Schutzmaßnahmen	12
2.4	Weitere Systemdokumentationen	13
3	Sicherheitskonzept	14
3.1	Sicherheit und Verfügbarkeit	14
3.1.1	PFD- und PFH-Berechnungen	15
3.1.2	Selbst-Test und Fehlerdiagnose	16
3.1.3	PADT	16
3.1.4	Redundanz	16
3.1.5	Aufbau von Sicherheitssystemen nach dem Arbeitsstromprinzip	17
3.2	Sicherheitsrelevante Zeiten	18
3.2.1	Prozess-Sicherheitszeit	18
3.2.2	Parameter «Sicherheitszeit [ms]» Ressource	18
3.2.3	Watchdog-Zeit (Ressource)	19
3.2.4	Abschätzung der Watchdog-Zeit	19
3.2.5	Watchdog-Zeit durch Test ermitteln	20
3.2.6	Reaktionszeit	21
3.3	Wiederholungsprüfung (Proof-Test nach IEC 61508)	22
3.4	Sicherheitsauflagen	23
3.4.1	Produktunabhängige Auflagen der Hardware	23
3.4.2	Produktabhängige Auflagen der Hardware	23
3.4.3	Produktunabhängige Auflagen der Programmierung	23
3.4.4	Produktabhängige Auflagen der Programmierung	24
3.4.5	Kommunikation	24
3.4.6	Wartung	24
3.4.7	Umgebungsbedingungen	25
3.5	Automation Security	26
3.5.1	Produkteigenschaften	26
3.5.2	Risikoanalyse und Planung	27
3.6	Zertifizierung	28
3.6.1	CE-Konformitätserklärung	28

3.6.2	EG-Baumusterprüfbescheinigung	28
3.6.3	Normenspiegel	29
3.6.4	Prüfbedingungen	30
3.6.5	Schadgase	32
4	Prozessormodul	33
4.1	Prozessormodul X-CPU 01	33
4.2	Prozessormodul X-CPU 31	33
4.3	Selbst-Tests	33
4.4	Reaktionen auf Fehler im Prozessormodul	33
4.5	Austausch von Prozessormodulen	33
5	Systembusmodul	35
5.1	Rack-ID	35
5.2	Attribut «Responsible»	35
6	Kommunikationsmodul	38
7	Eingangsmodule	39
7.1	Allgemein	39
7.2	Reaktion im Fehlerfall	40
7.3	Sicherheit von Sensoren, Encodern und Transmittern	40
7.4	Sicherheitsbezogene digitale Eingangsmodule	40
7.4.1	Test-Routinen	40
7.4.2	Redundanz von digitalen Eingängen	40
7.4.3	Surge auf digitalen Eingängen	40
7.5	Sicherheitsbezogene analoge Eingangsmodule	41
7.5.1	Test-Routinen	41
7.5.2	Redundanz von analogen Eingängen	41
7.5.3	Zustand von LL, L, N, H, HH bei X-AI 32 01 und X-AI 32 02	41
7.6	Sicherheitsbezogene Zählermodule	41
7.6.1	Test-Routinen	41
7.6.2	Beim Zählermodul X-CI 24 01 zu beachten!	42
7.6.3	Redundanz von Zählereingängen	42
7.7	Checklisten Eingänge	42
8	Ausgangsmodule	43
8.1	Allgemein	43
8.2	Reaktion im Fehlerfall	43
8.3	Sicherheit von Aktoren	43
8.4	Sicherheitsbezogene digitale Ausgangsmodule	44
8.4.1	Test-Routinen	44
8.4.2	Ausgangs-Störaustastung	44
8.4.3	LB-Austastung	44
8.4.4	Verhalten bei externem Kurzschluss oder Überlast	44
8.4.5	Redundanz von digitalen Ausgängen	44
8.5	Sicherheitsbezogene Relaismodule	45
8.5.1	Test-Routinen	45
8.5.2	Redundanz von Relaisausgängen	45

8.6	Sicherheitsbezogene analoge Ausgangsmodule	45
8.6.1	Test-Routinen	45
8.6.2	Ausgangs-Störaustattung	45
8.6.3	Verhalten bei externem Leitungsbruch	46
8.6.4	Beim analogen Ausgangsmodul X-AO 16 01 zu beachten!	46
8.6.5	Redundanz von analogen Ausgängen	46
8.7	Checklisten Ausgänge	46
9	Spezielle E/A-Module	47
9.1	HART-Modul X-HART 32 01	47
9.1.1	Sicherheitsfunktion	47
9.2	Überdrehzahlschutz-Modul X-MIO 7/6 01	48
9.2.1	Sicherheitsfunktion	48
9.2.2	Redundanz	48
10	Software	49
10.1	Sicherheitstechnische Aspekte von Betriebssystemen	49
10.2	Arbeitsweise und Funktionen von Betriebssystemen	49
10.3	Sicherheitstechnische Aspekte für die Programmierung	50
10.3.1	Sicherheitskonzept von SILworX	50
10.3.2	Überprüfung der Konfiguration und der Anwenderprogramme	50
10.3.3	Archivierung eines Projekts	51
10.3.4	Identifizierung von Konfiguration und Programmen	51
10.4	Parameter der Ressource	51
10.4.1	Systemparameter der Ressource	52
10.4.2	Abschließen und Aufschließen der Steuerung	60
10.5	Forcen	60
10.5.1	Verwendung von Forcen	61
10.5.2	Per Reload geänderte Zuweisung einer Datenquelle	61
10.5.3	Zeitbegrenzung	62
10.5.4	Einschränkung des Forcens	62
10.5.5	MultiForcen	62
10.6	Sicherer Versionsvergleich	64
10.7	Application Programming Interface (API) Sicherheitsmaßnahmen	66
11	Sicherheitstechnische Aspekte für Anwenderprogramme	67
11.1	Sicherheitsbezogener Einsatz	67
11.1.1	Basis der Programmierung	67
11.1.2	Schritte der Programmierung	68
11.1.3	Funktionen der Anwenderprogramme	68
11.1.4	Systemparameter der Anwenderprogramme	69
11.1.5	Hinweise zum Parameter <i>Codegenerierung Kompatibilität</i>	70
11.1.6	Code-Erzeugung	71
11.1.7	Laden und Starten des Anwenderprogramms	71
11.1.8	Reload	71
11.1.9	Online-Test	72
11.1.10	Testmodus	73
11.1.11	Online-Änderung von Systemparametern	73
11.1.12	Projekt-Dokumentation für sicherheitsbezogene Anwendungen	74
11.1.13	Multitasking	75

11.1.14	Abnahme durch Genehmigungsbehörden	75
11.2	Checkliste zur Erstellung eines Anwenderprogramms	75
12	Konfiguration der Kommunikation	76
12.1	Standardprotokolle	76
12.1.1	Verfügbare Protokolle und Übertragungsmedium	76
12.2	Sicherheitsbezogenes Protokoll safeethernet	76
12.3	Maximale Reaktionszeit für safeethernet	78
12.3.1	Berechnung der maximalen Reaktionszeit zweier HIMax Steuerungen	79
12.3.2	Berechnung der max. Reaktionszeit in Verbindung mit einer HIMatrix Steuerung	79
12.3.3	Berechnung der max. Reaktionszeit mit zwei HIMatrix Steuerungen oder Remote I/Os	80
12.3.4	Berechnung der max. Reaktionszeit mit zwei HIMax und einer HIMatrix Steuerung	80
12.4	Sicherheitsbezogenes Protokoll HIPRO-S V2	81
12.5	Sicherheitsbezogenes Protokoll PROFIsafe	81
13	Einsatz in Brandmelderzentralen	82
14	ATEX-konformer Einsatz als Sicherheits-, Kontroll- und Regelvorrichtung	84
15	Einsatz von HIMax in Zone 2	85
	Anhang	89
	Glossar	89
	Abbildungsverzeichnis	90
	Tabellenverzeichnis	91
	Index	92

1 Einleitung

Dieses Handbuch enthält Informationen für die bestimmungsgemäße Verwendung des sicherheitsbezogenen programmierbaren elektronischen Systems HIMax.

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 das System HIMax 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.
- Es sind nur zugelassene Fremdgeräte angeschlossen.

Aus Gründen der Übersichtlichkeit enthält dieses Handbuch nicht sämtliche Details aller Ausführungen des Systems.

Dieses Sicherheitshandbuch ist die Originalbetriebsanleitung im Sinne der Maschinenrichtlinie (Richtlinie 2006/42/EG).

Die Originaldokumentation für das HIMA System ist in deutscher Sprache verfasst. Es gelten die Aussagen der deutschsprachigen Dokumentation.

1.1 Gültigkeit und Aktualität

Dieses Sicherheitshandbuch ist für folgende Versionen erstellt:

- HIMax Betriebssysteme gemäß Versionsliste.
- SILworX ab Version V12.

Für die Anwendung früherer Versionen von HIMax und SILworX sind die entsprechenden früheren Revisionen dieses Handbuchs zu beachten.

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.
<i>Courier</i>	Wörtliche Benutzereingaben.
RUN	Bezeichnungen von Betriebszuständen (Großbuchstaben).
Kap. 1.2.3	Querverweise sind Hyperlinks, auch wenn sie nicht besonders gekennzeichnet sind. Im elektronischen Dokument (PDF): Wird der Mauszeiger auf einen Hyperlink positioniert, verändert er seine Gestalt. Bei einem Klick springt das Dokument zur betreffenden Stelle.

Sicherheits- und Gebrauchshinweise sind besonders gekennzeichnet.

1.3.1 Sicherheitshinweise

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

Die Sicherheitshinweise im Dokument sind wie folgt dargestellt.

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

Die Bedeutung der Signalworte ist:

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

SIGNALWORT



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

HINWEIS



Art und Quelle des Schadens!
Vermeidung des Schadens.

1.3.2 Gebrauchshinweise

Zusatzinformationen sind nach folgendem Beispiel aufgebaut:

i

An dieser Stelle steht der Text der Zusatzinformation.

Nützliche Tipps und Tricks erscheinen in der Form:

TIPP

An dieser Stelle steht der Text des Tipps.

1.4 Safety Lifecycle Services

HIMA unterstützt Sie in allen Phasen des Sicherheitslebenszyklus einer 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 für 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 Einsatz des Systems HIMax

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

Dieses Produkt wird mit SELV oder PELV betrieben. Mit dem HIMax Relaismodul X-DO 12 01 können externe Spannungen bis 250 VDC/VAC geschaltet werden. Vom Produkt selbst geht kein Risiko aus. Der Einsatz im Ex-Bereich ist nur mit zusätzlichen Maßnahmen erlaubt.

2.1 Bestimmungsgemäße Verwendung

Das Kapitel beschreibt die bestimmungsgemäße Verwendung des sicherheitsbezogenen Automatisierungssystems HIMax.

Das Automatisierungssystem ist ausgelegt für den Prozessmarkt zum Steuern und Regeln von Prozessen, Schutzsystemen, Brennersteuerungen, Maschinensteuerungen und verfahrenstechnischen Anlagen, sowie für die Fabrikautomatisierung. Für die Programmierung, Konfiguration, Überwachung, Bedienung und Dokumentation des Systems HIMax wird das HIMA Programmierwerkzeug SILworX eingesetzt.

Der redundante Betrieb von HIMax Modulen schließt den gleichzeitigen nicht-redundanten Betrieb anderer Module nicht aus.

2.1.1 Anwendung im Ruhestromprinzip

Das HIMax System ist für das Ruhestromprinzip konzipiert.

Ein System, das nach dem Ruhestromprinzip funktioniert, schaltet z. B. einen Aktor aus, um seine Sicherheitsfunktion auszuführen (de-energize to trip).

2.1.2 Anwendung im Arbeitsstromprinzip

Das HIMax System kann in Arbeitsstrom-Anwendungen eingesetzt werden.

Ein System, das nach dem Arbeitsstromprinzip funktioniert, schaltet z. B. einen Aktor ein, um seine Sicherheitsfunktion auszuführen (energize to trip).

Bei der Konzeption des Automatisierungssystems sind die Anforderungen aus den Anwendungsnormen zu beachten, z. B. kann eine Leitungsüberwachung (LS/LB) der Eingänge und Ausgänge oder eine Rückmeldung der ausgelösten Sicherheitsfunktion erforderlich sein.

2.1.3 Einsatz in Brandmelderzentralen

HIMax Systeme mit analogen Eingängen sind für Brandmelderzentralen nach DIN EN 54-2 und NFPA 72 geprüft und zertifiziert.

Die in diesem Handbuch aufgeführten Verwendungsbedingungen sind zu beachten, siehe Kapitel 13.

2.1.4 Explosionsschutz

Das Automatisierungssystem HIMax ist geeignet zum Einbau in die Zone 2.



Die in Kapitel 15 aufgeführten besonderen Bedingungen sind zu beachten!

2.2 Aufgaben der Maschinen- und Anlagenhersteller sowie des Betreibers

Die Maschinen- und Anlagenhersteller sowie der Betreiber sind dafür verantwortlich, dass die sichere Anwendung der HIMax Systeme in Automatisierungsanlagen und in Gesamtanlagen gewährleistet ist.

Die korrekte Programmierung der HIMax Systeme muss durch die Maschinen- und Anlagenhersteller ausreichend validiert werden.

2.2.1 Anschluss von Kommunikationspartnern

An die Kommunikationsschnittstellen dürfen nur Geräte angeschlossen werden, die eine sichere elektrische Trennung gewährleisten.

2.2.2 Verwendung der sicherheitsbezogenen Kommunikation

Bei der Verwendung der sicherheitsbezogenen Kommunikation zwischen verschiedenen Geräten muss beachtet werden, dass die Gesamtreaktionszeit des Systems nicht die Prozess-Sicherheitszeit überschreitet.

Die in Kapitel 11.2 und im Kommunikationshandbuch HI 801 100 D aufgeführten Berechnungsgrundlagen sind anzuwenden.

2.3 ESD-Schutzmaßnahmen

Arbeiten am HIMax System muss von Personal durchgeführt werden, das Kenntnisse von ESD-Schutzmaßnahmen besitzt.

HINWEIS



Schäden am HIMax System durch elektrostatische Entladung!

- Für die Arbeiten einen antistatisch gesicherten Arbeitsplatz benutzen und ein Erdungsband tragen.
- Module bei Nichtbenutzung elektrostatisch geschützt aufbewahren, z. B. in der Verpackung.

2.4 Weitere Systemdokumentationen

Für die Projektierung der HIMax Systeme stehen außerdem noch folgende Dokumentationen zur Verfügung:

Name	Inhalt	Dokument-Nr.
HIMax Systemhandbuch	Hardwarebeschreibung des modularen Systems	HI 801 000 D
Zertifikate	Prüfergebnisse	---
Versionsliste	TÜV-zertifizierte Versionen des Betriebssystems	---
Handbücher der Komponenten	Beschreibung der einzelnen Komponenten	---
Wartungshandbuch	Beschreibung wichtiger Tätigkeiten zum Betrieb und Wartung	HI 801 170 D
Kommunikationshandbuch	Beschreibung der safe ethernet Kommunikation und der verfügbaren Protokolle	HI 801 100 D
Automation Security Handbuch	Beschreibung von Automation Security Aspekten bei HIMA Systemen	HI 801 372 D
SILworX Erste Schritte Handbuch	Einführung in die Bedienung von SILworX bei Planung, Inbetriebnahme, Test und Betrieb	HI 801 102 D
SILworX Online-Hilfe (OLH)	SILworX Bedienung	---

Tabelle 1: Übersicht Systemdokumentation

Alle aktuellen Handbücher können über die E-Mail-Adresse documentation@hima.com angefragt werden. Für registrierte Kunden stehen die Produktdokumentationen im HIMA Extranet als Download zur Verfügung.

3 Sicherheitskonzept

Dieses Kapitel behandelt wichtige allgemeine Fragen der funktionalen Sicherheit des Systems HIMax:

- Sicherheit und Verfügbarkeit.
- Sicherheitsrelevante Zeiten.
- Wiederholungsprüfung.
- Sicherheitsauflagen.
- Automation-Security.
- Zertifizierung.
 - CE-Konformitätserklärung
 - EG-Baumusterprüfbescheinigung

3.1 Sicherheit und Verfügbarkeit

Das System HIMax ist auf Grund der 1oo2-Mikroprozessorstruktur der Prozessormodule bereits als Mono-Systeme für den Einsatz als sicherheitsbezogenes Automatisierungssystem bis zu einem Safety Integrity Level 3 (SIL 3) gemäß IEC 61508 zugelassen.

Vom sicherheitsbezogenen Automatisierungssystem HIMax selbst geht kein unmittelbares Risiko aus.

WARNUNG



Personenschaden durch falsch angeschlossene oder falsch programmierte sicherheitsbezogene Automatisierungssysteme!

Anschlüsse vor Inbetriebnahme prüfen und Gesamtanlage auf Einhaltung der spezifizierten Sicherheitsanforderungen testen!

Je nach geforderter Verfügbarkeit lässt sich das System HIMax mit redundanten Prozessormodulen (X-CPU 01, X-CPU 31), redundanten Systembusmodulen (X-SB 01), redundanten Kommunikationsmodulen (X-COM 01) und redundanten E/A-Modulen bestücken.

Redundante Module erhöhen die Verfügbarkeit. Bei einem Modulfehler geht das defekte Modul automatisch in den sicheren Zustand über und das redundante Modul erhält den Betrieb ohne Unterbrechung aufrecht.

HIMA empfiehlt dringend, ausgefallene Module nach möglichst kurzer Zeit zu ersetzen, um die Redundanz wieder herzustellen.

Der Austausch eines ausgefallenen Moduls ist im laufenden Betrieb möglich. Das neue Modul übernimmt automatisch die Funktion des ausgefallenen Moduls. Voraussetzung dafür ist, dass das Austauschmodul vom gleichen Typ oder ein zugelassener Ersatztyp ist.

Bei bestimmten anstehenden Fehlern länger 24 h werden weitere Systemkomponenten aus Sicherheitsgründen abgeschaltet.

3.1.1 PFD- und PFH-Berechnungen

Für das System HIMax wurden gemäß IEC 61508 die PFD- (Probability of Failure on Demand) und PFH- (Probability of Failure per Hour) Berechnungen durchgeführt.

Die IEC 61508-1 legt für SIL 3 folgende Werte fest:

$PFD = 10^{-4} \dots 10^{-3}$.

$PFH = 10^{-8} \dots 10^{-7}$ pro Stunde.

Die Werte für PFD, PFH und SFF können über die E-Mail-Adresse documentation@hima.com angefragt werden.

3.1.2 Selbst-Test und Fehlerdiagnose

Das Betriebssystem der Module führt beim Start und im laufenden Betrieb umfangreiche Selbst-Tests durch.

Getestet werden hauptsächlich:

- Die Prozessoren.
- Die Speicherbereiche (RAM, nichtflüchtiger Speicher).
- Der Watchdog.
- Die Verbindungen zwischen den Modulen.
- Die einzelnen Kanäle der E/A-Module.

Wenn die Selbst-Tests Fehler feststellen, dann schaltet das Betriebssystem das defekte Modul oder bei E/A-Modulen den defekte Kanal ab. Wenn beim Starten ein Modulfehler erkannt wird, gehen die Module erst gar nicht in Betrieb.

Bei einem System ohne Redundanz bedeutet dies, dass Teilfunktionen oder das gesamte PES abgeschaltet werden können. Bei einem redundanten System übernimmt im erkannten Fehlerfall das redundante Modul oder der redundante Kanal die auszuführende Funktion.

Alle HIMax Module verfügen jeweils über eigene LEDs zur Anzeige der entdeckten Fehler. Damit ist im Störfall eine schnelle Fehlerdiagnose über ein fehlerhaft gemeldetes Modul oder der externen Beschaltung möglich.

Zusätzlich kann das Anwenderprogramm verschiedene Systemvariable auswerten, die den Zustand der Module anzeigen.

Eine umfangreiche diagnostische Aufzeichnung des Systemverhaltens und erkannter Fehler werden im Diagnosespeicher des Prozessormoduls und der anderen Module abgelegt. Die Aufzeichnung kann auch nach einer Systemstörung über das PADT ausgelesen werden.

Weitere Informationen über die Auswertung der Diagnosemeldungen finden Sie im Systemhandbuch HI 801 000 D.

Bei einem sehr kleinen Teil der Bauelement-Ausfälle, welche die Sicherheit nicht beeinflussen, erzeugt das HIMax System keine Diagnoseinformation.

3.1.3 PADT

Mit dem PADT konfiguriert der Anwender die Steuerung und erstellt das Anwenderprogramm. Das Sicherheitskonzept des PADT unterstützt den Anwender bei der korrekten Umsetzung der Steuerungsaufgabe. Das PADT führt zahlreiche Maßnahmen zur Prüfung der eingegebenen Informationen durch.

Das PADT ist ein Personalcomputer, auf dem das Programmierwerkzeug SILworX installiert ist.

3.1.4 Redundanz

Zur Erhöhung der Verfügbarkeit ist es möglich, alle Komponenten, die aktive Bauelemente enthalten, redundant einzusetzen und im laufenden Betrieb auszutauschen.

Die Redundanz von Komponenten beeinträchtigt nicht die Sicherheit des Systems. Der Safety Integrity Level 3 (SIL 3) ist gewährleistet.

Durch die Redundanz ändern sich die PFD- und PFH-Werte des HIMax Systems, siehe Kapitel 3.1.1.

3.1.5 Aufbau von Sicherheitssystemen nach dem Arbeitsstromprinzip

Sicherheitssysteme, die nach dem Arbeitsstromprinzip (energize to trip) wirken, haben folgende Funktion:

1. Der sicherere Zustand eines Moduls ist der energielose Zustand. Dieser Zustand wird z. B. bei einem Fehler innerhalb des Moduls eingenommen.
2. Auf Anforderung kann die Steuerung die Sicherheitsfunktion durch Einschalten eines Aktors auslösen.

3.1.5.1 Erkennen ausgefallener Komponenten

Das Sicherheitssystem erkennt durch die automatisch ablaufende Diagnose, dass Module defekt sind.

3.1.5.2 Sicherheitsfunktion im Arbeitsstromprinzip

Die Ausführung der Sicherheitsfunktion besteht darin, dass das Sicherheitssystem einen oder mehrere Aktoren einschaltet (energize).

Anwenderseitig ist folgendes zu planen:

- Für jedes E/A-Modul muss ein redundantes Modul vorgesehen und parametrierung werden.
- Jedes Modul muss mit einer Leitungsschluss- und Leitungsbruch-Überwachung ausgestattet sein. Die Leitungsschluss- und Leitungsbruch-Überwachung muss parametrierung werden.
- Die Funktion von Aktoren kann über eine Stellungsrückmeldung überwacht werden.

3.1.5.3 Redundanz von Komponenten

Es kann erforderlich sein, folgende Komponenten redundant auszulegen:

- Stromversorgung der Steuerung.
- HlMax Module.
- Sensoren und Aktoren.

Bei Redundanzverlust muss die Steuerung in möglichst kurzer Zeit repariert werden.

Nähere Informationen zu Redundanz von Komponenten ist dem Systemhandbuch HI 801 000 D zu entnehmen.

Eine redundante Auslegung der Module des Sicherheitssystems ist nicht erforderlich, wenn die geforderte Sicherheit bei Ausfall des Sicherheitssystems durch andere, z. B. organisatorische, Maßnahmen erreicht werden kann.

3.2 Sicherheitsrelevante Zeiten

Folgende Zeiten sind für die Sicherheitsbetrachtung der Steuerung zu beachten:

- Prozess-Sicherheitszeit.
- Sicherheitszeit (Ressource).
- Watchdog-Zeit (Ressource).
- Reaktionszeit.

i

Mit Ressource wird die Abbildung der Steuerung (PES) im Programmierwerkzeug SILworX bezeichnet.

3.2.1 Prozess-Sicherheitszeit

Die Prozess-Sicherheitszeit ist gemäß IEC 61508-4 eine Zeitspanne zwischen dem Auftreten eines Ausfalls der EUC oder des EUC-Leit- oder Steuerungssystems mit dem Potenzial, einen gefährlichen Vorfall zu verursachen, und dem Zeitpunkt, bei dem die Reaktion in der EUC abgeschlossen sein muss, um das Auftreten des gefährlichen Vorfalls zu verhindern.

Innerhalb der Prozess-Sicherheitszeit kann der Prozess mit fehlerhaften Signalen beaufschlagt werden, ohne dass ein riskanter Zustand entsteht.

Eine sicherheitsbezogene Reaktion der Steuerung einschließlich aller Verzögerungen durch Sensoren, Aktoren, E/A-Module und der Prozessverzögerung (Reaktion der Anlage auf die Auslösung) muss innerhalb der Prozess-Sicherheitszeit erfolgen.

3.2.2 Parameter «Sicherheitszeit [ms]» Ressource

Die Reaktionszeit der Ressource t_{RR} wird durch den Parameter *Sicherheitszeit [ms]* in den Eigenschaften der Ressource t_{SR} wie folgt beeinflusst:

$$t_{RR} \leq t_{SR}$$

t_{SR} Parameter *Sicherheitszeit [ms]*

Folgende Faktoren verlängern die Reaktionszeit der Ressource und sind bei der Parametrierung zu beachten:

- Physikalische bedingte Verzögerungen, z. B. Schaltzeiten von externen Relais.
- Parametrierte Verzögerungen im Anwenderprogramm, z. B. durch Timer-Bausteine (TON, TOF).
- Verzögerung von Ausgangssignalen durch die Ausgangs-Störaustastung und LB-Austastung.

Der Parameter *Sicherheitszeit [ms]* t_{SR} in den Eigenschaften der Ressource ist im Bereich von 20 ... 22 500 ms in SILworX einstellbar.

Damit eine Fehlerreaktion innerhalb der parametrierten Sicherheitszeit gewährleistet ist, müssen folgende Voraussetzungen erfüllt sein:

- Die Reaktion des Anwenderprogramms muss innerhalb eines RUN-Zyklus erfolgen.
- Keine Verzögerung von Eingangssignalen durch in den Eingangsmodulen konfigurierte Verzögerungsglieder (EV, AV).
- Keine programmierten Verzögerungen durch das Anwenderprogramm.

3.2.3 Watchdog-Zeit (Ressource)

Die Watchdog-Zeit t_{WD} ist die maximal zulässige Dauer eines RUN-Zyklus (Zykluszeit). Die Steuerung schaltet ab, wenn die Zykluszeit die Watchdog-Zeit überschreitet.

Die Watchdog-Zeit kann vom Anwender gemäß der sicherheitstechnischen Erfordernisse der Anwendung eingestellt werden.

Bedingung für die Sicherheit:

$$t_{WD} \leq \frac{1}{2} \times t_{SR}$$

t_{WD} Watchdog-Zeit (Ressource)

t_{SR} Parameter *Sicherheitszeit [ms]* (Ressource)

Bedingung für die Sicherheit plus Verfügbarkeit:

$$t_{WD} \leq \frac{1}{3} \times t_{SR}$$

Die Watchdog-Zeit (Ressource) muss parametrierbar werden. Der Parameter *Watchdog-Zeit [ms]* ist im Bereich von 6 ... 7500 ms einstellbar und wird in den Eigenschaften der Ressource eingegeben. Die Standardeinstellung ist 200 ms.

Das PADT überprüft die Parameter *Sicherheitszeit [ms]* und *Watchdog-Zeit [ms]* und lehnt beim Generieren die Konfiguration ab, wenn die Watchdog-Zeit größer als $\frac{1}{2}$ mal die Sicherheitszeit der Ressource eingestellt wurde.

Die Watchdog-Zeit kann durch Abschätzung bestimmt werden. Dabei ist der folgende Zeitbedarf zu berücksichtigen:

- Zyklusdauer der Anwenderprogramme (RUN-Zyklus der Ressource).
 - Einlesen der Daten.
 - Datenverarbeitung.
 - Prozessdaten-Kommunikation.
 - Ausgeben der Daten.
- Synchronisierung der Prozessormodule.
- Besonderer Zeitbedarf für Reloads.

HINWEIS



Der Anwender muss die genannten Restriktionen bei Online-Änderungen an der Steuerung berücksichtigen und einhalten!

Einstellungen vor jeder Online-Änderung genau prüfen!

3.2.4 Abschätzung der Watchdog-Zeit

HIMA empfiehlt für eine ausreichende Verfügbarkeit dringend folgende Einstellung:

$$2 \times t_{WD} + t_{Sync} + 2 \times t_{E/A-Zyklus} \leq t_{SR} \text{ (Parameter } \textit{Sicherheitszeit [ms]})$$

t_{Sync} Maximale Synchronisationszeit der Prozessormodule, siehe Kapitel 3.2.4.

$t_{E/A-Zyklus}$ E/A-Zykluszeit = 2 ms

Wenn eine sichere Abschätzung der max. CPU-Zykluszeit nicht möglich ist, so ist die Watchdog-Zeit wie folgt einzustellen:

$$3 \times t_{WD} + 2 \times t_{E/A-Zyklus} \leq t_{SR}$$

3.2.5 Watchdog-Zeit durch Test ermitteln

Die Watchdog-Zeit t_{WD} kann während der Inbetriebnahme durch Test ermittelt werden. Dazu muss das System im RUN-Betrieb unter Volllast betrieben werden. Alle projektierten Module müssen gesteckt und alle konfigurierten Kommunikationsverbindungen (z. B. safeethernet und weitere Protokolle) müssen in Betrieb sein.

Die maximale Systemlast entsteht durch das Aufsynchronisieren, wenn Prozessormodule entfernt und gesteckt werden. Die Watchdog-Zeit muss so eingestellt werden, dass das Aufsynchronisieren unter Volllast immer möglich ist.

Test durchführen

1. In den Ressource-Eigenschaften die *Sicherheitszeit [ms]* auf den Maximalwert (22 500 ms) einstellen.
2. In den Ressource-Eigenschaften die *Watchdog-Zeit [ms]* auf den Maximalwert (7 500 ms) einstellen.
3. Die Werte t_{Komm} , t_{Konfig} , t_{Latenz} müssen, wie im Systemhandbuch beschrieben, berechnet und eingestellt sein.
4. Die Konfiguration kompilieren und per Download in die Steuerung laden.
5. Die Ressource starten (Kaltstart).
6. Das Control Panel der Ressource öffnen und die Zykluszeitstatistik zurücksetzen.

Für die folgenden Schritte muss das System unter Volllast betrieben werden.

7. Die maximale Ausführungsdauer der Anwenderprogramme (AP) im Control Panel ablesen und die Schwankungen und Lastspitzen nach Ablauf mehrere Minuten notieren.
Danach t_{Spitze} berechnen:

$$t_{Spitze} = \text{Ausführungsdauer (max.)} - \text{Ausführungsdauer (min.)}, \text{ für jedes AP}$$
 ausrechnen und diese Werte für alle AP addieren.
8. Nacheinander jedes Prozessormodul entfernen und wieder in den Basisträger einfügen. Jeweils vor dem Entfernen eines Prozessormoduls warten, bis sich das gerade eingefügte Prozessormodul synchronisiert hat.

i

Die redundanten Prozessormodule synchronisieren sich beim Hinzufügen automatisch mit der Konfiguration der vorhandenen Prozessormodule. Die für die Synchronisation benötigte Zeit verlängert den Zyklus der Steuerung auf die maximale Zykluszeit.

Die für die Synchronisation benötigte Zeit wächst mit der Anzahl der bereits synchronisierten Prozessormodule.

Beschreibung zum Einbau und Ausbau eines Prozessormoduls siehe Handbuch X-CPU 01, HI 801 008 D, oder X-CPU 31, HI 801 354 D.

9. In der Diagnosehistorie des nicht synchronisierten Moduls die Synchronisationszeit von n auf n+1 Prozessormodule bei jedem Synchronisationsvorgang ablesen. Die größte dieser Synchronisationszeiten wird zur Bestimmung der Watchdog-Zeit benutzt.

10. Die notierten Zeiten in die folgende Formel einsetzen:

$$t_{WD} = t_{Sync} + t_{Reserve} + t_{Komm} + t_{Konfig} + t_{Latenz} + t_{Spitze}$$

t_{Sync}	Ermittelte Zeit für die Synchronisation eines Prozessormoduls.
$t_{Reserve}$	Sicherheitsreserve 12 ms.
t_{Komm}	In den Ressource-Eigenschaften eingestellter Systemparameter <i>Max. Kom.Zeitscheibe [ms]</i> .
t_{Konfig}	In den Ressource-Eigenschaften eingestellter Systemparameter <i>Maximale Dauer der Konfigurationsverbindung [ms]</i> .
t_{Latenz}	Eingestellter Systemparameter <i>Maximale Systembus-Latenzzeit [μs] x 4</i> .
t_{Spitze}	Summe aller in Schritt 7 errechneten AP-Lastspitzen.

3.2.6 Reaktionszeit

Die Reaktionszeit von zyklisch arbeitenden HIMax Steuerungen ist die doppelte Zykluszeit dieser Systeme im fehlerfreien Betrieb, wenn nicht durch Parametrierung oder durch die Logik des Anwenderprogramms eine Verzögerung erfolgt.

TIPP	HIMA empfiehlt für eine konservative Berechnung der Reaktionszeit im fehlerfreien Betrieb, anstatt der Zykluszeit die parametrierte Watchdog-Zeit zu verwenden.
-------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

3.3 Wiederholungsprüfung (Proof-Test nach IEC 61508)

Ziel der Wiederholungsprüfung ist die Aufdeckung versteckter gefahrbringender Ausfälle in einem sicherheitsbezogenen System, so dass das System, wenn nötig, wieder in den Zustand gebracht werden kann, indem es seine geplante Funktion erfüllt. Danach ist der sichere Betrieb einschließlich der Sicherheitsfunktionen wieder gewährleistet.

Die Durchführung der Wiederholungsprüfung ist abhängig von:

- Der Beschaffenheit der Anlage (EUC = equipment under control).
- Dem Risikopotenzial der Anlage.
- Den Normen, die für den Betrieb der Anlage zur Anwendung kommen.
- Den Normen, die von der Prüfstelle als Grundlage für die Genehmigung der Anlage benutzt wurden.

Nach den Normen IEC 61508 1-7, IEC 61511 1-3, IEC 62061 und VDI/VDE 2180 Blatt 1 bis 4 hat bei sicherheitsbezogenen Systemen der Betreiber für eine Wiederholungsprüfung zu sorgen. Bei einer Wiederholungsprüfung müssen die kompletten Sicherheitsfunktionen des sicherheitsbezogenen HIMA Systems überprüft werden.

HIMA Sicherheitssysteme sind in regelmäßigen Abständen einer Wiederholungsprüfung zu unterziehen. Für HIMA Steuerungen muss die Wiederholungsprüfung in einem Intervall erfolgen, welches dem applikationsspezifisch notwendigen Safety Integrity Level (SIL) entspricht.

Die Durchführung der Wiederholungsprüfung ist im Wartungshandbuch HI 801 170 D beschrieben.

3.4 Sicherheitsauflagen

Für den Einsatz des sicherheitsbezogenen Automatisierungssystems HIMax gelten die folgenden Sicherheitsauflagen.

3.4.1 Produktunabhängige Auflagen der Hardware

Personen, welche HIMax Hardware projektieren, müssen die folgenden produktunabhängigen Sicherheitsauflagen beachten:

- Für den sicherheitsbezogenen Betrieb müssen dafür zugelassene fehlersichere Hardware-Komponenten und Software-Komponenten verwendet werden. Die zugelassenen Komponenten sind in der HIMax Versionsliste aufgeführt. Die jeweils aktuellen Versionsstände sind der Versionsliste zu entnehmen, die gemeinsam mit der Prüfstelle geführt wird.
- Die spezifizierten Verwendungsbedingungen bezüglich EMV, mechanischen, chemischen und klimatischen Einflüssen müssen eingehalten werden.
- Nicht fehlersichere, jedoch rückwirkungsfreie Hardware-Komponenten und Software-Komponenten können für die Verarbeitung nicht sicherheitsrelevanter Signale eingesetzt werden. Ein Einsatz von nicht fehlersicheren Komponenten für die Bearbeitung sicherheitsbezogener Aufgaben ist verboten.
- Bei allen extern an das System angeschlossenen Sicherheitsstromkreisen ist das Ruhestromprinzip einzuhalten.

3.4.2 Produktabhängige Auflagen der Hardware

Personen, welche HIMax Hardware projektieren, müssen die folgenden produktabhängigen Sicherheitsauflagen beachten:

- An ein System müssen Geräte angeschlossen werden, die eine sichere elektrische Trennung zum Netz aufweisen.
- Für die Bearbeitung sicherheitsbezogener Aufgaben sind nur sicherheitsbezogene Module einzusetzen.
- Die im Systemhandbuch genannten Verwendungsbedingungen sind einzuhalten, insbesondere hinsichtlich Versorgungsspannung und Klima.
- Die Spannungsversorgung muss durch Netzgeräte in den Ausführung SELV und PELV erfolgen. Für die Netzgeräte gilt:
 - **24 VDC** Spannungsversorgung: Die Netzgeräte dürfen keine Versorgungsspannung größer als 31 V abgeben.
 - **48 VDC** Spannungsversorgung: Die Netzgeräte dürfen keine Versorgungsspannung größer als 62 V abgeben.
- Für die Spannungsversorgung über ein Stromnetz gelten die gleichen Auflagen wie für die Netzgeräte.

3.4.3 Produktunabhängige Auflagen der Programmierung

Personen, welche Anwenderprogramme erstellen, müssen die folgenden produktunabhängigen Sicherheitsauflagen beachten:

- In sicherheitsrelevanten Anwendungen ist auf eine zur Anwendung passenden Parametrierung der sicherheitsrelevanten Systemgrößen zu achten.
- Insbesondere ist die Festlegung von Systemkonfiguration, maximaler Zykluszeit und Sicherheitszeit zu beachten.

3.4.4 Produktabhängige Auflagen der Programmierung

Für die Programmierung von HIMax ist das Programmierwerkzeug SILworX zu verwenden. Folgende Auflagen für die Verwendung von SILworX sind zu beachten:

- Die in der Spezifikation beschriebene Applikation ist zu validieren, zu verifizieren und die korrekte Umsetzung ist zu dokumentieren. Es muss eine vollständige Prüfung der Logik durch Funktionstests erfolgen.
- Nach einer Änderung der Applikation müssen alle Teile der Logik geprüft werden, die von dieser Änderung betroffen sind.
- Für Fehler in den sicherheitsbezogenen Eingangs- und Ausgangsmodulen muss gemäß den anlagenspezifischen, sicherheitsbezogenen Bedingungen eine Fehlerreaktion des Systems festgelegt werden. Diese sind zum Beispiel Fehlerreaktionen im Anwenderprogramm und die Parametrierung von sicheren Initialwerten für Variablen.

3.4.5 Kommunikation

Folgende Auflagen für die Kommunikation von Daten und zu Systemen sind zu beachten:

- Bei Verwendung der sicherheitsbezogenen Kommunikation zwischen verschiedenen HIMA Systemen ist zu beachten, dass die Gesamtreaktionszeit eines Systems die zulässige maximale Reaktionszeit für safe**ethernet** oder HIPRO-S V2 nicht überschreitet. Die im Kapitel *Maximale Reaktionszeit für safeethernet* aufgeführten Berechnungsgrundlagen sind anzuwenden.
- Bei der Übertragung von (sicherheitsrelevanten) Daten sind IT-Sicherheitsregeln zu beachten.
- Eine Übertragung von sicherheitsrelevanten Daten über öffentliche oder öffentlich zugängliche Netze (z. B. Internet, WLAN) ist nur mit zusätzlichen Sicherheitsmaßnahmen, z. B. VPN-Tunnel und Firewall zulässig.
- Falls die Datenübertragung über firmen-/fabrikinterne Netze erfolgt, muss durch administrative und technische Maßnahmen dafür Sorge getragen werden, dass ausreichender Schutz vor Manipulation gegeben ist (z. B. Abschottung des sicherheitsrelevanten Teiles des Netzes von anderen Netzen mit einer Firewall).
- Standardprotokolle dürfen nicht für die Übertragung sicherheitsbezogener Daten eingesetzt werden.
- An Kommunikationsschnittstellen müssen Geräte angeschlossen werden, die eine sichere elektrische Trennung aufweisen.

3.4.6 Wartung

Die Wartung liegt in der Verantwortung des Betreibers. Der Betreiber muss geeignete Maßnahmen treffen, um den sicheren Betrieb während der Wartung zu gewährleisten.

Erforderlichenfalls muss der Betreiber in Absprache mit der für die Applikation zuständigen Prüfstelle durch administrative und technische Maßnahmen den Zugangsschutz zum System festlegen.

3.4.7 Umgebungsbedingungen

Für den Einsatz des sicherheitsbezogenen Automatisierungssystems HIMax sind die folgenden allgemeinen Umgebungsbedingungen einzuhalten:

Allgemein	
Schutzklasse	Schutzklasse II nach IEC/EN 61131-2
Umgebungstemperatur	0 ... +60 °C
Transport- und Lagertemperatur	-40 ... +70 °C
Verschmutzung	Verschmutzungsgrad II nach IEC/EN 60664-1
Aufstellhöhe	< 2000 m
Gehäuse	Standard: IP20 Falls es die zutreffenden Applikationsnormen (z. B. EN 60204) fordern, muss das System in ein Gehäuse der geforderten Schutzart (z. B. IP54) eingebaut werden.
Eingangsspannung Netzteil	24 VDC

Tabelle 2: Umgebungsbedingungen

Mögliche Abweichungen sind dem entsprechenden Datenblatt zu entnehmen.

3.5 Automation Security

HIMA unterscheidet zwischen den Begriffen *Safety* im Sinne der funktionalen Sicherheit und *Security* im Sinne von Schutz eines Systems vor Manipulationen.

Industrielle Steuerungen (PES) müssen gegen IT-typische Problemquellen geschützt werden, z. B.:

- Unzureichender Schutz von IT-Einrichtungen (z. B. offenes WLAN, veraltete Betriebssysteme).
- Fehlendes Bewusstsein für den richtigen Umgang mit Betriebsmitteln (z. B. USB-Stick).
- Direkte Zugänge zu schützenswerten Bereichen.
- Angreifer innerhalb von Betriebsgeländen.
- Angreifer über Kommunikations-Netzwerke innerhalb und außerhalb von Betriebsgeländen.

HIMA Safety-Systeme bestehen aus folgenden zu schützenden Teilen:

- Sicherheitsbezogenes Automatisierungssystem.
- PADT.
- Optionale X-OPC Server (auf einem Host-PC).
- Optionale Kommunikationsverbindungen zu externen Systemen.

3.5.1 Produkteigenschaften

HIMax Steuerungen erfüllen bereits in den Grundeinstellungen Anforderungen an Automation Security.

In Steuerungen und im Programmierwerkzeug sind Schutzmechanismen integriert, die versehentliche oder nicht genehmigte Veränderungen verhindern:

- Jede Änderung am Anwenderprogramm oder an der Konfiguration einer Steuerung führt zu einem neuen Konfigurations-CRC.
- In der Steuerung können Online-Änderungen der Sicherheitsparameter deaktiviert werden. Dadurch sind Änderungen der Sicherheitsparameter nur durch Download oder Reload möglich.
- Der Anwender kann eine Benutzerverwaltung einrichten, um die Security zu erhöhen. Hier werden Benutzergruppen, Benutzerkonten, Zugriffsrechte für das PADT und für die Steuerungen (PES) projektbezogen festgelegt. In einer Benutzerverwaltung kann der Anwender definieren, ob für das Öffnen des Projekts und für den Login in eine Steuerung eine Autorisierung erforderlich ist.
- Der Zugang zu Daten einer Steuerung ist nur dann möglich, wenn im PADT das gleiche Anwenderprojekt geladen wurde wie in der Steuerung. Die CRCs müssen identisch sein (Archiv-Pflege!).
- Eine physikalische Verbindung zwischen einem PADT und einer Steuerung (PES) ist im Betrieb nicht notwendig und muss aus Gründen der Security getrennt werden. Das PADT kann für Diagnose- und Wartungszwecke erneut mit der Steuerung verbunden werden.

Die Anforderungen der Normen für Safety und Security sind zu beachten. Die Autorisierung von Personal und die notwendigen Schutzmaßnahmen unterliegen der Verantwortung des Betreibers.

⚠️ WARNUNG

Personenschaden durch unbefugte Manipulationen an Steuerungen möglich!

Steuerungen sind gegen unbefugte Zugriffe zu schützen:

- **Standardeinstellungen für Logins und Passworte sind zu ändern.**
- **Zugänge zu Steuerungen und PADTs sind zu kontrollieren!**
- **Weitere Schutzmaßnahmen entnehmen Sie dem Automation Security Handbuch (HI 801 372 D).**

3.5.2 Risikoanalyse und Planung

Security ist kein Produkt, sondern ein Prozess. So helfen z. B. gepflegte Netzwerkpläne sicherzustellen, dass sichere Netzwerke dauerhaft von öffentlichen Netzwerken getrennt sind. Sinnvollerweise sollte nur ein definierter Übergang über eine Firewall oder ein eigenständiges Subnetz bestehen.

Eine sorgfältige Planung nennt die erforderlichen Maßnahmen. Nach erfolgter Risikoanalyse sind die benötigten Maßnahmen zu ergreifen, wie z. B.:

- Zugriffsrechte für Benutzergruppen und Benutzerkonten gemäß den vorgesehenen Aufgaben zuweisen.
- Passwörter verwenden, die den Anforderungen an die Security entsprechen.

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

i

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

Weitere Informationen finden Sie im HIMA Automation Security Handbuch HI 801 372 D.

3.6 Zertifizierung

Das programmierbare elektronische System HIMax erfüllt die in diesem Kapitel aufgelisteten Normen.

3.6.1 CE-Konformitätserklärung

Das Automatisierungssystem HIMax entspricht in Betriebsverhalten und Konstruktion den internationalen und europäischen Richtlinien sowie den ergänzenden nationalen Anforderungen. Die Konformität wurde mit der CE-Kennzeichnung nachgewiesen.

Die Konformitätserklärung des Automatisierungssystems kann auf der Webseite unter www.hima.com/de abgerufen oder über die E-Mail-Adresse documentation@hima.com angefordert werden.

3.6.2 EG-Baumusterprüfbescheinigung

Das Prüfinstitut TÜV Rheinland hat das sicherheitsbezogene Automatisierungssystem HIMax für Anwendungen gemäß den Normen zur Funktionalen Sicherheit geprüft und zertifiziert. Das sicherheitsbezogene Automatisierungssystem HIMax trägt das folgende Prüfzeichen:



TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie
Am Grauen Stein
51105 Köln

EG-Baumusterprüfbescheinigung
Sicherheitsbezogenes programmierbares System
HIMax

3.6.3 Normenspiegel

Das sicherheitsbezogene Automatisierungssystem HIMax ist gemäß den folgenden Normen für die funktionale Sicherheit geprüft und vom TÜV zertifiziert:

Internationale Normen	Sicherheitsstufe
IEC 61508, Teile 1-7:2010	SIL 3
IEC 61511-1:2016 + Corr.1:2016 + AMD1:2017	SIL 3
EN ISO 13849-1:2015	PL e
EN 62061:2005 + AC:2010 + A1:2013 + A2:2015	SIL CL 3
EN 50156:2015	SIL 3
EN 12067-2:2004	---
EN 298:2012	---
EN 60079-0:2012 + A11:2013	---
EN 60079-11:2012	---
EN 60079-15:2010	---
EN 60079-29-1: 2007	---
NFPA 72:2019	---
NFPA 85:2019	---
NFPA 86:2019	---
EN 61131-2:2007	Zone C
EN 61326-1:2013	---
EN 61326-3-1:2017	---
EN 54-2:1997 + AC:1999 + A1:2006	---
EN 50130-4:2011 + A1:2014	---
EN 61000-6-7:2015	---
DIN IEC 60533:2010-11	---

Tabelle 3: Internationale Normen und Sicherheitsstufen

Das folgende Kapitel enthält eine detaillierte Aufstellung aller durchgeführten Umwelt- und EMV-Prüfungen.

3.6.4 Prüfbedingungen

Das HiMax System wurde auf die Einhaltung der Anforderungen folgender Normen für EMV, klimatische-, mechanische- und Spannungsprüfungen geprüft:

Norm	Inhalt
IEC/EN 61131-2 Zone C	Speicherprogrammierbare Steuerungen Teil 2: Betriebsmittelanforderungen und Prüfungen
IEC/EN 61000-6-2	Elektromagnetische Verträglichkeit (EMV), Teil 6-2: Fachgrundnormen – Störfestigkeit für Industriebereiche.
IEC/EN 61000-6-4	Elektromagnetische Verträglichkeit (EMV), Teil 6-4: Fachgrundnorm – Störaussendung für Industriebereiche
EN 298	Feuerungsautomaten für Brenner und Brennstoffgeräte für gasförmige oder flüssige Brennstoffe.
EN 61326-1	Elektrische Mess-, Steuer-, Regel- und Laborgeräte - EMV-Anforderungen Teil 1: Allgemeine Anforderungen.
EN 61326-3-1	Elektrische Mess-, Steuer-, Regel- und Laborgeräte - EMV-Anforderungen Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) - Allgemeine industrielle Anwendungen.
EN 50130-4	Alarmanlagen, Teil 4: Elektromagnetische Verträglichkeit- Produktfamilienorm: Anforderungen an die Störfestigkeit von Anlageteilen für Brandmeldeanlagen, Einbruch- und Überfallmeldeanlagen, Video-Überwachungsanlagen, Zutrittskontrollanlagen sowie Personen- und Hilferufanlagen.
EN 54-2	Brandmelderzentralen

Tabelle 4: Normen für EMV-, Klima- und Umweltsanforderungen

Für sicherheitsbezogene Systeme werden erhöhte Pegel bei der Störbeeinflussung gefordert. HiMax Systeme erfüllen diese Anforderungen nach IEC 62061 und IEC 61326-3-1.

IEC/EN 61000-6-4	Prüfungen der Störaussendung
EN 55011 Klasse A	Störaussendung: gestrahlt, leitungsgebunden

Tabelle 5: Prüfungen der Störaussendung

3.6.4.1 Klimatische Prüfungen

Die wichtigsten Prüfungen und Grenzwerte für die klimatischen Bedingungen sind in der folgenden Tabelle aufgelistet:

Norm	Klimaprüfungen
IEC/EN 61131-2	Trockene Wärme und Kälte; Beständigkeitsprüfungen: +70 °C / -40 °C, 16 h, +85 °C, 1 h Stromversorgung nicht angeschlossen.
	Temperaturwechsel; Beständigkeitsprüfung: Schneller Temperaturwechsel: -40 °C / +70 °C, Stromversorgung nicht angeschlossen.
	Unempfindlichkeitsprüfung: Langsamer Temperaturwechsel: -10 °C / +70 °C, Stromversorgung angeschlossen.
	Zyklen mit feuchter Wärme; Beständigkeitsprüfungen: +25 °C / +55 °C, 95 % relative Feuchte, Stromversorgung nicht angeschlossen.
EN 54-2	Feuchte Wärme: 93 % relative Feuchte, 40 °C, 4 Tage Steuerung in Betrieb. 93 % relative Feuchte, 40 °C, 21 Tage, Stromversorgung nicht angeschlossen.

Tabelle 6: Klimatische Prüfungen

3.6.4.2 Mechanische Prüfungen

Die wichtigsten Prüfungen und Grenzwerte für die mechanischen Bedingungen sind in der folgenden Tabelle aufgelistet:

Norm	Mechanische Prüfungen
IEC/EN 61131-2	Unempfindlichkeitsprüfung gegen Schwingungen: 5 ... 8,4 Hz / 3,5 mm. 8,4 ... 150 Hz / 1 g, Steuerung in Betrieb, 10 Zyklen pro Achse.
	Unempfindlichkeitsprüfung gegen Schocks: 15 g, 11 ms, HlMax in Betrieb, 3 Schocks pro Achse und Richtung (18 Schocks).

Tabelle 7: Mechanische Prüfungen

3.6.4.3 EMV-Prüfungen

Die Steuerung erfüllt die Anforderungen der EMV-Richtlinie der Europäischen Union, siehe die EU-Konformitätserklärung des Systems.

Alle Module der Steuerung erfüllen die Anforderungen der EMV-Richtlinie (2014/30/EU) der Europäischen Union und haben das CE-Zeichen.

Bei Störbeeinflussung über die angegebenen Grenzen hinaus reagiert die Steuerung sicherheitsbezogen.

3.6.4.4 Versorgungsspannung

Die wichtigsten Prüfungen und Grenzwerte für die Versorgungsspannung sind in der folgenden Tabelle aufgelistet:

Norm	Nachprüfung der Gleichstromversorgungs-Eigenschaften
IEC/EN 61131-2	Die Spannungsversorgung muss mindestens eine der folgenden Normen oder Anforderungen erfüllen: <ul style="list-style-type: none"> ▪ IEC 61131-2. ▪ SELV (Safety Extra Low Voltage). ▪ PELV (Protective Extra Low Voltage).
	Die Absicherung des HIMax Systems muss gemäß den Angaben in den Handbüchern erfolgen.
	Prüfung des Spannungsbereichs: 24 VDC, -20 ... +25 % (19,2 ... 30,0 VDC).
	Prüfung auf Unempfindlichkeit gegen Kurzzeitunterbrechung der externen Stromversorgung: DC, 2 ms.
	Polaritätsumkehr der Versorgungsspannung.
	Pufferdauer, Beständigkeitsprüfung: Prüfung B, 1000 h

Tabelle 8: Nachprüfung der Gleichstromversorgungs-Eigenschaften

3.6.5 Schadgase

HIMax Komponenten können ohne Einschränkung der Funktion und der Sicherheit bei Schadgaskonzentrationen betrieben werden, die in folgenden Normen beschrieben sind:

- ANSI/ISA -S71.04:1985 Klasse G3
- DIN EN 60068-2-60:2016

Bei höheren als den genannten Konzentrationen ist mit einer Verkürzung der Lebensdauer der Komponenten zu rechnen. Der Nachweis einer ausreichenden Freiheit von Schadgasen liegt beim Anwender.

4 Prozessormodul

Das sicherheitsbezogene Prozessormodul besteht aus 2 Mikroprozessoren mit je einem RAM-Speicher, welche gleichzeitig das Betriebssystem und das Anwenderprogramm abarbeiten. Ein Hardware-Vergleicher führt ständig einen Abgleich der Daten der beiden Mikroprozessoren und der Speicher durch. Das Prozessormodul meldet auftretende Differenzen und geht automatisch in den Zustand FEHLERSTOPP.

Das Prozessormodul führt weitere Selbst-Tests, wie die Überwachung des Programmlaufs (Watchdog) durch.

4.1 Prozessormodul X-CPU 01

Das Prozessormodul X-CPU 01 ist bis zu 4-fach redundant einsetzbar. Es darf in Rack 0 oder 1 auf den Steckplätzen 3 ... 6 eingefügt sein.

4.2 Prozessormodul X-CPU 31

Das Prozessormodul X-CPU 31 vereinigt die Funktionen von Prozessormodul und Systembusmodul. Es kann daher nur in Rack 0, Steckplatz 1 oder 2 eingesetzt werden. In diesem Fall darf kein weiteres Prozessormodul in Rack 0 oder 1 auf den Steckplätzen 3 ... 6 vorhanden sein!

4.3 Selbst-Tests

Das Betriebssystem des Prozessormoduls führt beim Start und im laufenden Betrieb umfangreiche Selbst-Tests durch. Entdeckt das Betriebssystem Einzelfehler, die zu einem riskanten Betriebszustand führen können, so werden die fehlerhaften Teile abgeschaltet. Dies ist der sichere Zustand und wird innerhalb der Sicherheitszeit ausgeführt.

Getestet werden hauptsächlich:

- Die Mikroprozessoren.
- Die Speicherbereiche (RAM, nicht-flüchtigen Speicher).
- Der Watchdog.
- Der Hardware-Vergleicher.

4.4 Reaktionen auf Fehler im Prozessormodul

Detektiert das Prozessormodul einen internen Modulfehler so wird ein Eintrag in die Diagnosehistorie geschrieben. Anschließend wird automatisch ein Reboot durchgeführt.

Nach dem ersten Fehler-Reboot startet das Prozessormodul erneut und versucht, nachdem alle Selbst-Test abgeschlossen sind, Systembetrieb aufzunehmen. Steht der interne Modulfehler weiter an, führt das Prozessormodul einen zweiten Reboot durch.

Tritt innerhalb einer Minute nach dem Neustart ein weiterer interner Fehler auf, dann nimmt das Prozessormodul nicht mehr am Systembetrieb teil.

Fällt das letzte oder einzige Prozessormodul aus, so beendet das gesamte System den Systembetrieb, d. h. Protokollverbindungen werden geschlossen, E/A-Ausgänge werden energielos.

Ist ein automatischer Neustart nicht erwünscht, so ist der Ressource-Parameter *Autostart* zu deaktivieren.

4.5 Austausch von Prozessormodulen

Vor dem Austausch von Prozessormodulen ist darauf zu achten, dass ein noch laufendes HIMax System dabei nicht gestoppt wird.

Dies gilt besonders für Systeme, die nach dem Arbeitsstromprinzip arbeiten. Bei diesen führt ein Ausfall des Systems zum Verlust der Sicherheitsfunktion.

Redundante Prozessormodule können im laufenden Betrieb ausgetauscht werden, sofern noch mindestens ein Prozessormodul verfügbar ist, das während des Austauschs den sicherheitsbezogenen Betrieb aufrechterhält.

HINWEIS



Unterbrechung des sicherheitsbezogenen Betriebs möglich!

Der Betrieb der Steuerung kann durch Austausch eines Prozessormoduls unterbrochen werden, bei dem die LED Ess leuchtet oder blinkt.

Prozessormodule, bei denen die LED Ess leuchtet oder blinkt, nicht entfernen!

Die leuchtende oder blinkende LED **Ess** ist ein Hinweis, dass das Prozessormodul für das Funktionieren des Systems unbedingt benötigt wird.

Auch wenn die LED nicht leuchtet oder blinkt, sind die Systemredundanzen, an denen dieses Prozessormodul beteiligt ist, mit Hilfe von SILworX zu überprüfen. Dabei sind auch die Kommunikationsverbindungen zu beachten, die über das Prozessormodul abgewickelt werden.

Weitere Informationen über den Austausch von Prozessormodulen finden Sie in den Handbüchern der Prozessormodule, HI 801 008 D und HI 801 354 D, und im Systemhandbuch HI 801 000 D.

5 Systembusmodul

Ein Systembusmodul verwaltet einen der beiden sicherheitsbezogenen Systembusse. Die beiden Systembusse arbeiten redundant zueinander. Jeder Systembus verbindet alle Module und Basisträger miteinander. Über die Systembusse werden die sicheren Daten mit Hilfe eines sicherheitsbezogenen Protokolls übertragen.

Es ist möglich, ein HIMax System, das **nur ein Prozessormodul** enthält, bei verminderter Verfügbarkeit mit nur einem Systembus zu betreiben.

Anstelle der Systembusmodule können in Rack 0 auch Prozessormodule vom Typ X-CPU 31 eingesetzt werden. Für diese gelten die Aussagen dieses Kapitels ebenfalls. Die Prozessormodule X-CPU 31 erfordern ein spezielles Connector Board mit doppelter Breite.

5.1 Rack-ID

Die Rack-ID identifiziert einen Basisträger innerhalb einer Ressource und muss für jeden Basisträger eindeutig sein.

Die Rack-ID ist der **Sicherheitsparameter** für die Adressierung der einzelnen Basisträger und der darauf befindlichen Module!

Die Rack-ID wird im Connector Board des Systembusmoduls gespeichert.

Die Vorgehensweise zum Einstellen der Rack-ID ist im Systemhandbuch HI 801 000 D und im Erste-Schritte-Handbuch HI 801 102 D beschrieben.

5.2 Attribut «Responsible»

Nur eines der Systembusmodule pro Systembus darf das Attribut *Responsible* haben und damit als verantwortlich für den Betrieb des Systembusses parametrierbar sein.

- Für den Systembus A ist das Attribut *Responsible* fest für das Systembusmodul oder das Prozessormodul X-CPU 31 in Rack 0, Steckplatz 1 gesetzt.
- Für den Systembus B gilt:
 - Bei Verwendung von Systembusmodulen ist das Attribut mit SILworX einstellbar. Das Attribut *Responsible* kann entweder für das Systembusmodul im Rack 0, Steckplatz 2, oder für das Systembusmodul im Rack 1, Steckplatz 2, gesetzt werden.
 - Bei Verwendung des Prozessormoduls X-CPU 31 ist das Attribut *Responsible* fest für das Modul in Rack 0, Steckplatz 2 gesetzt.

Vor der Aufnahme des sicherheitsbezogenen Betriebs muss die korrekte Konfiguration des Attributs *Responsible* für beide Systembusse sichergestellt werden.

Die Vorgehensweise zum Einstellen des Attributs *Responsible* ist im Erste-Schritte-Handbuch HI 801 102 D beschrieben.

WARNUNG



Personenschaden möglich!

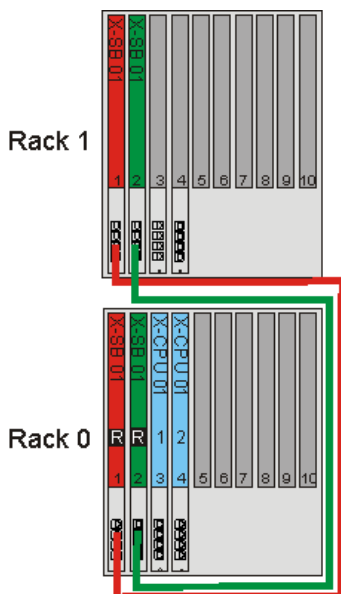
Die Parametrierung muss mit Hilfe von SILworX verifiziert werden.

Dabei ist unbedingt folgende Vorgehensweise einzuhalten:

- In SILworX per Modul-Login am Systembusmodul in Rack 0, Steckplatz 2 anmelden.
- In SILworX per Modul-Login am Systembusmodul in Rack 1, Steckplatz 2 anmelden.
- In den geöffneten Control Panels beider Systembusmodule überprüfen, dass das Attribut *Responsible* nur beim richtigen Systembusmodul gesetzt ist (siehe Bild 1 und Bild 2)!

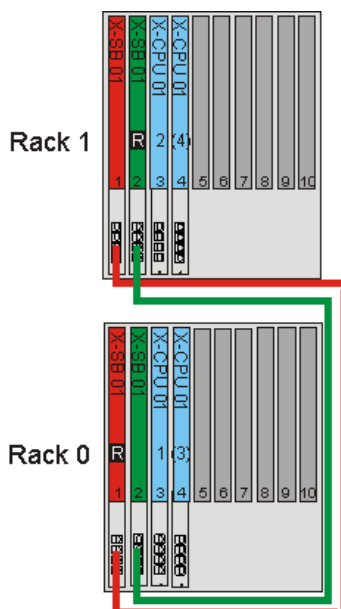
Empfohlene Konfigurationen:

- Enthält nur das Rack 0 Prozessormodule, dann ist das Attribut *Responsible* bei beiden Systembusmodulen des Racks 0 zu setzen (Bild 1).
- Enthält auch das Rack 1 Prozessormodule (Bild 2), dann ist das Attribut *Responsible* wie folgt zu setzen:
 - Für das Systembusmodul in Rack 0 auf Steckplatz 1 (automatisch).
 - Für das Systembusmodul in Rack 1 auf Steckplatz 2.



R Systembusmodul ist responsible

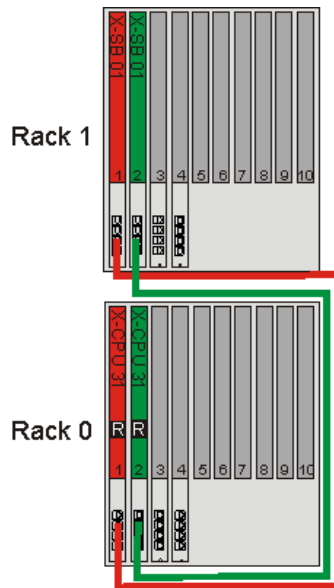
Bild 1: Empfohlene Konfiguration: alle Prozessormodule auf Rack 0



R Systembusmodul ist responsible

Bild 2: Empfohlene Konfiguration: Prozessormodule X-CPU 01 auf Rack 0 und Rack 1

- Bei Einsatz von Prozessormodulen X-CPU 31 in Rack 0, Steckplatz 1 und 2 (Bild 3) ist das Attribut *Responsible* immer für die Prozessormodule zu setzen. Für das Systembusmodul in Rack 1, Steckplatz 2 darf das Attribut *Responsible* nicht gesetzt sein!



R Prozessormodul ist responsible

Bild 3: Konfiguration mit Prozessormodulen X-CPU 31 auf Rack 0, Steckplätze 1 und 2

6 Kommunikationsmodul

Kommunikationsmodule dienen sowohl dem sicherheitsbezogenen Datenaustausch mit anderen HIMA Steuerungen, als auch dem Standard-Datenaustausch über Feldbusse und Ethernet.

- Das Prozessormodul steuert den sicherheitsbezogenen Datenverkehr durch das SIL 3-zertifizierte Übertragungsprotokoll **safeethernet** und HIPRO-S V2. Das Kommunikationsmodul leitet die Daten an die verbundenen HIMA Steuerungen weiter. Durch das sicherheitsbezogene Protokoll **safeethernet** ist sichergestellt, dass Verfälschungen von Nachrichten erkannt werden (Black-Channel-Prinzip).
Dadurch ist sicherheitsbezogene Kommunikation über nicht sicherheitsbezogene Übertragungswege, d. h., Standard-Netzwerkkomponenten, möglich.
- Die unterstützten Standardprotokolle sind der Tabelle 18 zu entnehmen.

Näheres zu Kommunikation und Kommunikationsmodulen finden Sie in den folgenden Dokumenten:

- Kapitel 12.1 dieses Handbuchs.
- Handbuch des Kommunikationsmoduls HI 801 010 D.
- Kommunikationshandbuch HI 801 100 D.
- Systemhandbuch HI 801 000 D.

7 Eingangsmodule

Nachfolgende Tabelle gibt eine Übersicht über die Eingangsmodule des HIMax Systems:

Digitale Eingangsmodule ¹⁾	Kanäle	Sicherheitsbezogen	Anmerkung
X-DI 32 01	32	SIL 3	24 VDC
X-DI 32 02	32	SIL 3	Näherungsschalter (NAMUR)
X-DI 32 03	32	SIL 3	48 VDC
X-DI 32 04	32	SIL 3	Ereigniserfassung
X-DI 32 05	32	SIL 3	Näherungsschalter (NAMUR) und Ereigniserfassung
X-DI 32 51	32	---	24 VDC
X-DI 32 52	32	---	Näherungsschalter (NAMUR)
X-DI 64 01	64	SIL 3	24 VDC
X-DI 64 51	64	---	24 VDC
Analoge Eingangsmodule ¹⁾	Kanäle	Sicherheitsbezogen	Anmerkung
X-AI 16 51	16	SIL 1	0/4 ... 20 mA Thermoelemente
X-AI 32 01	32	SIL 3	0/4 ... 20 mA
X-AI 32 02	32	SIL 3	0/4 ... 20 mA Ereigniserfassung
X-AI 32 51	32	---	0/4 ... 20 mA
Zählermodule ¹⁾	Kanäle	Sicherheitsbezogen	Anmerkung
X-CI 24 01	24	SIL 3	---
X-CI 24 51	24	---	---
¹⁾ Rückwirkungsfrei: Führt ein Modul einen Teil einer Sicherheitsfunktion aus, so wird diese durch den Betrieb weiterer Module nicht gestört. Unabhängig davon, ob die Module sicherheitsbezogen sind oder nicht.			

Tabelle 9: Übersicht Eingangsmodule

7.1 Allgemein

Sicherheitsbezogene Eingänge dürfen sowohl für sicherheitsbezogene als auch für nicht sicherheitsbezogene Signale benutzt werden. Die nicht sicherheitsbezogenen Signale dürfen jedoch nicht für Sicherheitsfunktionen verwendet werden!

Die sicherheitsbezogenen Eingangsmodule führen während des Betriebs automatisch einen hochwertigen, zyklischen Selbst-Test durch.

Werden bei den Selbst-Tests Fehler erkannt führt dies automatisch zu einer sicherheitsbezogenen Reaktion. Dem Anwenderprogramm wird über eine globale Variable der Initialwert zur Verfügung gestellt und entsprechenden Fehlermeldungen erzeugt. Die detaillierten Fehlermeldungen können im Anwenderprogramm durch das Auslesen der Fehlercodes ausgewertet werden.

Zu den Einzelheiten der Eingangsmodule siehe die Modulhandbücher.

7.2 Reaktion im Fehlerfall

Wird an den Signaleingängen ein Fehler festgestellt, verarbeitet das Anwenderprogramm den Initialwert des Eingangs. Ein Modulfehler des Eingangsmoduls führt dazu, dass das Anwenderprogramm für alle Eingänge den Initialwert verarbeitet. Der Initialwert der globalen Variable muss in SILworX entsprechend parametrisiert sein (Standardwert = 0). Das Modul aktiviert die LED *Error*.

Die Fehlermeldungen, die Statusmeldungen und die Systemvariablen können zur Programmierung von anwenderspezifischen Fehlerreaktionen verwendet werden. Weitere Informationen finden Sie in den Handbüchern des jeweiligen Moduls.

7.3 Sicherheit von Sensoren, Encodern und Transmittern

In einer sicherheitsbezogenen Anwendung müssen sowohl die Steuerung (PES) als auch die daran angeschlossenen Sensoren, Encoder und Transmitter den Sicherheitsanforderungen und dem spezifizierten SIL entsprechen. Hinweise zum Erreichen des notwendigen SIL für die Sensoren ist zum Beispiel in IEC 61511-1, Abschnitt 11.4 zu finden.

7.4 Sicherheitsbezogene digitale Eingangsmodule

Die Eingangsmodule lesen die digitalen Signale an den Eingängen ein und liefern in jedem Zyklus des Prozessormoduls sichere Werte an das Anwenderprogramm. Die Module testen die Eingänge zyklisch auf sichere Funktion.

7.4.1 Test-Routinen

Die Test-Routinen prüfen, ob die Eingangskanäle in der Lage sind, beide Signalpegel (Low- und High-Pegel) durchzuschalten, unabhängig von den anstehenden Eingangssignalen. Dieser Funktionstest wird bei jedem Lesen der Eingangssignale durchgeführt. Bei jedem Fehler im Eingangsmodul wird im Anwenderprogramm der Low-Pegel (sicherer Zustand) verarbeitet.

7.4.2 Redundanz von digitalen Eingängen

Die redundante Verschaltung von digitalen Eingängen ist zulässig. Eine redundante Verschaltung dient der Erhöhung der Verfügbarkeit der Eingänge.

7.4.3 Surge auf digitalen Eingängen

Durch die kurze Zykluszeit der HIMax Systeme können digitale Eingänge einen Surge-Impuls nach EN 61000-4-5 als kurzzeitigen High-Pegel einlesen.

Bei Verwendung abgeschirmter Kabel für digitale Eingänge sind keine weiteren Maßnahmen zur Vorsorge gegen Surge erforderlich.

Folgende Maßnahmen vermeiden Fehlfunktionen in Umgebungen, in denen Surges auftreten können:

- Installation abgeschirmter Eingangsleitungen.
- Einstellen einer Einschaltverzögerung $EV [\mu s]$ von mindestens 2000 μs in den Moduleigenschaften des Hardware-Editors.
- Einstellen einer Ausschaltverzögerung $AV [\mu s]$ von mindestens 2000 μs in den Moduleigenschaften des Hardware-Editors.

Beim Einstellen einer Ein- oder Ausschaltverzögerung erfolgt die Fehlerreaktion entsprechend verzögert. Dies ist bei der Auslegung der Sicherheitszeit der Ressource zu beachten.

i

Auf obige Maßnahmen kann verzichtet werden, wenn durch die Auslegung der Anlage Surges im System ausgeschlossen werden können.

Zur Auslegung gehören insbesondere Schutzmaßnahmen betreffend Überspannung, Blitzschlag, Erdung und Anlagenverdrahtung auf Basis der Angaben im Systemhandbuch HI 801 000 D und der relevanten Normen.

7.5 Sicherheitsbezogene analoge Eingangsmodule

Analoge Eingangsmodule wandeln die gemessenen Eingangsströme in einen Wert vom Datentyp DINT (double integer); den *Rohwert*, und in einen *Prozesswert* vom Datentyp REAL um. Der *Rohwert* enthält das gemessene Eingangssignal, während der Prozesswert ein skalierter Wert ist.

Näherungsschalter-Eingänge erzeugen durch Vergleich des Rohwerts mit parametrierbaren Schwellenwerten einen Digitalwert.

7.5.1 Test-Routinen

Das Modul erfasst die Analogwerte auf zwei Wegen und vergleicht die Ergebnisse miteinander. Zusätzlich testet es zyklisch die Funktion der Eingangswege.

7.5.2 Redundanz von analogen Eingängen

Die redundante Verschaltung von analogen Eingängen ist zulässig. Eine redundante Verschaltung wird für die Verfügbarkeit der Eingänge verwendet.

Der SIL-Wert des Eingangsmoduls X-AI 16 51 lässt sich durch die im Handbuch HI 801 178 D beschriebenen Verschaltungen erhöhen.

7.5.3 Zustand von LL, L, N, H, HH bei X-AI 32 01 und X-AI 32 02

Für sicherheitsbezogene Anwendungen der Module X-AI 32 01 und X-AI 32 02 gilt:

Wenn für einen Kanal skalare Ereignisse für Grenzwerte definiert sind, dann müssen die Zustandsvariablen -> *Zustand LL*, -> *Zustand L*, -> *Zustand N*, -> *Zustand H*, -> *Zustand HH* mit der Variablen *Kanal OK* verknüpft werden.

Im Fehlerfall liefern die Zustandsvariablen den Wert FALSE.

7.6 Sicherheitsbezogene Zählermodule

Sicherheitsbezogene Zählermodule können, abhängig von ihrer Konfiguration, folgende Prozesswerte liefern:

- Zählerstände als ganzzahlige Werte oder als skalierte Gleitkommawerte.
- Drehzahlen oder Frequenzen als ganzzahlige Werte oder als skalierte Gleitkommawerte.
- Weitere Hilfswerte wie Überlauf.

Nähere Einzelheiten siehe Modulhandbuch HI 801 112 D.

7.6.1 Test-Routinen

Das Modul erfasst die Zählerwerte auf drei Wegen parallel und vergleicht die Ergebnisse miteinander. Zusätzlich testet es zyklisch die Funktion der Eingangswege.

7.6.2 Beim Zählermodul X-CI 24 01 zu beachten!

Beim Einsatz des Zählermoduls X-CI 24 01 sind folgende Besonderheiten zu beachten, siehe auch das Modulhandbuch HI 801 112 D:

- Während des Reload können innerhalb der ersten 3 Zyklen Eingangs-Impulse verlorengehen, wenn folgende Parameter während des Reloads geändert werden:
 - Auswertart Zählimpulse
 - Benutzte Kanalpaare
- Fällt bei der Flankenwertung „2 Phasen, 4 Flanken“ der Sensor eines Kanals aus, ohne dass ein Leitungsbruch oder Leitungsschluss erkannt wird, registriert das Modul die Hälfte der tatsächlichen Frequenz.
- Zu zählende Impulse können bei automatischem Wiederanlauf verlorengehen.
- Automatischer oder manueller Wiederanlauf des Moduls ist applikationsspezifisch zu betrachten.
- Applikationsempfehlung:
 - bei Mehrphasen-Auswertung und Drehrichtungserkennung wird der Einsatz redundanter Sensoren empfohlen, da nur so der Sensorausfall erkannt werden kann.
 - Die Parametrierung von Störaustastung ist bei Frequenzmessung sicherheitstechnisch unbedenklich.

7.6.3 Redundanz von Zählereingängen

Die redundante Verschaltung von Zählereingängen ist zulässig. Eine redundante Verschaltung erhöht die Verfügbarkeit der Eingänge.

7.7 Checklisten Eingänge

HIMA empfiehlt, die verfügbare Checkliste zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsbezogenen Eingängen einzusetzen. Die Checkliste ist als Planungsunterlage einsetzbar und dient gleichzeitig als Nachweis für eine sorgfältig durchgeführte Planung.

Für jeden einzelnen der in einem System eingesetzten sicherheitsbezogenen Eingangskanäle ist im Rahmen der Projektierung und Inbetriebnahme eine eigene Checkliste zur Kontrolle der zu berücksichtigenden Anforderungen auszufüllen. Nur dann ist sichergestellt, dass die Anforderungen vollständig und übersichtlich erfasst sind. Die Checkliste ist auch eine Dokumentation über den Zusammenhang zwischen externer Verdrahtung und Anwenderprogramm.

Die aktuellen Checklisten können über die E-Mail-Adresse documentation@hima.com angefragt werden. Für registrierte Kunden stehen die Produktdokumentationen im HIMA Extranet als Download zur Verfügung.

8 Ausgangsmodule

Nachfolgende Tabelle zeigt eine Übersicht der HIMax Ausgangsmodule:

Digitale Ausgangsmodule	Kanäle	Sicherheitsbezogen	Anmerkung
X-DO 12 02	12	SIL 3	24 VDC, ≤ 2 A
X-DO 24 01	24	SIL 3	24 VDC, $\leq 0,5$ A
X-DO 24 02	24	SIL 3	48 VDC, $\leq 0,5$ A
X-DO 32 01	32	SIL 3	24 VDC, $\leq 0,5$ A
X-DO 32 51	32	---	24 VDC, $\leq 0,5$ A
Relaismodule ¹⁾	Kanäle	Sicherheitsbezogen	Anmerkung
X-DO 12 01	12	SIL 3	230 VAC/VDC
X-DO 12 51	12	---	230 VAC/VDC
Analoge Ausgangsmodule	Kanäle	Sicherheitsbezogen	Anmerkung
X-AO 16 01	16	SIL 3	0 ... 20 mA, paarweise sicher elektr. getrennt
X-AO 16 51	16	---	0 ... 20 mA
¹⁾ Sicher elektrisch getrennt.			

Tabelle 10: Übersicht Ausgangsmodule

8.1 Allgemein

Die sicherheitsbezogenen Ausgangsmodule werden einmal in jedem Zyklus beschrieben, die Ausgangssignale zurückgelesen und mit den vorgegebenen Ausgangsdaten verglichen.

Bei den Ausgängen ist der Wert «0» oder der geöffnete Relaiskontakt der sichere Zustand.

Zu den Einzelheiten der Ausgangsmodule siehe die Modulhandbücher.

8.2 Reaktion im Fehlerfall

Wenn die Test-Routinen einen Fehler feststellen, überführt die Steuerung den jeweiligen Ausgang in den sicheren Zustand. Ein Fehlercode wird erzeugt.

Der Fehlercode und weitere Systemvariablen können zur Programmierung von anwenderspezifischen Fehlerreaktionen verwendet werden. Weitere Informationen finden Sie in den Handbüchern des jeweiligen Moduls.

Fehler des gesamten Ausgangsmoduls führen dazu, dass alle Ausgänge in den sicheren Zustand überführt werden.

Im Fehlerfall aktiviert das Modul aktiviert die LED *Error*.

8.3 Sicherheit von Aktoren

In einer sicherheitsbezogenen Anwendung müssen sowohl die Steuerung (PES) als auch die daran angeschlossenen Aktoren den Sicherheitsanforderungen und dem spezifizierten SIL entsprechen. Hinweise zum Erreichen des notwendigen SIL für Aktoren zum Beispiel in IEC 61511-1, Abschnitt 11.4.

8.4 Sicherheitsbezogene digitale Ausgangsmodule

In den sicherheitsbezogenen Ausgangskanälen sind zusätzlich zur Einzelkanalabschaltung drei testbare Schalter in Serie integriert. Somit ist die Anforderung für SIL 3 nach einem sicheren, unabhängigen zweiten Abschaltweg erfüllt. Diese integrierte Sicherheitsabschaltung schaltet im Fehlerfall die einzelnen Kanäle des defekten Ausgangsmoduls sicher ab (energieloser Zustand).

Außerdem ist das Watchdog-Signal des Moduls der zweite Abschaltweg: Ein Wegfall des Watchdog-Signals bewirkt den sofortigen Übergang in den sicheren Zustand.

8.4.1 Test-Routinen

Die Module werden automatisch während des Betriebs getestet. Die wesentlichen Testfunktionen sind:

- Rücklesen der Ausgangssignale.
- Prüfen der integrierten zweifachen Sicherheitsabschaltung.
- Abschalttest der Ausgänge.
- Überwachung der Betriebsspannung.

8.4.2 Ausgangs-Störaustastung

Die Ausgangs-Störaustastung wird vom Ausgangsmodul selbst ausgeführt. Diese unterdrückt die Abschaltreaktion eines Kanals auf eine Abweichung zwischen Vorgabewert und Rücklesewert des Ausgangskanals. Die Ausgangs-Störaustastung kann für jedes Ausgangsmodul aktiviert werden (Standardeinstellung: Deaktiviert), siehe Handbücher der Ausgangsmodule.

Wenn die Ausgangs-Störaustastung aktiviert ist, kann sich die Reaktionszeit bis auf den Wert *Sicherheitszeit – Watchdog-Zeit* verlängern.

8.4.3 LB-Austastung

Die LB-Austastung kann für die Module X-DO 24 01 und X-DO 24 02 parametrierbar werden und wird vom Ausgangsmodul selbst ausgeführt.

Der Parameter *LB-Austastung (Anzahl LS/LB-Intervalle)* definiert die Anzahl von Testintervallen (Parameter *LS/LB-Intervall [μs]*), die ablaufen müssen, bis ein erkannter Feldfehler als Leitungsbruch an das Prozessormodul (X-CPU) übermittelt wird. Bis zur Fehlerreaktion werden transiente Störungen unterdrückt. Die Einstellung von *LB-Austastung (Anzahl LS/LB-Intervalle)* wird für alle Kanäle übernommen.

Mit der Einstellung von *LB-Austastung (Anzahl LS/LB-Intervalle) > 1* verlängert sich die Reaktionszeit. Dies ist bei der Parametrierung der Sicherheitszeit und der Watchdog-Zeit zu beachten.

8.4.4 Verhalten bei externem Kurzschluss oder Überlast

Bei einem Schluss des Ausgangs nach L- oder bei Überlast bleibt die Sicherheit des Moduls erhalten.

Die Ausgänge werden in diesem Zustand zyklisch im Abstand weniger Sekunden geprüft, ob die Überlast noch vorhanden ist. Bei Normalzustand werden die Ausgänge wieder zugeschaltet.

8.4.5 Redundanz von digitalen Ausgängen

Die redundante Verschaltung von digitalen Ausgängen ist zulässig. Eine redundante Verschaltung dient der Erhöhung der Verfügbarkeit der Ausgänge.

8.5 Sicherheitsbezogene Relaismodule

Relaismodule werden eingesetzt, wenn eine oder mehrere der folgenden Bedingungen für den angeschlossenen Aktor zutreffen:

- Elektrische und galvanische Trennung notwendig.
- Schalten von hohen Stromstärken.
- Schalten von Wechselströmen.

Beim Modul sind die Ausgänge mit zwei Sicherheitsrelais mit zwangsgeführten Kontakten ausgestattet. Damit können die Ausgänge für Sicherheitsabschaltungen entsprechend SIL 3 verwendet werden.

Außerdem ist das Watchdog-Signal des Moduls der zweite Abschaltweg: Ein Wegfall des Watchdog-Signals bewirkt den sofortigen Übergang in den sicheren Zustand.

8.5.1 Test-Routinen

Die Module werden automatisch während des Betriebs getestet. Die wesentlichen Testfunktionen sind:

- Rücklesen der Ausgangssignale der Schaltverstärker vor den Relais.
- Prüfen des Schaltens der Relais mit zwangsgeführten Kontakten.
- Prüfen der integrierten zweifachen Sicherheitsabschaltung.
- Überwachung der Betriebsspannung.

8.5.2 Redundanz von Relaisausgängen

Die redundante Verschaltung von Relaisausgängen ist zulässig. Eine redundante Verschaltung dient der Erhöhung der Verfügbarkeit der Relaisausgänge.

8.6 Sicherheitsbezogene analoge Ausgangsmodule

Sicherheitsbezogene analoge Ausgangsmodule geben die im Anwenderprogramm ermittelten Werte an Aktoren weiter.

Sicherheitsbezogene analoge Ausgänge lesen ihre Ausgangswerte zurück und vergleichen diese mit den auszugebenden Werten. Bei Abweichungen erfolgt die Fehlerreaktion.

8.6.1 Test-Routinen

Die Module werden automatisch während des Betriebs getestet. Die wesentlichen Testfunktionen sind:

- Rücklesen der Ausgangssignale.
- Prüfen der integrierten zweifachen Sicherheitsabschaltung.

Wenn Fehler auftreten, werden die Ausgänge auf den sicheren Wert 0 mA gesetzt.

8.6.2 Ausgangs-Störaustastung

Die Ausgangs-Störaustastung wird vom Ausgangsmodul selbst ausgeführt. Diese unterdrückt die Abschaltreaktion eines Kanals auf eine Abweichung zwischen Vorgabewert und Rücklesewert des Ausgangskanals. Die Ausgangs-Störaustastung kann für jedes Ausgangsmodul aktiviert werden (Standardeinstellung: Deaktiviert), siehe Handbücher der Ausgangsmodule.

Wenn die Ausgangs-Störaustastung aktiviert ist, kann sich die Reaktionszeit bis auf den Wert *Sicherheitszeit – Watchdog-Zeit* verlängern.

8.6.3 Verhalten bei externem Leitungsbruch

Bei einem Leitungsbruch schaltet das Modul den Strom für ca. 8 ms zu und prüft, ob der Leitungsbruch noch besteht. Ist das der Fall, schaltet es für ca. 10 s ab. Dieser Ablauf kann sich beliebig oft wiederholen.

8.6.4 Beim analogen Ausgangsmodul X-AO 16 01 zu beachten!

Beim Einsatz des analogen Ausgangsmoduls unbedingt folgende Besonderheiten beachten:

- Nur die im Modulhandbuch HI 801 110 D aufgeführten Verschaltungen sind zulässig!
- Bei serieller Redundanz von mehr als zwei Modulen kann die SELV-Spannung überschritten werden!
- Bei serieller Redundanz ist von jeder Gruppe von zwei Kanälen nur einer zu verwenden!
- Findet HART-Kommunikation zwischen einem angeschlossenen Aktor und einem HART-Terminal statt, kann die Kommunikation das Ausgangssignal um bis zu 1 % vom Endwert verfälschen!
- Beim Auftreten eines Fehlers kann die Zeit bis zum Erreichen des sicheren Zustands im Worst Case bis zu 16 ms betragen. Diese Zeit ist bei der Reaktionszeit und bei der Sicherheitszeit zu berücksichtigen!
- Das Anwenderprogramm darf analoge Ausgänge nicht in kürzeren Zyklen als 6 ms beschreiben.
- Im Fehlerfall gibt das Modul den sicheren Wert 0 mA aus, auch bei Überschreitung der oberen Grenze des Einstellbereichs.

Zu Einzelheiten siehe das Modulhandbuch HI 801 110 D.

8.6.5 Redundanz von analogen Ausgängen

Die redundante Verschaltung von analogen Ausgängen ist zulässig. Eine analoge Verschaltung wird für die Verfügbarkeit der Ausgänge verwendet.

8.7 Checklisten Ausgänge

HIMA empfiehlt, die verfügbare Checkliste zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsbezogenen Ausgängen einzusetzen. Die Checkliste ist als Planungsunterlage einsetzbar und dient gleichzeitig als Nachweis für eine sorgfältig durchgeführte Planung.

Für jeden einzelnen der in einem System eingesetzten sicherheitsbezogenen Ausgangskanäle ist im Rahmen der Projektierung und Inbetriebnahme eine eigene Checkliste zur Kontrolle der zu berücksichtigenden Anforderungen auszufüllen. Nur dann ist sichergestellt, dass die Anforderungen vollständig und übersichtlich erfasst sind. Die Checkliste ist auch eine Dokumentation über den Zusammenhang zwischen externer Verdrahtung und Anwenderprogramm.

Die aktuellen Checklisten können über die E-Mail-Adresse documentation@hima.com angefragt werden. Für registrierte Kunden stehen die Produktdokumentationen im HIMA Extranet als Download zur Verfügung.

9 Spezielle E/A-Module

HIMA hat für spezielle Anwendungen folgende E/A-Module entwickelt:

- HART-Kommunikationsmodul X-HART 32 01.
- Überdrehzahlschutz-Modul X-MIO 7/6 01.

9.1 HART-Modul X-HART 32 01

Das HART-Modul dient zur Kommunikation mit HART-fähigen Sensoren und Aktoren.

Weitere Informationen finden Sie im Modulhandbuch HI 801 306 D.

9.1.1 Sicherheitsfunktion

Die Sicherheitsfunktion des X-HART 32 01 Moduls umfasst die folgenden Punkte:

- HART-Deaktivierung: Im abgeschalteten Fall werden die HART-Kanäle gemäß SIL 3 sicher deaktiviert.
- HART-Filterung: HART-Zugriffe auf HART-Transmitter oder Sensoren werden gemäß SIL 3 gesperrt.
- Die HART-Kommunikation beeinflusst die Genauigkeit der analogen Messung um 1 %.
Weitere Rückwirkungen auf die analogen Module sind ausgeschlossen.
- Wird die HART-Filterung auf dem X-HART-Modul deaktiviert, ist ein Umprogrammieren des zugehörigen analogen Sensors oder Aktors möglich. Dies kann die Sicherheit beeinträchtigen.

9.2 Überdrehzahlschutz-Modul X-MIO 7/6 01

Das Modul dient der Drehzahlüberwachung und der NOT-AUS-Abschaltung (Trip-Funktion) einer Turbine. Zu Einzelheiten siehe das Modulhandbuch HI 801 304 D.

Mit dem Modul können Applikationen gemäß der API 670 realisiert werden. Das Modul erfüllt die in der API 670 geforderten Anforderungen zu Drehzahlüberwachung und Abschalttroutinen für Turbinen. Die Drehzahlüberwachung und die Abschalttroutinen arbeiten hierbei unabhängig vom HIMax Gesamtsystem und dem Anwenderprogramm.

9.2.1 Sicherheitsfunktion

Das Modul überwacht unabhängig vom HIMax Gesamtsystem und dem Anwenderprogramm die Drehzahl einer Turbine. Das Modul führt eigenständig die Abschaltung der Turbine über die digitalen Ausgänge aus.

Je Messeingang nimmt das Modul die Drehzahl und die Drehrichtung eines Sensors mit sicherheitstechnischer Genauigkeit auf. Für die Ermittlung der Drehzahl sind für eine Turbine drei Sensoren vorgesehen. Aus den ermittelten Drehzahlwerten der drei Sensoren führt das Modul eine 2oo3-Auswertung durch. Das Ergebnis steht dem sicherheitsbezogenen Prozessorsystem der X-MIO 7/6 01 und dem Anwenderprogramm zur Verfügung.

Für die 2oo3-Auswertung müssen mindestens zwei der drei Drehzahleingänge fehlerfrei erfasst werden. Wenn einer der Drehzahleingänge nicht fehlerfrei erfasst werden kann, gibt das Modul eine Warnung aus. Wenn nur ein oder kein Drehzahleingang fehlerfrei erfasst werden kann, wird die Trip-Funktion ausgelöst!

Die aufgenommenen Drehzahlwerte werden miteinander verglichen und auf die Einhaltung der Grenzwerte sicherheitstechnische Genauigkeit ($\pm 0,1$ % vom Messwert) und Parameter *Max. zulässige Drehzahlabweichung [U/min]* überprüft. Für die Auswertung ist immer der Größere der beiden Grenzwerte maßgebend.

Weicht ein Drehzahlwert von den anderen beiden Drehzahlwerten über die beiden Grenzwerte ab, erfolgen die oben beschriebenen Aktionen. Liegt mehr als ein Drehzahlwert außerhalb dieser Grenzen, wird die Trip-Funktion ausgelöst.

Bei der Einstellung des Parameters *Max. zulässige Drehzahlabweichung [U/min]* ist folgendes zu beachten: Je größer der Parameter gewählt wird, desto höher ist die Reaktionszeit bis zur Abschaltung (Verzögerungszeit). Ist für die Auswertung der Parameter *Max. zulässige Drehzahlabweichung [U/min]* maßgebend, berechnet sich die Verzögerungszeit (t_v) wie folgt:

$$t_v[s] = \frac{\text{Maximal zulässige Drehzahlabweichung} \left[\frac{U}{\text{min}} \right]}{\text{Beschleunigung} \left[\frac{U/\text{min}}{s} \right]} + \text{Trip- Störaustastungszeit in (s)}$$

Ist für die Auswertung die sicherheitstechnische Genauigkeit ($\pm 0,1$ % vom Messwert) maßgebend, berechnet sich die Verzögerungszeit (t_v) wie folgt:

$$t_v[s] = \frac{\text{Sicherheitstechnische Genauigkeit in } \left(\frac{U}{\text{min}} \right)}{\text{Beschleunigung} \left[\frac{U/\text{min}}{s} \right]} + \text{Trip Störaustastungszeit in (s)}$$

Das Modul enthält sicherheitsbezogene digitale Ausgänge wie in Kapitel 8.3 beschrieben.

Die Sicherheitsfunktion aller Eingänge und Ausgänge ist gemäß SIL 3 ausgeführt. Der Relaisausgang ist als potentialfreier, nicht sicherheitsbezogener Meldekontakt (Wechsler) ausgeführt.

9.2.2 Redundanz

Zur Erhöhung der Verfügbarkeit ist das Modul zweifach redundant einzusetzen. Dazu stehen ausschließlich zweifache Connector Boards zur Verfügung.

10 Software

Die Software für das sicherheitsbezogene Automatisierungssystem HIMax gliedert sich in die folgenden Teile:

- Programmierwerkzeug SILworX nach IEC 61131-3.
- Betriebssystem.
- Anwenderprogramm.

Mit dem Programmierwerkzeug wird das Anwenderprogramm erstellt, das die anlagenspezifischen Funktionen enthält, die das Automatisierungssystem ausführt. Das Programmierwerkzeug parametriert und bedient die Betriebssystemfunktionen der Hardware-Komponenten.

Der Codegenerator des Programmierwerkzeugs übersetzt das Anwenderprogramm in den Maschinencode. Das Programmierwerkzeug überträgt diesen Maschinencode über eine Ethernet-Schnittstelle in die Flash-EPROMs des Automatisierungssystems.

10.1 Sicherheitstechnische Aspekte von Betriebssystemen

Jedes zugelassene Betriebssystem ist eindeutig durch die Revisionsnummer und die CRC-Signatur gekennzeichnet. Die jeweils gültigen, vom TÜV für sicherheitsbezogene Automatisierungsgeräte zugelassenen Versionen des Betriebssystems und die dazugehörigen Signaturen (CRCs) unterliegen der Revisionskontrolle und werden in einer Versionsliste dokumentiert.

Die Versionsliste des HIMax Systems wird von der TÜV Rheinland GmbH und der HIMA Paul Hildebrandt GmbH gemeinsam erstellt und geführt.

Ein Auslesen der laufenden Betriebssystemversion ist nur mit dem Programmierwerkzeug SILworX möglich. Der Anwender muss prüfen, ob die in den Modulen geladenen Betriebssystemversionen gültig sind.

10.2 Arbeitsweise und Funktionen von Betriebssystemen

Das Betriebssystem arbeitet das Anwenderprogramm zyklisch ab. Dabei führt es in stark vereinfachter Form folgende Funktionen aus:

- Lesen der Eingangsdaten.
- Verarbeiten der Logikfunktionen, die gemäß IEC 61131-3 programmiert worden sind.
- Schreiben der Ausgangsdaten.

Hinzu kommen folgende wesentliche Funktionen:

- Umfangreiche Selbst-Tests.
- Tests der Eingänge und Ausgänge während des Betriebs.
- Datenübertragung.
- Diagnose.

10.3 Sicherheitstechnische Aspekte für die Programmierung

Bei der Erstellung oder Änderung eines Anwenderprogramms sind die in diesem Kapitel genannten Anforderungen zu beachten.

10.3.1 Sicherheitskonzept von SILworX

Das Sicherheitskonzept des Programmierwerkzeugs SILworX beinhaltet folgende Punkte:

- Bei der Installation von SILworX sichert eine CRC-Prüfsumme die Integrität des Programmierwerkzeugs auf dem Weg vom Hersteller zum Anwender.
- SILworX führt Plausibilitätsprüfungen durch, um Fehler bei der Eingabe zu verringern.
- SILworX führt eine doppelte Kompilierung mit anschließendem Vergleich der erzeugten Konfigurations-CRCs (Prüfsummen) durch. Dadurch ist sichergestellt, dass Verfälschungen an der Konfiguration durch temporäre Fehlfunktionen des benutzten PCs erkannt werden.
- SILworX und die in diesem Sicherheitshandbuch definierten Maßnahmen machen es hinreichend unwahrscheinlich, dass ein semantisch und syntaktisch korrekter Code erzeugt wird, der unerkannte systematische Fehler aus dem Prozess der Code-Erzeugung enthält.

Bei der ersten Inbetriebnahme einer sicherheitsbezogenen Steuerung ist die Sicherheit des gesamten Systems durch einen vollständigen Funktionstest vom Anwender zu prüfen.

- Prüfen, ob die Umsetzung der Steuerungsaufgabe anhand der Daten und Signalflüsse korrekt realisiert wurde.
- Prüfen der Logik aller Funktionen durch Erproben.

Nach Änderung an einem Anwenderprogramm sind mindestens diejenigen Programmteile zu testen, die von der Änderung betroffen sind. Mit dem sicheren Versionsvergleich von SILworX werden Änderungen gegenüber einer vorherigen Version ermittelt und nachgewiesen.

Bei jeder Inbetriebnahme einer sicherheitsbezogenen Steuerung sind die Anforderungen zur Verifikation und Validation bezüglich der Anwendungsnormen zu beachten!

10.3.2 Überprüfung der Konfiguration und der Anwenderprogramme

Um Anwenderprogramme auf Einhaltung der Sicherheitsfunktionen zu prüfen, muss der Anwender geeignete Testfälle erzeugen, welche die spezifizierten Sicherheitsfunktionen validieren.

In der Regel ist der unabhängige Test jedes einzelnen Loops (Eingang, Verarbeitung inklusive den anwenderseitigen Verknüpfungen, Ausgang) ausreichend.

Für die numerische Auswertung von Formeln sind geeignete Testfälle zu generieren. Die Auswertung kann z. B. mit Hilfe von Äquivalenzklassentests erfolgen. Die Testfälle müssen so gewählt werden, dass die Korrektheit der Berechnung nachgewiesen wird. Die notwendige Anzahl der Testfälle hängt von der verwendeten Formel ab und muss kritische Wertepaare umfassen.

HIMA empfiehlt, eine aktive Simulation mit Datenquellen durchzuführen. Damit ist eine korrekte Verdrahtung der Sensoren und Aktoren des Systems nachweisbar. Dies gilt ebenfalls für Sensoren und Aktoren, die über Remote I/Os am System angeschlossen sind.

SILworX ist als Prüfmittel verwendbar für:

- Prüfung von Eingängen.
- Forcen von Ausgängen.

Diese Vorgehensweise ist sowohl bei der Ersterstellung eines Anwenderprogramms als auch dessen Änderungen einzuhalten.

10.3.3 Archivierung eines Projekts

HIMA empfiehlt, nach jedem Download oder Reload das Projekt zu archivieren.

SILworX speichert alle Daten eines Projekts in einer einzigen Datei. HIMA empfiehlt aus Gründen der Datensicherheit das Projekt zusätzlich auf einem externen Medium zu speichern.

10.3.4 Identifizierung von Konfiguration und Programmen

Änderungen an Programmen haben Änderungen der Programm-CRCs zur Folge und somit Auswirkungen auf den Konfigurations-CRC.

Um Änderungen an der aktuellen Konfiguration festzustellen, wird das Projekt mit einer gespeicherten oder einer geladenen Konfiguration verglichen. Mit Hilfe des sicheren SILworX Versionsvergleichs können die Änderungen einzeln nachgewiesen werden.

10.4 Parameter der Ressource

Einige Parameter werden in SILworX für zulässige Aktionen im sicherheitsbezogenen Betrieb der Ressource festgelegt und als Sicherheitsparameter bezeichnet.

WARNUNG



Personenschaden durch fehlerhafte Konfiguration möglich!

Weder das Programmierwerkzeug noch die Steuerung können projektspezifisch festgelegte Parameter überprüfen. Deshalb unbedingt die Sicherheitsparameter korrekt ins Programmierwerkzeug eintragen und den erfolgten Eintrag nach dem Laden in die Steuerung (PES) dort überprüfen.

Diese Parameter sind:

- **Rack-ID, siehe 5.1 und das Systemhandbuch HI 801 000 D.**
- **Responsible-Attribut von Systembusmodulen oder Prozessormodulen, siehe 5.1.**
- **Die in Tabelle 11 als sicherheitsbezogen gekennzeichneten Parameter.**

Die während des sicherheitsbezogenen Betriebs möglichen Festlegungen sind nicht starr an eine bestimmte Anforderungsklasse gebunden, sondern müssen für jeden Einsatz der Steuerung mit der zuständigen Prüfstelle abgestimmt werden.

10.4.1 Systemparameter der Ressource

Die Systemparameter der Ressource legen das Verhalten der Steuerung während des Betriebs fest. Die Systemparameter sind in SILworX im Dialog *Eigenschaften* der Ressource einstellbar.

Systemparameter	S ¹⁾	Beschreibung	Einstellung für sicheren Betrieb
Name	N	Name der Ressource	Beliebig
System-ID [SRS]	J	System-ID der Ressource Wertebereich: 1 ... 65 535 Standardwert: 60 000 Es ist notwendig, der System-ID einen anderen Wert als den Standardwert zu zuweisen, sonst ist das Projekt nicht ablauffähig!	Eindeutiger Wert innerhalb des Netzwerks der Steuerungen. Das sind alle Steuerungen, die potenziell miteinander verbunden sind.
Sicherheitszeit [ms]	J	Sicherheitszeit der Ressource in Millisekunden, siehe Kapitel <i>Sicherheitsrelevante Zeiten</i> im Sicherheitshandbuch. Wertebereich: 20 ... 22 500 ms. Standardwert: 600 ms (online änderbar)	Applikations-spezifisch
Watchdog-Zeit [ms]	J	Watchdog-Zeit in Millisekunden, siehe Kapitel <i>Sicherheitsrelevante Zeiten</i> im Sicherheitshandbuch. Wertebereich: 6 ... 7500 ms Standardwert: 200 ms (online änderbar)	Applikations-spezifisch
Sollzykluszeit [ms]	N	Gewünschte oder maximale Zykluszeit, siehe <i>Sollzykluszeit-Modus</i> . Wertebereich 0 ... 7500 ms Standardwert: 0 ms (online änderbar) Die Sollzykluszeit darf höchstens so groß sein wie die eingestellte <i>Watchdog-Zeit [ms]</i> abzüglich des kleinsten einstellbaren Werts der <i>Watchdog-Zeit [ms]</i> (6 ms, s. o.), andernfalls wird die Eingabe abgelehnt. Ist der Standardwert 0 ms eingestellt, so wird die Sollzykluszeit nicht beachtet. Weitere Details siehe nachfolgende Kapitel.	Applikations-spezifisch
Sollzykluszeit-Modus	N	Verwendung der <i>Sollzykluszeit [ms]</i> , siehe nachfolgende Kapitel. Die Standardeinstellung ist fest-tolerant (online änderbar).	Applikations-spezifisch
Multitasking-Modus	N	Mode 1 Die Länge eines Zyklus der CPU richtet sich nach der benötigten Ausführungsdauer aller Anwenderprogramme.	Applikations-spezifisch
		Mode 2 Prozessor stellt von Anwenderprogrammen niederer Priorität nicht benötigte Ausführungszeit den Anwenderprogrammen hoher Priorität zur Verfügung. Betriebsart für hohe Verfügbarkeit.	
		Mode 3 Prozessor wartet nicht benötigte Ausführungszeit von Anwenderprogrammen ab und verlängert so den Zyklus.	
		Standardwert: Mode 1	
Max. Kom.-Zeitscheibe [ms]	N	Höchstwert in ms der Zeitscheibe, die innerhalb des Zyklus der Ressource für Kommunikation verwendet wird, siehe Kommunikationshandbuch HI 801 100 D. Wertebereich: 2 ... 5000 ms Standardwert: 60 ms	---

Systemparameter	S ¹⁾	Beschreibung	Einstellung für sicheren Betrieb
Optimierte Nutzung der Kom.-Zeitscheibe	N	<p>Der Systemparameter verkürzt die Antwortzeiten für die Kommunikation über das oder die Prozessormodule.</p> <hr/> <p>i Es kann sich die zeitliche Ausnutzung der <i>Max. Kom.-Zeitscheibe [ms]</i> und somit der Systemparameter <i>Max. Dauer Konfigurationsverbindungen [ms]</i> ändern, so dass diese stärker beansprucht werden können, z. B. beim Reload.</p> <hr/>	---
Max. Dauer Konfigurationsverbindungen [ms]	N	<p>Definiert, wie viel Zeit innerhalb eines CPU-Zyklus für die Konfigurationsverbindungen zur Verfügung steht: Wertebereich: 2 ... 3500 ms Standardwert: 20 ms Weitere Details siehe nachfolgende Kapitel.</p>	Applikations-spezifisch
Maximale Systembus-Latenzzeit [µs]	N	<p>Maximale Verzögerung einer Nachricht zwischen einem E/A-Modul und einem Prozessormodul. 100 ... 50 000 µs, Standardwert: <i>System-Standardwerte</i></p> <hr/> <p>i Für die Einstellung der maximalen Systembuslatenz auf einen Wert \neq <i>System-Standardwerte</i> ist eine Lizenz erforderlich.</p> <hr/>	Applikations-spezifisch
Online-Einstellungen erlauben	J	<p>TRUE: Alle unter FALSE genannten Schalter/Parameter sind online mit dem PADT änderbar. Dies gilt nur, wenn die Systemvariable <i>Read-only in RUN</i> den Wert FALSE hat. Standardwert: TRUE.</p>	HIMA empfiehlt die Einstellung FALSE.
		<p>FALSE: Folgende Parameter sind nicht online änderbar:</p> <ul style="list-style-type: none"> ▪ <i>System-ID</i> ▪ <i>Autostart</i> ▪ <i>Globales Forcen erlaubt</i> ▪ <i>Globales MultiForcen erlaubt</i> ▪ <i>Globale Force-Timeout-Reaktion</i> ▪ <i>Laden erlaubt</i> ▪ <i>Reload erlaubt</i> ▪ <i>Start erlaubt</i> <p>Wenn <i>Reload erlaubt</i> = TRUE ist, sind folgende Parameter online änderbar:</p> <ul style="list-style-type: none"> ▪ <i>Watchdog-Zeit (der Ressource)</i> ▪ <i>Sicherheitszeit</i> ▪ <i>Sollzykluszeit</i> ▪ <i>Sollzykluszeit-Modus</i> 	
		Bei gestoppter Steuerung und durch einen Reload ist es möglich, <i>Online-Einstellungen erlauben</i> = TRUE zu setzen.	

Systemparameter	S ¹⁾	Beschreibung		Einstellung für sicheren Betrieb
Autostart	J	TRUE:	Wenn die Steuerung an die Versorgungsspannung angeschlossen wird, starten die Anwenderprogramme automatisch. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Kein automatischer Start nach Zuschalten der Versorgungsspannung.	
		Einstellungen in den Programm-Eigenschaften der Ressource beachten!		
Start erlaubt	J	TRUE:	Kaltstart oder Warmstart durch PADT im Zustand RUN oder STOPP erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Kein Start erlaubt.	
Laden erlaubt	J	TRUE:	Download der Konfiguration erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Kein Start erlaubt.	
Reload erlaubt	J	TRUE:	Reload der Konfiguration erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Reload der Konfiguration nicht erlaubt. Ein laufender Reload-Prozess wird beim Umschalten auf FALSE nicht abgebrochen.	
Globales Forcen erlaubt	J	TRUE:	Globales Forcen für diese Ressource erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Globales Forcen für diese Ressource nicht erlaubt.	
Globale Force-Timeout-Reaktion	N	Legt fest, wie sich die Ressource beim Ablauf des globalen Force-Timeout verhält: <ul style="list-style-type: none">Nur Forcen beenden.Forcen beenden und Ressource stoppen. Standardwert: Nur Forcen beenden.		Applikations-spezifisch
Globales MultiForcen erlaubt	J	TRUE:	Anwender mit MultiForcen-Zugriff können in einer Ressource Force-Daten (Force-Werte und Force-Einzelschalter) für globale Variablen schreiben, wenn die dafür erforderlichen, übergeordneten Bedingungen gegeben und Force-Freigaben erfolgt sind.	Applikations-spezifisch
		FALSE:	Anwender mit MultiForcen-Zugriff können keine globale Variablen forcen. Standardwert: FALSE (online änderbar).	
Minimale Konfigurations-version	N	Mit dieser Einstellung ist es möglich, Code zu generieren, der entsprechend den Projektanforderungen zu alten oder zu neuen Versionen des HIMax Betriebssystems kompatibel ist. Als Standardwert wird die installierte SILworX Version angezeigt.		Applikations-spezifisch
Schneller Hochlauf	N	Für HIMax nicht anwendbar.		---

¹⁾ Systemparameter wird vom Betriebssystem sicherheitsbezogen behandelt, ja (J) oder nein (N).

Tabelle 11: Die Systemparameter der Ressource

10.4.1.1 Verwendung der Parameter *Sollzykluszeit* und *Sollzykluszeit-Modus*

Mit den Einstellungen im Systemparameter *Sollzykluszeit-Modus* kann die Zykluszeit möglichst konstant auf dem Wert der *Sollzykluszeit [ms]* gehalten werden. Dazu muss der Systemparameter auf einen Wert > 0 eingestellt sein.

HIMax begrenzt dabei den Reload und die Synchronisierung redundanter Prozessormodule soweit, dass die *Sollzykluszeit* eingehalten wird.

Die folgende Tabelle beschreibt die Einstellungen im Systemparameter *Sollzykluszeit-Modus*:

Einstellung	Beschreibung
fest	<p>Ist ein CPU-Zyklus kürzer als die definierte <i>Sollzykluszeit</i>, wird der CPU-Zyklus bis zur <i>Sollzykluszeit</i> verlängert.</p> <p>Ist der CPU-Zyklus länger als die <i>Sollzykluszeit</i>, setzt die CPU den Zyklus ohne Verzögerung fort.</p> <hr/> <p>i Ein Reload oder eine Aufsynchroisation wird abgelehnt, wenn die Reservezeit (<i>Sollzykluszeit</i> minus tatsächliche Zykluszeit) nicht ausreicht.</p>
fest-tolerant	<p>Wie <i>fest</i>, jedoch mit den folgenden Unterschieden:</p> <ol style="list-style-type: none"> 1. Wenn erforderlich wird bei der Aufsynchroisation die <i>Sollzykluszeit</i> für einen CPU-Zyklus nicht eingehalten, um die Aufsynchroisation erfolgreich durchführen zu können. 2. Wenn erforderlich wird beim Reload die <i>Sollzykluszeit</i> für 1 bis n (n = Anzahl der geänderten Anwenderprogramme) CPU-Zyklen nicht eingehalten, um den Reload erfolgreich durchführen zu können. <p>Die Standardeinstellung ist <i>fest-tolerant</i>!</p> <hr/> <p>i Nach dem 1. Reload-Aktivierungszyklus gelten Watchdog-Zeit, <i>Sollzykluszeit</i> und <i>Sollzykluszeit-Modus</i> gemäß der neuen Konfiguration. Höchstens jeder fünfte Zyklus kann während des Reload verlängert werden. Ein einziger Zyklus kann während der Synchronisation verlängert werden.</p>
dynamisch	<p>Die CPU führt jeden CPU-Zyklus so schnell wie möglich aus. Dies entspricht einer eingestellten <i>Sollzykluszeit</i> von 0 ms.</p> <hr/> <p>i Ein Reload oder eine Aufsynchroisation wird abgelehnt, wenn die Reservezeit (<i>Sollzykluszeit</i> minus tatsächliche Zykluszeit) nicht ausreicht. Höchstens jeder fünfte Zyklus kann während des Reload verlängert werden. Ein einziger Zyklus kann während der Synchronisation verlängert werden.</p>
dynamisch-tolerant	<p>Wie <i>dynamisch</i>, jedoch mit den folgenden Unterschieden:</p> <ol style="list-style-type: none"> 1. Wenn erforderlich wird bei der Aufsynchroisation die <i>Sollzykluszeit</i> für einen CPU-Zyklus automatisch erhöht, um die Aufsynchroisation erfolgreich durchführen zu können. 2. Wenn erforderlich wird beim Reload die <i>Sollzykluszeit</i> für 1 bis n (n = Anzahl der geänderten Anwenderprogramme) CPU-Zyklen automatisch erhöht, um den Reload erfolgreich durchführen zu können. <hr/> <p>i Nach dem 1. Reload-Aktivierungszyklus gelten Watchdog-Zeit, <i>Sollzykluszeit</i> und <i>Sollzykluszeit-Modus</i> gemäß der neuen Konfiguration. Ein Reload oder eine Aufsynchroisation wird abgelehnt, wenn die Reservezeit (<i>Sollzykluszeit</i> minus tatsächliche Zykluszeit) nicht ausreicht.</p>

Tabelle 12: Einstellungen *Sollzykluszeit-Modus*

10.4.1.2 Maximale Kommunikationszeitscheibe

Die maximale Kommunikationszeitscheibe ist die zugeteilte Zeit in Millisekunden (ms) pro CPU-Zyklus, innerhalb welcher das Prozessormodul die Kommunikationsaufgaben abarbeitet.

Können nicht alle in einem CPU-Zyklus anstehenden Kommunikationsaufgaben ausgeführt werden, erfolgt die komplette Übertragung der Kommunikationsdaten über mehrere CPU-Zyklen (Anzahl der Kommunikationszeitscheiben > 1). Die sicherheitsrelevanten Überwachungen für alle Protokolle werden jedoch immer in jedem CPU-Zyklus durchgeführt.

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

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

10.4.1.3 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 Kommunikationsmodul (X-COM) 3 ms.
- Pro redundante safe**ethernet** Verbindung 1 ms.
- Pro nicht redundante safe**ethernet** 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 HIMax System unter voller Last betreiben (FAT, SAT):
Alle Kommunikationsprotokolle sind in Betrieb (safe**ethernet** und Standardprotokolle).
2. Das **Control Panel** öffnen und im Strukturbaum das Verzeichnis **Kom.-Zeitscheibe** wählen.
3. Anzeige *Maximale Kom.-Zeitscheibe Dauer pro Zyklus [ms]* auslesen.
4. Anzeige *Maximale Anzahl benötigter Kom.-Zeitscheibe Zyklen* auslesen.

10.4.1.4 Berechnung der *Max. Dauer Konfigurationsverbindungen [ms]* t_{Konfig}

Der Systemparameter *Max. Dauer Konfigurationsverbindungen [ms]* entspricht dem erforderlichen Zeitbudget t_{Konfig} für die systeminternen Kommunikationsverbindungen (Tasks):

- PADT Online Verbindungen (z. B. Download/Reload, BS-Update, Online-Test, Diagnose).
- Remote I/O Status-Verbindungen (Start, Stopp und Diagnose).
- Konfiguration von Modulen (z. B. Laden ausgetauschter Module).

Können diese Tasks nicht in einem CPU-Zyklus abgeschlossen werden, werden die verbleibenden Tasks im nächsten CPU-Zyklus abgearbeitet. Dadurch können unerwartete Verzögerungen für diese Tasks entstehen.

i

HIMA empfiehlt t_{Konfig} so zu dimensionieren, dass alle Tasks in einem CPU-Zyklus abgearbeitet werden können.

Für die Betriebssysteme HIMax CPU \leq V3 wird t_{Konfig} von SILworX mit 6 ms vorgegeben. Jedoch darf die Verarbeitungsdauer der genannten Tasks in einem CPU-Zyklus die Vorgabe überschreiten.

Für die Betriebssysteme HIMax CPU \geq V4 wird t_{Konfig} wie folgt berechnet:

X-CPU 01: $t_{\text{Konfig}} = (n_{\text{Com}} + n_{\text{PADT}} + n_{\text{RIO}}) \cdot 0,25 \text{ ms} + 4 \text{ ms} + 4 \cdot (t_{\text{Latenz}} \cdot 2 + 0,31 \text{ ms})$

X-CPU 31: $t_{\text{Konfig}} = (n_{\text{Com}} + n_{\text{PADT}}) \cdot 1 \text{ ms} + n_{\text{RIO}} \cdot 0,25 \text{ ms} + 4 \text{ ms} + 4 \cdot (t_{\text{Latenz}} \cdot 2 + 0,8 \text{ ms})$

t_{Konfig} :	Systemparameter <i>Max. Dauer Konfigurationsverbindungen [ms]</i>
n_{COM} :	Anzahl Module mit Ethernet-Schnittstellen (X-SB, X-CPU, X-COM)
n_{PADT} :	5, maximale Anzahl PADT-Verbindungen
n_{RIO} :	Anzahl konfigurierter Remote I/Os
t_{Latenz} :	Aktive <i>maximale Systembus-Latenzzeit einsetzen, siehe nachfolgende Beschreibungen.</i> Wenn der Wert der maximalen Systembus-Latenzzeit in μs angegeben ist, dann muss dieser vor der Berechnung durch 1000 dividiert werden, um den Wert in ms zu erhalten.

Je nachdem welche Systembusstruktur für das HIMax System gewählt wurde, muss für die Systembus-Latenzzeit folgender Wert eingesetzt werden:

Netzwerkstruktur:	Wenn für den Parameter Maximale Systembus-Latenzzeit [μs] ein Wert von 100 ... 50 000 μs manuell eingetragen wurde, dann ist dieser Wert als t_{Latenz} in die Formel einzusetzen.
Linierstruktur:	Wenn der Parameter <i>Maximale Systembus-Latenzzeit [μs]</i> auf <i>System-Standardwerte</i> eingestellt ist, dann ist der entsprechende Standardwert der maximalen Systembus-Latenzzeit für t_{Latenz} aus der nachfolgenden Tabelle zu entnehmen und in die Formel einzusetzen. Alternativ zu dem Wert der Tabelle kann zunächst der mögliche Maximalwert eingesetzt werden für X-CPU 01 = 550,4 μs und für X-CPU 31 = 1166,4 μs .

Bei der Codegenerierung und bei der Projektkonvertierung wird im Logbuch des PADTs ein Hinweis ausgegeben, wenn t_{Konfig} kleiner ist, als nach obiger Formel errechnet.

i

Wenn t_{Konfig} zu klein eingestellt wurde, kann sich die Performance von PADT Online Verbindungen (Tasks) extrem verschlechtern und die Verbindung zu Remote I/Os abgebrochen werden.

HIMA empfiehlt den berechneten Wert t_{Konfig} mit dem im Control Panel angezeigten Wert zu vergleichen und gegebenenfalls in den Eigenschaften der Ressource zu korrigieren. Dies kann z. B. in einem SAT (Site Acceptance Test) durchgeführt werden.

Zu Testzwecken kann t_{Konfig} im Control Panel auch online eingestellt werden.

Der eingestellte Wert von t_{Konfig} muss für die Dimensionierung der erforderlichen Watchdog-Zeit berücksichtigt werden, siehe Kapitel *Sicherheitsrelevante Zeiten*.

Maximaler Rack-Abstand	Maximale Systembus-Latenzzeit in μs				Beispiele: System ist aufgebaut aus den genannten Racks
	X-CPU 01		X-CPU 31		
	Min	Max ¹⁾	Min	Max ¹⁾	
0	49,1	-	665,2	-	Nur Rack 0
1	105,5	155,5	721,6	771,6	Racks 0 und 1
2	161,9	211,9	778,0	828,0	Racks 0, 1, 3
3	218,4	268,4	834,4	884,4	Racks 0, 1, 3, 5
4	274,8	324,8	890,8	940,8	Racks 0, 1, 3,5, 7
5	331,2	381,2	947,2	997,2	Racks 0, 1, 3, 5, 7, 9
6	387,6	437,6	1003,6	1053,6	Racks 0, 1, 3, 5, 7, 9, 11
7	444,0	494,0	1060,9	1110,9	Racks 0, 1, 3, 5 ,7, 9, 11, 13,
8	500,4	550,4	1116,4	1166,4	Racks 1, 0, 2, 4, 6, 8, 10, 12, 14
1) Maximale Systembus-Latenzzeit einschließlich maximaler zusätzlicher Verzögerung durch die Netzwerk-Infrastruktur					

Tabelle 13: Standardwerte der maximalen Systembus-Latenzzeit

10.4.1.5 Parameter *Minimale Konfigurationsversion*

- Bei einem neu angelegten Projekt wird immer die höchste *Minimale Konfigurationsversion* ausgewählt. Prüfen Sie, ob diese Einstellung zur verwendeten Betriebssystem-Version passt!
- Bei einem älteren Projekt, das in die aktuelle SILworX Version konvertiert wurde, bleibt die ursprüngliche *Minimale Konfigurationsversion* erhalten. Dadurch ändert sich bei der Codegenerierung der Konfigurations-CRC gegenüber der Vorversion nicht, und die Konfiguration bleibt kompatibel zu den Betriebssystemen der Module.

Bei konvertierten Projekten muss die *Minimale Konfigurationsversion* nur dann erhöht werden, wenn Sie zusätzliche Funktionen einer Steuerung nutzen möchten.

- SILworX erzeugt automatisch eine höhere als die eingestellte *Minimale Konfigurationsversion*, wenn im Projekt Fähigkeiten benutzt werden, die eine höhere Konfigurationsversion erfordern. Dies zeigt SILworX im Logbuch der Codegenerierung an. Module lehnen das Laden von Konfigurationen ab, wenn die Konfigurationsversion nicht zu ihren Betriebssystemen passt.

Mit dem sicheren Versionsvergleich von SILworX werden Änderungen an einem Projekt gegenüber einer vorherigen Projektversion ermittelt und nachgewiesen.

10.4.1.6 Systemvariable des Racks

Diese Systemvariablen dienen dazu, das Verhalten der Steuerung im laufenden Betrieb bei bestimmten Zuständen zu verändern. Diese Variablen sind einstellbar im Hardware-Editor von SILworX, in der Detailansicht der Racks, Register *System*.

Systemvariable	S ¹⁾	Funktion	Einstellung für sicheren Betrieb
Force-Deaktivierung	J	Verhindert das Starten des Forcen-Vorgangs und beendet einen laufenden Force-Vorgang. Die Standardeinstellung ist FALSE.	Applikations-spezifisch
Leer 0 ... Leer 16	J	Keine Funktion!	---
MultiForcen gesperrt	J	MultiForcen kann per Systemvariable MultiForcen gesperrt aktiviert und deaktiviert werden, so dass die damit verbundenen Funktionen vom Anwenderprogramm gesteuert werden können. Für globales MultiForcen muss die Systemvariable FALSE sein. Die Standardeinstellung ist FALSE.	Applikations-spezifisch
Notaus 1 ... Notaus 4	J	Schaltet die Steuerung in vom Anwenderprogramm erkannten Störfällen ab. Die Standardeinstellung ist FALSE.	Applikations-spezifisch
Read-only in RUN	J	Nach dem Starten der Steuerung sind die Zugriffsrechte auf die Zugriffsart <i>Lesen</i> herabgestuft. Ausnahmen sind Forcen und Reload. Die Standardeinstellung ist FALSE.	Applikations-spezifisch
Reload-Deaktivierung	J	Sperrt die Durchführung von Reload. Die Standardeinstellung ist FALSE.	Applikations-spezifisch
¹⁾ Systemparameter wird vom Betriebssystem sicherheitsbezogen behandelt, ja (J) oder nein (N).			

Tabelle 14: Systemvariable der Hardware

Diesen Systemvariablen lassen sich globale Variable zuweisen, deren Wert durch einen physikalischen Eingang oder die Logik des Anwenderprogramms verändert wird.

10.4.2 Abschließen und Aufschließen der Steuerung

Abschließen der Steuerung bedeutet das Verriegeln von Eingriffsmöglichkeiten des Anwenders während des Betriebs. Eine unbefugte Manipulation des Anwenderprogramms wird damit verhindert.

Aufschließen der Steuerung bedeutet das Entfernen der aktiven Verriegelung, zum Beispiel zur Durchführung von Maßnahmen an der Steuerung.

Zum Verriegeln dienen die Systemvariablen *Read-only in RUN*, *Reload-Deaktivierung*, *Force-Deaktivierung* und *MultiForcen gesperrt*.

Wenn alle der oben genannten Systemvariablen TRUE sind, dann ist kein Zugriff auf die Steuerung mehr möglich. In diesem Fall kann die Steuerung nur durch Neustart aller Prozessormodule mit dem Mode-Schalter in Stellung *Init* wieder in den Zustand STOP versetzt werden. Erst dann ist ein Neuladen eines Anwenderprogramms möglich. Das Beispiel beschreibt den einfachen Fall, dass mit einem Schlüsselschalter alle Eingriffe in die Ressource gesperrt oder zugelassen werden.

Beispiel: Steuerung abschließbar machen

1. Globale Variablen vom Typ BOOL definieren, Initialwerte auf FALSE setzen.
 2. Globale Variablen den oben genannten Systemvariablen als Ausgangsvariable zuweisen.
 3. Globale Variable dem Kanalwert eines digitalen Eingangs zuweisen.
 4. Schlüsselschalter an den digitalen Eingang anschließen.
 5. Programm kompilieren, auf die Steuerung laden und starten.
- Der Besitzer eines passenden Schlüsselschalters kann die Steuerung ab- und aufschließen. Bei einem Fehler im entsprechenden digitalen Eingangsmodul wird die Steuerung automatisch aufgeschlossen.

Dieses einfache Beispiel lässt sich durch die Verwendung von mehreren globalen Variablen, digitalen Eingängen und Schlüsselschaltern abwandeln. Die Berechtigungen für Forcen, Reload, MultiForcen und weiteren Bedienfunktionen können auf unterschiedliche Schlüssel und Personen verteilt werden.

10.5 Forcen

Unter Forcen versteht man das manuelle Beschreiben von Variablen mit Werten, die sich nicht aus dem Prozess ergeben, sondern vom Anwender vorgegeben werden, während die Steuerung das Anwenderprogramm abarbeitet.

In einem System existieren verschiedene Arten von global force-baren Datenquellen:

- Alle Eingangs und Statusinformationen von Modulen (z. B. E/A-Module) und Kommunikationsprotokollen.
- Alle nicht beschriebenen, aber gelesenen globalen Variablen (VAR_EXTERNAL).
- Alle von einem Anwenderprogramm beschriebenen globalen Variablen (VAR_EXTERNAL).

Neben den global force-baren Datenquellen existieren in einem System auch verschiedene Arten von lokal (im Anwenderprogramm) force-baren Datenquellen:

- Alle nicht beschriebenen, aber gelesenen Anwenderprogramm-Variablen (VAR).
- Alle von einem Anwenderprogramm beschriebenen Variablen (VAR).

i

Beim Forcen einer Variable wird immer ihre Datenquelle geforct! Eine geforcte Variable ist vom Prozess unabhängig, da der Wert vom Anwender vorgegeben wird.

10.5.1 Verwendung von Forcen

Forcen unterstützt den Anwender bei folgenden Aufgaben, z. B.:

- Zum Testen des Anwenderprogramms für Fälle, die im Normalbetrieb nicht oder nur selten eintreten und somit nur bedingt prüfbar sind.
- Zur Simulation von Sensorwerten, z. B. nicht verbundener Sensoren.
- Zu Service- und Reparaturarbeiten.
- Zur allgemeinen Fehlersuche.

WARNUNG



Personenschäden durch geforcte Werte möglich!

- **Werte nur nach Absprache mit dem Anlagenverantwortlichen und bei Inbetriebnahme mit der Prüfstelle forcen.**
- **Einschränkungen des Forcens nur nach Absprache mit Anlagenverantwortlichen und bei Inbetriebnahme mit der Prüfstelle aufheben.**

Während des Forcens muss der Verantwortliche die sicherheitstechnisch ausreichende Überwachung des Prozesses durch andere technische und organisatorische Maßnahmen gewährleisten. Es wird empfohlen, das Forcen zeitlich zu begrenzen, siehe Kapitel 10.5.3.

WARNUNG



Störung des sicherheitsbezogenen Betriebs durch geforcte Werte möglich!

- **Geforcte Werte können zu unerwarteten Ausgangswerten führen.**
- **Forcen verlängert die Zykluszeit. Dadurch kann die Watchdog-Zeit überschritten werden.**

Forcen kann in zwei Geltungsbereichen erfolgen:

- Globales Forcen: Globale Variable werden für alle Verwendungen geforct.
- Lokales Forcen: Lokalen Variablen werden innerhalb eines Anwenderprogramms geforct.

10.5.2 Per Reload geänderte Zuweisung einer Datenquelle

Das Ändern von Zuweisungen von Variablen zu einer anderen Datenquelle per Reload kann bei folgenden Eingängen zu einem unerwarteten Ergebnis führen:

- Hardware.
- Kommunikationsprotokolle.
- Systemvariablen.

Folgende per Reload durchgeführte Änderungen führen zu geänderten Force-Zuständen:

1. Eine globale Variable A ist einer geforcten Datenquelle zugewiesen und ist damit geforct.
2. Die Zuweisung der globalen Variable A wird per Reload entfernt. Die Datenquelle behält die Eigenschaft *geforct*. Die globale Variable A ist jetzt nicht mehr geforct.
3. Die geforcte Datenquelle wird einer anderen globalen Variable B zugeordnet.
4. Beim nächsten Reload ist dann die globale Variable B geforct, obwohl dies nicht beabsichtigt war.

Konsequenz

Um dies zu vermeiden, beenden Sie zuerst das Forcen einer Variable, bevor die Datenquelle geändert wird. Dazu den Force-Einzelschalter deaktivieren.

Welche Kanäle geforct sind, ist im Register *Eingänge* des Force-Editors erkennbar.



Globale Variablen, deren Datenquelle das Anwenderprogramm ist, behalten die Eigenschaft *geforcet* auch dann bei, wenn die Zuweisung geändert wird.

10.5.3 Zeitbegrenzung

Für das globale wie für das lokale Forcen sind unterschiedliche Zeitbegrenzungen einstellbar. Nach Ablauf der eingestellten Zeit beendet die Steuerung das Forcen.

Das Verhalten des HlMax Systems nach dem Ablauf der Zeitbegrenzung ist einstellbar:

- Beim globalen Forcen sind folgende Einstellungen wählbar:
 - *Ressource stoppen*.
 - *Nur Forcen beenden*, d. h. die Ressource läuft weiter.
- Beim lokalen Forcen sind folgende Einstellungen wählbar:
 - *Programm stoppen*.
 - *Nur Forcen beenden*, d. h. das Anwenderprogramm läuft weiter.

Forcen ist auch ohne Zeitbegrenzung möglich. In diesem Fall ist das Forcen manuell zu beenden.

Der für das Forcen Verantwortliche muss klären, welche Auswirkungen das Beenden des Forcens auf die Gesamtanlage hat!

10.5.4 Einschränkung des Forcens

Der Anwender hat die Möglichkeit die Benutzung des Forcens einzuschränken, eventuelle Störungen des Betriebs durch das Forcen sind zu vermeiden. In der Konfiguration können folgende Maßnahmen dafür getroffen werden:

- Die Einrichtung unterschiedlicher Benutzerkonten mit und ohne Force-Rechten.
- Das Forcen für eine Ressource (PES) explizit erlauben.
- Die Einrichtung von MultiForce-Benutzerkonten in der PES-Benutzerverwaltung.
- Das lokale Forcen für ein Anwenderprogramm explizit erlauben.
- Die Wirkung des Forcens kann über die Systemvariable *Force-Deaktivierung* per Schlüsselschalter unmittelbar abgeschaltet werden.
- Zusätzlich kann über die Systemvariable *MultiForcen gesperrt* MultiForcen unterbunden werden.

10.5.5 MultiForcen

Anwender mit MultiForcen-Zugriff können in einer Ressource Force-Daten (Force-Werte und Force-Einzelschalter) für globale Variablen schreiben, wenn die dafür erforderlichen, übergeordneten Bedingungen gegeben und Force-Freigaben erfolgt sind. Auf alle anderen Funktionen einer Ressource kann der Anwender nur lesend zugreifen. Das Starten, Stoppen oder Zurücksetzen eines Force-Vorgangs ist nicht möglich.

Das MultiForcen ist auf bis zu 5 Benutzer gleichzeitig begrenzt. Die Benutzer können räumlich voneinander entfernt sein und auch zeitlich unabhängig voneinander arbeiten. Die Abgrenzung der Aufgaben der einzelnen Benutzer ist durch organisatorische Maßnahmen des Betreibers sicherzustellen.

⚠ WARNUNG

Nicht steuerbares Verhalten durch den Anwender möglich!

Der Betreiber muss dafür sorgen, dass verschiedene Force-User nicht gleichzeitig dieselben Variablen forcen und es nicht zu zeitlichen Überschneidungen kommt. Schreiben mehrere Force-User auf dieselben Variablen, setzen sich diejenigen Force-Werte und Force-Einzelschalter durch, die von der Firmware zuletzt geschrieben wurden. Da Force-Daten in mehreren Blöcken übertragen werden, können auf einer einzelnen Steuerung anderenfalls auch Einstellungen unterschiedlicher Force-User wirksam werden. Dieses Verhalten ist für den Anwender nicht steuerbar!

⚠ WARNUNG

***MultiForcen gesperrt* = TRUE, bestehende Force-Daten werden nicht deaktiviert!**

Wenn *MultiForcen gesperrt* = TRUE ist, können Anwender mit MultiForcen-Zugriff keine Veränderungen an den Force-Werten und den Force-Einzelschaltern vornehmen. Bestehende Force-Daten werden nicht deaktiviert, wenn *MultiForcen gesperrt* = TRUE ist! Globales Forcen ist, wenn erlaubt, dann nur für einen einzigen Benutzer mit mindestens Bedienerrechten möglich.

Weitere Informationen zum Forcen finden Sie im Systemhandbuch HI 801 000 D und in der SILworX Online-Hilfe.

10.5.5.1 Ziele von MultiForcen

Für die Inbetriebnahme sind im Rahmen der Site Acceptance Tests normativ und funktional Loop-Tests vorgeschrieben, wobei ein Loop den Weg vom Sensor zum Aktor darstellt. MultiForcen ermöglicht es, die anfallenden Aufgaben auf bis zu 5 PADTs zu verteilen und damit effizient abzuarbeiten.

Anhand von Loop-Tests wird der nominale Betriebsbereich geprüft, ebenso wie die Reaktionen bei Leitungsbruch und Leitungsschluss. Da häufig zahlreiche Loops getestet werden müssen, ist die Dauer von Site Acceptance Tests ein wesentlicher Kostenfaktor. MultiForcen kann helfen, diese Aufgaben zu optimieren.

- Das Verhalten von Aktoren und verknüpften Informationen (z. B. Endlagenrückmeldung) wird durch Forcen getestet. Die Ausgangssignale werden direkt geforct. Dadurch wird die Verdrahtung und externe Schaltung geprüft.
- In einer Anlage, die sich im Teilbetrieb befindet, werden Sensoren durch Forcen so getestet, dass die Tests keine Auswirkung auf die Aktoren haben. Diese Variante kann auch bei der Fehlersuche im Zusammenhang mit Sensoren zur Anwendung kommen.

10.5.5.2 Globales MultiForcen

Globales MultiForcen ist das gleichzeitige Schreiben von Force-Daten (Force-Werte und Force-Einzelschalter) für globale Variablen durch mehr als einen Benutzer (Force-User).

Ein Force-User ist eine Person, die entweder mit MultiForcen-Rechten, Bedienerrechten, Schreibrechten oder mit Administratorrechten in einer Steuerung eingeloggt ist. Jeder Force-User kann neben dem Lesen von Daten mindestens auch Force-Daten schreiben. Pro Steuerung können maximal 5 Force-User eingeloggt sein. Die Anzahl der aktuellen Force-User wird in der SILworX -Statuszeile angezeigt.

Um die durch Force-User mit MultiForcen-Zugriff eingestellten Force-Werte und Force-Einzelschalter wirksam werden zu lassen ist ein Anwender erforderlich, der mit mindestens Bedienerrechten in der Steuerung eingeloggt ist. Nur dieser Anwender kann Forcen starten und stoppen.



Um globales MultiForcen durchführen zu können, muss auch globales Forcen erlaubt sein! Die Einstellungen werden online angezeigt.

10.6 Sicherer Versionsvergleich

Bei der Codegenerierung werden durch SILworX verschiedene Dateien erzeugt. Dieser Datensatz wird als die Ressource-Konfiguration bezeichnet. Beim Download oder Reload wird immer die komplette Ressource-Konfiguration in die Ressource geladen.

Beim sicheren Versionsvergleich werden verschiedene Ressource-Konfigurationen miteinander verglichen und die Unterschiede zwischen den einzelnen Dateien angezeigt.

Im Wesentlichen gibt es drei Typen von Ressource-Konfigurationen:

1. Die erzeugte Ressource-Konfiguration ist das Ergebnis der letzten Codegenerierung.
2. Die geladene Ressource-Konfiguration ist die durch einen Download oder Reload in die Steuerung geladene Ressource-Konfiguration.
3. Eine unbekannte Ressource-Konfiguration, die exportiert und gesichert wurde. Diese stellt einen beliebigen Stand einer Ressource-Konfiguration dar.

Zur Prüfung von Programmänderungen ist der sichere Versionsvergleich **vor** dem Laden in die Steuerung einzusetzen.

Der Versionsvergleich bestimmt genau die geänderten Teile der Ressource-Konfiguration. Dies erleichtert die Prüfung und die Eingrenzung der zu testenden Änderungen. Das Ergebnis hat SIL 3-Qualität und dient als Nachweis gegenüber Prüfstellen.

Strukturierte Programmierung und eine Verwendung von aussagekräftigen Namen, von der ersten Ressource-Konfiguration an, helfen beim Verstehen des Vergleichsergebnisses.

Weitere Informationen zum sicheren Versionsvergleich finden Sie im Handbuch Versionsvergleich HI 801 285 D.

10.7 Application Programming Interface (API) Sicherheitsmaßnahmen

Das SILworX Application Programming Interface (SILworX API) unterstützt folgende Sicherheitsmaßnahmen:

- Die Benutzung der SILworX API erfordert eine Lizenz.
- Die SILworX API muss explizit in der *settings.ini* aktiviert werden.
- Zugriffe auf die SILworX API sind ausschließlich über SSL (TLS 1.2) möglich. Hierzu ist die Installation von OpenSSL und ein gültiges Zertifikat nötig.
- Zugriffe über die SILworX API auf Projekte benötigen die gleichen Benutzerrechte wie beim manuellen Arbeiten.
- Konfigurierbare Timeouts bei der Benutzung der SILworX API-Zugriffe sorgen dafür, dass Projekte automatisch geschlossen werden, wenn bis zum Timeout keine weitere API-Anfragen gesendet werden.
- SILworX API-Aktivitäten werden in der Statusleiste angezeigt.
- Alle Aktionen werden im SILworX Logbuch protokolliert. Dies gilt sowohl für das manuelle Arbeiten, als auch für API-Zugriffe.

i

Wichtig:

Der Anwender muss für seine SILworX API-Anwendung eine Tool-Klassifikation durchführen und entsprechend qualifizieren.

Im Unterordner ...\\c3\\openapi des SILworX Installationsverzeichnis befindet sich die API-Dokumentation in HTLM-Format und ein C# Anwendungsbeispiel.

11 Sicherheitstechnische Aspekte für Anwenderprogramme

In diesem Kapitel werden sicherheitstechnische Aspekte für Anwenderprogramme behandelt.

Ziele bei der Programmierung eines Anwenderprogramms:

- Verständlich.
- Nachvollziehbar.
- Testbar.
- Leicht zu ändern.

11.1 Sicherheitsbezogener Einsatz

Die Anwenderprogramme müssen mit dem Programmierwerkzeug SILworX erstellt werden.

SILworX kann nur auf einem Personal Computer mit Microsoft Windows Betriebssystem installiert werden. Die Mindestanforderungen an den Rechner für den Betrieb von SILworX sind auf der jeweiligen Installations-DVD angegeben.

Das Programmierwerkzeug SILworX enthält im Wesentlichen:

- Globaler Variablen Editor (Anlegen von globalen Variablen mit symbolischen Namen und Datentyp).
- Hardware-Editor (Zuordnung der Steuerungen des Systems HlMax).
- Programm-Editor (Zur Erstellung des Anwenderprogramms).
- Codegenerator (Übersetzen des Anwenderprogramms in den Maschinencode).
- Konfiguration der Kommunikation.
- Überwachung und Dokumentation.

Die in diesem Handbuch beschriebenen Sicherheitsauflagen müssen beachtet werden, siehe Kapitel 3.4!

11.1.1 Basis der Programmierung

Die Steuerungsaufgabe muss in Form einer Spezifikation oder eines Pflichtenheftes vorliegen. Diese Dokumentation ist die Basis zur Überprüfung der korrekten Umsetzung in das Anwenderprogramm.

Die Dokumentation richtet sich nach der Steuerungsaufgabe und kann auf zwei Arten dargestellt werden.

Kombinatorische Logik:

- Ursache/Wirkungs-Schema (cause/effect diagram).
- Logik der Verknüpfung mit Funktionen und Funktionsbausteinen.
- Funktionsblöcke mit spezifizierten Eigenschaften.

Sequentielle Steuerungen (Ablauf-Steuerungen):

- Verbale Beschreibung der Schritte mit Fortschalt-Bedingungen und der zu steuernden Aktoren.
- Ablaufpläne.
- Matrix- oder Tabellenform der Fortschalt-Bedingungen und der zu steuernden Aktoren.
- Definition der Randbedingungen, z. B. Betriebsarten, NOT-AUS.

11.1.1.1 E/A-Konzept

Das E/A-Konzept der Anlage muss die Analyse der Feldkreise enthalten, d. h. die Art der Sensoren und Aktoren.

Digitale und analoge Sensoren:

- Signal im Normalbetrieb (Ruhestromprinzip bei digitalen Sensoren, life-zero bei analogen Sensoren).
- Signal im Fehlerfall.
- Festlegung von sicherheitstechnisch erforderlichen Redundanzen (1oo2, 2oo3).
- Diskrepanz-Überwachung und Reaktion.

Aktoren:

- Stellung und Ansteuerung im Normalbetrieb.
- Sichere Reaktion/Stellung bei Abschaltung oder Energieausfall.

11.1.2 Schritte der Programmierung

Die Programmierung von HIMax Systemen für sicherheitstechnische Anwendungen ist in folgenden Schritten durchzuführen:

1. Steuerungsfunktionen spezifizieren.
2. Anwenderprogramme schreiben.
3. Anwenderprogramme mit dem C-Code-Generator kompilieren.
 - Die Anwenderprogramme sind fehlerfrei erzeugt und lauffähig.
4. Anwenderprogramme verifizieren und validieren (FAT, SAT).
5. Anwenderprogramme testen.

Danach sind die Anwenderprogramme bereit für den sicherheitsbezogenen Betrieb.

11.1.3 Funktionen der Anwenderprogramme

Die Funktionen der Anwenderprogramme sind frei programmierbar.

- Innerhalb der Logik werden ausschließlich Elemente nach IEC 61131-3 mit ihren jeweiligen Funktionsbedingungen verwendet.
- Die physikalischen Eingänge und Ausgänge arbeiten generell im Ruhestromprinzip, d. h. ihr sicherer Zustand ist „0“.
- Die Anwenderprogramme werden aus logischen und/oder arithmetischen Funktionen ohne Rücksicht auf das Ruhestromprinzip der physikalischen Eingänge und Ausgänge erstellt.
- Die Logik muss übersichtlich konzipiert und verständlich dokumentiert sein, um die Fehlersuche zu erleichtern. Das schließt die Verwendung von Funktionsdiagrammen ein.
- Zur Vereinfachung der Logik können die Eingänge und Ausgänge aller Funktionsbausteine und Variablen beliebig invertiert werden.
- Fehlersignale von Eingängen und Ausgängen oder aus Logik-Bausteinen müssen vom Programmierer ausgewertet werden.

Empfehlenswert ist die Kapselung von Funktionen in selbst erstellten Funktionsbausteinen und Funktionen, die aus Standardfunktionen aufgebaut sind. Dadurch können Anwenderprogramme in Modulen (Funktionen, Funktionsbausteine) klar strukturiert werden. Jedes Modul kann für sich einzeln betrachtet und getestet werden. Durch das Zusammenschalten der Module zu einem größeren Modul und zu einem Anwenderprogramm ergibt sich eine fertige, komplexe Funktion.

11.1.4 Systemparameter der Anwenderprogramme

Die folgenden Parameter von Anwenderprogrammen lassen sich im Dialogfenster *Eigenschaften* des Anwenderprogramms einstellen:

Systemparameter	S ¹⁾	Beschreibung	Einstellung für sicheren Betrieb
Name	N	Name des Anwenderprogramms. Der Name muss innerhalb der Ressource eindeutig sein.	Beliebig
Programm ID	J	ID für die Identifizierung des Programms bei der Anzeige in SILworX. Wertebereich: 0 ... 4 294 967 295 Standardwert: 0 Bei Einstellung von <i>Codegenerierung Kompatibilität</i> auf <i>SILworX V2</i> ist nur der Wert 1 zulässig.	Applikations-spezifisch
Priorität	J	Priorität des Anwenderprogramms. Wertebereich: 0 ... 31 Standardwert: 0 (maximale Priorität) Einstellung nur nötig bei Verwendung mehrerer APs!	Applikations-spezifisch
Maximale CPU-Zyklen Programm	J	Maximale Anzahl an CPU-Zyklen, die ein Zyklus des Anwenderprogramms dauern darf. Wertebereich: 1 ... 4 294 967 295 Standardwert: 1 Einstellung nur nötig bei Verwendung mehrerer APs!	Applikations-spezifisch
Max. Dauer pro Zyklus [µs]	N	Maximale Ausführungsdauer pro Zyklus des Prozessormoduls für ein Anwenderprogramm. Wertebereich: 0 ... 4 294 967 295 Standardwert: 0 (keine Begrenzung) Die sicherheitsbezogene Reaktion wird über den Watchdog gewährleistet. Einstellung nur nötig bei Verwendung mehrerer APs!	Applikations-spezifisch
Watchdog-Zeit [ms] (berechnet)	---	Überwachungszeit des Anwenderprogramms, berechnet aus dem Produkt der Watchdog-Zeit der Ressource und der parametrisierten maximaler Anzahl von CPU-Zyklen. Nicht änderbar!	
Klassifikation	N	Einstufung des Anwenderprogramms in <i>sicherheitsgerichtet</i> oder <i>standard</i> , dient nur zur Dokumentation und hat keinen Einfluss auf die Funktion des Programms. Die Standardeinstellung ist sicherheitsgerichtet	Applikations-spezifisch
Online-Einstellungen erlauben	J	Wenn <i>Online-Einstellungen erlauben</i> ausgeschaltet ist, können die Einstellungen der anderen Programmschalter nicht per Online-Zugriff (Control Panel) verändert werden. Wirkt nur, wenn <i>Online-Einstellungen erlauben</i> der Ressource TRUE ist! Standardwert: TRUE.	
Autostart	J	Freigegebene Art des Autostarts: Kaltstart, Warmstart, Aus. Die Standardeinstellung ist Warmstart.	Applikations-spezifisch
Start erlaubt	J	TRUE: Start des Anwenderprogramms durch das PADT erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE: Start des Anwenderprogramms durch das PADT nicht erlaubt.	

Systemparameter	S ¹⁾	Beschreibung		Einstellung für sicheren Betrieb
Testmodus erlaubt	J	TRUE:	Testmodus für das Anwenderprogramm ist erlaubt.	Applikations-spezifisch ²⁾
		FALSE:	Testmodus für das Anwenderprogramm ist nicht erlaubt. Standardwert: FALSE.	
Reload erlaubt	J	TRUE:	Reload des Anwenderprogramms ist erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Reload des Anwenderprogramms ist nicht erlaubt.	
		Einstellungen in den Ressource-Eigenschaften beachten!		
Lokales Forcen erlaubt	J	TRUE:	Forcen auf Programmebene erlaubt.	FALSE empfohlen
		FALSE:	Forcen auf Programmebene nicht erlaubt. Standardwert: FALSE.	
Lokale Force-Timeout-Reaktion	J	Verhalten des Anwenderprogramms nach Ablauf der Force-Zeit: <ul style="list-style-type: none">Nur Forcen beenden.Programm stoppen. Die Standardeinstellung ist <i>Nur Forcen beenden</i> .		
Codegenerierung Kompatibilität	-	Die Codegenerierung arbeitet kompatibel zu früheren Versionen von SILworX.		Applikations-spezifisch
		SILworX V2	Codegenerierung arbeitet kompatibel zu SILworX V2.	
		SILworX V3	Codegenerierung arbeitet kompatibel zu SILworX V3.	
		SILworX V4 – V6b	Codegenerierung arbeitet kompatibel zu SILworX V4 bis SILworX V6b.	
		ab SILworX V7	Codegenerierung arbeitet kompatibel zu SILworX V7.	
		Die Standardeinstellung ist bei allen neuen Projekten <i>ab SILworX V7</i> .		

1) Systemparameter wird vom Betriebssystem sicherheitsbezogen behandelt, ja (J) oder nein (N)

2) Nach Ende des Testbetriebs muss ein Kaltstart des Programms durchgeführt werden, bevor ein sicherheitsbezogener Betrieb aufgenommen wird!

Tabelle 15: Systemparameter des Anwenderprogramms

11.1.5 Hinweise zum Parameter *Codegenerierung Kompatibilität*

Für den Parameter *Codegenerierung Kompatibilität* folgende Punkte beachten:

- Bei einem neu angelegten Projekt wählt SILworX die aktuellste Einstellung für *Codegenerierung Kompatibilität* aus. Damit werden die aktuellen, optimierten Einstellungen aktiviert und die aktuellsten Versionen von Modulen und Betriebssystemen unterstützt. Prüfen Sie, ob diese Einstellung zur verwendeten Hardware passt!
- Bei einem älteren Projekt, das in die aktuelle SILworX Version konvertiert wurde, bleibt die ursprünglichen *Codegenerierung Kompatibilität* erhalten. Dadurch ändert sich bei der Codegenerierung der Konfigurations-CRC gegenüber der Vorversion nicht, und die Konfiguration bleibt kompatibel zu den Betriebssystemen der Module. Bei konvertierten Projekten muss die *Codegenerierung Kompatibilität* *nur dann geändert werden, wenn Sie zusätzliche Funktionen einer Steuerung nutzen möchten*.
- Wenn in der Eigenschaft der Ressource eine *Minimale Konfigurationsversion* von *SILworX V4* oder höher eingestellt ist, dann muss in jedem Anwenderprogramm der Parameter *Codegenerierung Kompatibilität* auf *ab SILworX V7* eingestellt werden.

11.1.6 Code-Erzeugung

Nach der Fertigstellung der Anwenderprogramme und der Konfiguration der Ressource erzeugt der Codegenerator einen Code mit einem typischen Konfigurations-CRC.

Der Konfigurations-CRC ist eine Signatur aller konfigurierten Elemente und wird als Hex-Code im 32-Bit-Format ausgegeben.

Für den sicherheitsbezogenen Betrieb muss das Anwenderprogramm zweimal kompiliert werden. Die beiden beim Kompilieren erzeugten Prüfsummen müssen identisch sein!

Durch das zweimalige Kompilieren mit Vergleich der Prüfsummen lassen sich mögliche Verfälschungen der Anwenderprogramme entdecken, die durch zufällige Fehler in der Hardware oder im Betriebssystem des verwendeten PC verursacht wurden.

Das Ergebnis des CRC-Vergleichs wird im Logbuch angezeigt.

11.1.7 Laden und Starten des Anwenderprogramms

Der Download einer Ressource-Konfiguration in eine Steuerung ist nur möglich, wenn die Steuerung in STOPP ist.

Nach dem erfolgreichen Download einer Ressource-Konfiguration können die Anwenderprogramme gestartet werden.

i

Das PADT kann die Steuerung nur dann bedienen, z. B. Reload und Forcen durchführen, wenn in SILworX das zur Ressource-Konfiguration passende Projekt geöffnet ist.

HIMA empfiehlt, nach jedem Download oder Reload das Projekt zu archivieren.

SILworX speichert alle Daten eines Projekts in einer einzigen Datei. HIMA empfiehlt aus Gründen der Datensicherheit das Projekt zusätzlich auf einem externen Medium zu speichern.

Das Backup gewährleistet, dass die zur Ressource-Konfiguration passenden Projektdaten weiterhin verfügbar sind, auch wenn das PADT ausfällt.

11.1.8 Reload

Wenn Änderungen an einem Projekt vorgenommen werden, dann können diese im laufenden Betrieb durch einen Reload auf die Steuerung übertragen werden. Nach Prüfungen durch das Betriebssystem wird dann das geänderte Projekt aktiviert und übernimmt die Steuerungsaufgabe.

Reload ist nur möglich, wenn der Systemparameter *Reload erlaubt* auf TRUE und die Systemvariable *Reload-Deaktivierung* auf FALSE eingestellt ist.

i

Reload ist nur nach Rücksprache mit der für die Anlagenabnahme zuständigen Prüfstelle zulässig. Während des gesamten Reload-Prozesses muss der für den Reload Verantwortliche die sicherheitstechnisch ausreichende Überwachung des Prozesses durch andere technische und organisatorische Maßnahmen sicherstellen.

i**Beim Reload von Schrittketten ist zu beachten:**

Die Reload-Information für Schrittketten berücksichtigt nicht den aktuellen Status der Kette. Daher ist es möglich, dass durch Reload die Schrittkette geändert und durch diese Änderung die Schrittkette in einen undefinierten Zustand versetzt wird. Die Verantwortung für den fehlerfreien Reload liegt beim Anwender.

Beispiele:

- Löschen eines aktiven Schritts hat zur Folge, dass alle Schritte der Schrittkette den Zustand *aktiv* verlieren.
 - Umbenennen eines Initialschritts, während ein anderer Schritt aktiv ist, führt zu einer Schrittkette mit zwei aktiven Schritten!
-

i**Beim Reload von Actions ist zu beachten:**

Reload lädt Actions mit ihren kompletten Daten. Die Konsequenzen daraus sind vor dem Reload sorgfältig zu überdenken.

Beispiele:

- Entfernen eines Timer-Bestimmungszeichens durch den Reload führt dazu, dass der Timer sofort abgelaufen ist. Dadurch kann der Ausgang *Q* in Abhängigkeit von der restlichen Belegung auf *TRUE* wechseln.
 - Entfernen eines Bestimmungszeichens bei haftenden Elementen (z. B. Bestimmungszeichen *S*), die gesetzt waren, führt dazu, dass die Elemente gesetzt bleiben.
 - Entfernen eines Bestimmungszeichens *P0*, das *TRUE* gesetzt war, löst den Trigger aus.
-

Vor der Ausführung eines Reload prüft das Betriebssystem, ob die notwendigen Zusatzaufgaben die Zykluszeit der laufenden Anwenderprogramme so stark erhöhen würden, dass die festgelegte Watchdog-Zeit überschritten würde. In diesem Fall wird der Reload mit einer Fehlermeldung abgebrochen und die Steuerung läuft mit der bisherigen Ressource-Konfiguration weiter.

i**Die Steuerung kann einen Reload abbrechen.**

Um Reload erfolgreich durchzuführen, ist bei der Festlegung der Watchdog-Zeit eine Reserve für den Reload einzuplanen oder die Watchdog-Zeit der Steuerung vorübergehend um eine Reserve zu erhöhen.

Die vorübergehende Erhöhung der Watchdog-Zeit ist mit der zuständigen Prüfstelle abzustimmen.

Eine Überschreitung der Sollzykluszeit kann ebenfalls zum Abbruch eines Reload führen.

i

Es liegt in der Verantwortung des Anwenders, bei der Bemessung der Watchdog-Zeit Reserven einzuplanen. Diese sollen die folgenden Situationen beherrschbar machen:

- Schwankungen bei der Zykluszeit des Anwenderprogramms.
 - Plötzliche, starke Belastungen des Zyklus, z. B. durch Kommunikation.
 - Ablauf von Zeitgrenzen bei der Kommunikation.
-

11.1.9 Online-Test

Es ist zulässig, in der Logik des Anwenderprogramms Online-Test-Felder (OLT-Felder) zur Anzeige von Variablen während des Betriebs der Steuerung zu verwenden.

Weitere Informationen zur Verwendung von OLT-Feldern finden Sie unter dem Stichwort OLT-Feld in der Online-Hilfe von SILworX und im Erste-Schritte-Handbuch HI 801 102 D.

11.1.10 Testmodus

Zur punktuellen Fehlersuche bietet SILworX einen Testmodus an. Im Testmodus kann das Anwenderprogramm in Einzelschritten, d. h., Zyklus für Zyklus, ausgeführt werden. Jeder Zyklus wird durch ein Kommando vom PADT ausgelöst. In der Zeit zwischen 2 Zyklen sind die von diesem Anwenderprogramm beschriebenen globalen Variablen **eingefroren**. Dadurch reagieren die zugeordneten physikalischen Ausgänge und Kommunikationsdaten nicht mehr auf Änderungen im Prozess.

Der Testmodus kann über den Parameter *Testmodus erlaubt* für jedes Anwenderprogramm einzeln aktiviert/deaktiviert werden.

<i>Testmodus erlaubt</i>	Beschreibung
Deaktiviert	Testmodus deaktiviert (Standardeinstellung).
Aktiviert	Testmodus aktiviert.

Tabelle 16: Anwenderprogramm-Parameter *Testmodus erlaubt*

HINWEIS



Störung des sicherheitsbezogenen Betriebs möglich!

Wenn ein Anwenderprogramm im Testmodus gestoppt ist, kann das Anwenderprogramm nicht auf Änderungen an den Eingängen sicherheitsbezogen reagieren und die Ausgänge nicht ansteuern!

Daher ist im sicherheitsbezogenen Betrieb der Testmodus nicht zulässig!

Für den sicherheitsbezogenen Betrieb muss der Parameter *Testmodus erlaubt* deaktiviert sein!

11.1.11 Online-Änderung von Systemparametern

Es ist möglich, die Systemparameter der Tabelle 17 online in der Steuerung zu ändern.

Ein typischer Anwendungsfall ist die vorübergehende Erhöhung der Watchdog-Zeit, um ein Reload durchführen zu können.

Vor dem Setzen der Parameter durch ein Online-Kommando ist zu bedenken, ob diese Parameteränderung zu einem riskanten Zustand der Anlage führen kann. Falls nötig, sind organisatorische und/oder technische Maßnahmen zu treffen, um einen Schadensfall auszuschließen. Die Anwendungsnormen sind zu beachten!

Die Werte der Sicherheitszeit und Watchdog-Zeit sind gegen die von der Anwendung geforderte Sicherheitszeit und gegen die tatsächliche Zykluszeit zu prüfen. Diese Werte können von der Steuerung nicht verifiziert werden!

Die Steuerung verhindert die Einstellung der Watchdog-Zeit auf einen Wert, der kleiner ist als die Watchdog-Zeit der in der Steuerung geladenen Konfiguration.

Parameter	Änderbar im Zustand der Steuerung
System-ID	STOPP
Watchdog-Zeit (der Ressource)	RUN, STOPP/GÜLTIGE_KONFIGURATION
Sicherheitszeit	RUN, STOPP/GÜLTIGE_KONFIGURATION
Sollzykluszeit	RUN, STOPP/GÜLTIGE_KONFIGURATION
Sollzykluszeit-Modus	RUN, STOPP/GÜLTIGE_KONFIGURATION
Online-Einstellungen erlauben	TRUE -> FALSE: Alle FALSE -> TRUE: STOPP
Autostart	Alle
Start erlaubt	Alle
Laden erlaubt	Alle
Reload erlaubt	Alle
Globales Forcen erlaubt	Alle
Globale Force Timeout-Reaktion	Alle
Globales MultiForcen erlaubt	Alle

Tabelle 17: Online änderbare Parameter

11.1.12 Projekt-Dokumentation für sicherheitsbezogene Anwendungen

Das Programmierwerkzeug SILworX ermöglicht den automatischen Ausdruck der Dokumentation eines Projektes. Die wichtigsten Dokumentationsarten sind:

- Schnittstellendeklaration.
- Signalliste.
- Logik.
- Beschreibung der Datentypen.
- Konfigurationen für System, Module und Systemparameter.
- Konfiguration des Netzwerks.
- Signal-Querverweisliste.

Die Dokumentation ist Bestandteil der Funktionsabnahme einer genehmigungspflichtigen Anlage durch eine Prüfstelle, z. B. TÜV.

11.1.13 Multitasking

Multitasking bezeichnet die Fähigkeit des HIMax Systems, bis zu 32 Anwenderprogramme innerhalb des Prozessormoduls abzuarbeiten.

Die einzelnen Anwenderprogramme lassen sich unabhängig voneinander starten und stoppen.

Der Zyklus eines Anwenderprogramms kann mehrere Zyklen des Prozessormoduls dauern. Dies ist durch Parameter der Ressource und des Anwenderprogramms steuerbar. Aus diesen Parametern errechnet SILworX die Watchdog-Zeit des Anwenderprogramms zu:

Watchdog-Zeit_{Anwenderprogramm} = Watchdog-Zeit_{Prozessormodul} x Maximale Zyklenanzahl

Die einzelnen Anwenderprogramme laufen generell rückwirkungsfrei voneinander ab. Gegenseitige Beeinflussung ist jedoch möglich durch:

- Verwendung derselben globalen Variablen in mehreren Anwenderprogrammen.
- Unvorhersehbar lange Laufzeiten bei einzelnen Anwenderprogrammen, falls keine Limitierung durch *Max Dauer pro Zyklus* parametrisiert ist.
- Die Verteilung der Anwenderprogramm-Zyklen auf Prozessormodul-Zyklen beeinflusst die Reaktionszeit des Anwenderprogramms und der vom Anwenderprogramm beschriebenen Variablen!
- Ein Anwenderprogramm wertet globale Variablen, die ein anderes Anwenderprogramm beschrieben hat, frühestens einen CPU-Zyklus später aus. Abhängig von der Einstellung *Maximale CPU-Zyklen Programm* in den Programmeigenschaften kann sich das Auswerten um eine größere Anzahl von CPU-Zyklen verzögern, was auch die Reaktion verzögert!

Weitere Informationen zum Multitasking finden Sie im Systemhandbuch HI 801 000 D.

11.1.14 Abnahme durch Genehmigungsbehörden

HIMA empfiehlt, bei der Projektierung einer abnahmepflichtigen Anlage so früh wie möglich die Genehmigungsbehörden einzuschalten.

Die Abnahme bezieht sich nur auf die Anwenderfunktion, nicht aber auf die sicherheitsbezogenen Module und Automatisierungsgeräte des Systems HIMax, die bereits baumustergeprüft sind.

11.2 Checkliste zur Erstellung eines Anwenderprogramms

HIMA empfiehlt, die verfügbare Checkliste zur Einhaltung sicherheitstechnischer Aspekte bei der Programmierung, vor und nach dem Laden des neuen oder geänderten Programms einzusetzen. Die Checkliste ist als Planungsunterlage einsetzbar, dient aber gleichzeitig auch als Nachweis für eine sorgfältig durchgeführte Planung.

Die aktuellen Checklisten können über die E-Mail-Adresse documentation@hima.com angefragt werden. Für registrierte Kunden stehen die Produktdokumentationen im HIMA Extranet als Download zur Verfügung.

12 Konfiguration der Kommunikation

Neben den physikalischen Eingangs- und Ausgangsvariablen können Variablenwerte auch über eine Datenverbindung mit einem anderen System ausgetauscht werden. Hierzu werden die Variablen mit dem Programmierwerkzeug SILworX im Bereich Protokolle der jeweiligen Ressource deklariert.

12.1 Standardprotokolle

Eine Reihe von Kommunikationsprotokollen erlaubt nur eine nicht sicherheitsbezogene Übertragung von Daten. Diese können für nicht sicherheitsbezogene Teile einer Automatisierungsaufgabe verwendet werden.

WARNUNG



Personenschaden durch Verwendung unsicherer Importdaten möglich!

Aus nicht sicheren Quellen importierte Daten nicht für die Sicherheitsfunktionen des Anwenderprogramms verwenden!

12.1.1 Verfügbare Protokolle und Übertragungsmedium

Für die HIMax stehen die in der folgenden Tabelle aufgelisteten Standardprotokolle über die Kommunikationsmodule zur Verfügung.

Protokoll	Feldbus	TCP/UDP
ComUserTask	X	X
Modbus Master	X	X
Modbus Slave Set	X	X
Modbus Slave Set V2	X	X
PROFIBUS DP Slave	X	-
SNTP Client	-	X
SNTP Server	-	X

Tabelle 18: Verfügbare Protokolle und Übertragungsmedium

12.2 Sicherheitsbezogenes Protokoll safeethernet

Die sicherheitsbezogene Kommunikation über **safeethernet** ist bis SIL 3 zertifiziert.

Die Überwachung der sicherheitsbezogenen Kommunikation ist im **safeethernet**-Editor zu parametrieren.

Weitere Einzelheiten zu **safeethernet** sind dem Kommunikationshandbuch HI 801 100 D zu entnehmen.

i

Unbeabsichtigter Übergang in den sicheren Zustand möglich!

***ReceiveTMO* und *Production Rate* sind sicherheitsbezogene Parameter!**

ReceiveTMO ist die Überwachungszeit, innerhalb der eine korrekte Antwort von einer anderen Steuerung empfangen werden muss.

Trifft innerhalb der *ReceiveTMO* keine korrekte Antwort des Kommunikationspartners ein, schließt HIMax die sicherheitsbezogene Kommunikation. Die Input-Variablen dieser **safeethernet** Verbindung verhalten sich gemäß dem eingestellten Parameter *Freeze-Daten bei Verbindungsverlust [ms]*. Für sicherheitsbezogene Funktionen, die über **safeethernet** realisiert werden, muss die Einstellung **Initialwert verwenden** benutzt werden.

Es ist möglich, in den folgenden Berechnungen der maximalen Reaktionszeit (*Worst Case Reaction Time*) die *Sollzykluszeit* an Stelle der *Watchdog-Zeit* einzusetzen, wenn gewährleistet ist, dass das Prozessormodul die Sollzykluszeit einhält, auch bei Reload und Synchronisierung.

In diesem Fall gelten für die Einstellung des *Sollzykluszeit-Modus* auf *fest-tolerant* oder *dynamisch-tolerant* die folgenden Voraussetzungen:

1. **Watchdog-Zeit** \geq **1,5 x Sollzykluszeit**
2. **ReceiveTMO** \geq **5 x Sollzykluszeit** + **4 x Latenz**

Latenz ist die Verzögerung auf der Übertragungsstrecke.

3. Bei Reload gibt es entweder nur ein Anwenderprogramm oder mehrere Anwenderprogramme, deren Zyklus sich auf einen Zyklus des Prozessormoduls beschränkt.

12.3 Maximale Reaktionszeit für safeethernet

In den folgenden Beispielen gelten die Formeln für die Berechnung der maximalen Reaktionszeit im Fall einer Verbindung mit HIMatrix Steuerungen nur dann, wenn auf diesen keine Störaustattung programmiert wurde. 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.
Reaktionszeit der HIMax Steuerung	Für weitere Informationen zur Reaktionszeit der HIMax Steuerung (Ressource) t_{RR} , siehe Kapitel <i>Sicherheitsrelevante Zeiten</i> .
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 19: Beschreibung safeethernet Parameter und Bedingungen

Für die folgenden 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.

12.3.1 Berechnung der maximalen 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:

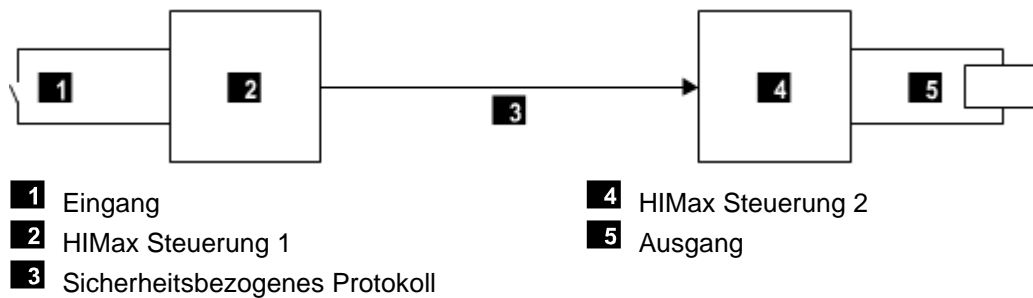


Bild 4: Reaktionszeit bei Verbindung zweier HIMax Steuerungen

$$T_R = t_1 + t_2 + t_3$$

T_R Worst Case Reaction Time

t_1 Sicherheitszeit der HIMax Steuerung 1

t_2 *ReceiveTMO*

t_3 Sicherheitszeit der HIMax Steuerung 2

12.3.2 Berechnung der max. Reaktionszeit in Verbindung mit einer HIMatrix Steuerung

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

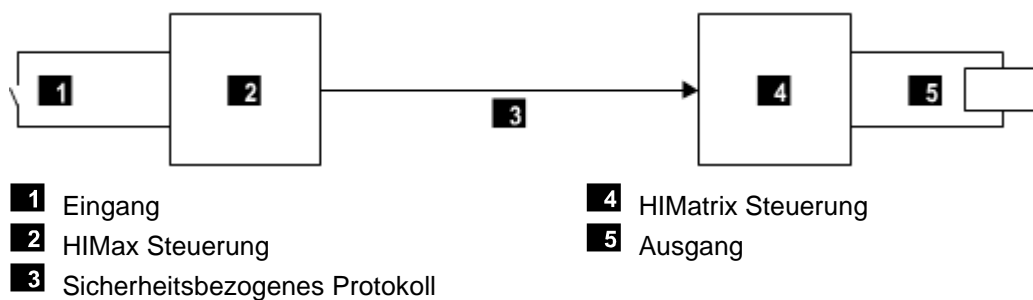


Bild 5: Reaktionszeit bei Verbindung einer HIMax mit einer HIMatrix Steuerung

$$T_R = t_1 + t_2 + t_3$$

T_R Worst Case Reaction Time

t_1 Sicherheitszeit der HIMax Steuerung

t_2 *ReceiveTMO*

t_3 2 * Watchdog-Zeit der HIMatrix Steuerung

12.3.3 Berechnung der max. Reaktionszeit 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:

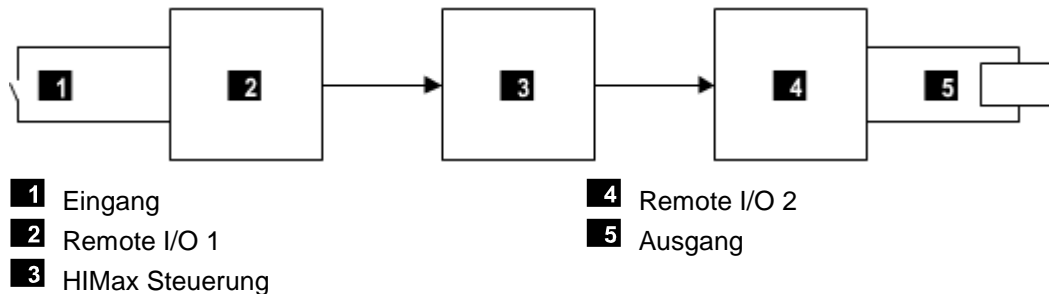


Bild 6: Reaktionszeit mit zwei HIMatrix Steuerungen/Remote I/Os und einer HIMax Steuerung

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

T_R Worst Case Reaction Time

t_1 2 * Watchdog-Zeit der HIMatrix Steuerung/Remote I/O 1

t_2 *ReceiveTMO1*

t_3 2 * Watchdog-Zeit der HIMax Steuerung

t_4 *ReceiveTMO2*

t_5 2 * Watchdog-Zeit der HIMatrix Steuerung/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.

12.3.4 Berechnung der max. Reaktionszeit mit zwei HIMax und einer HIMatrix Steuerung

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:

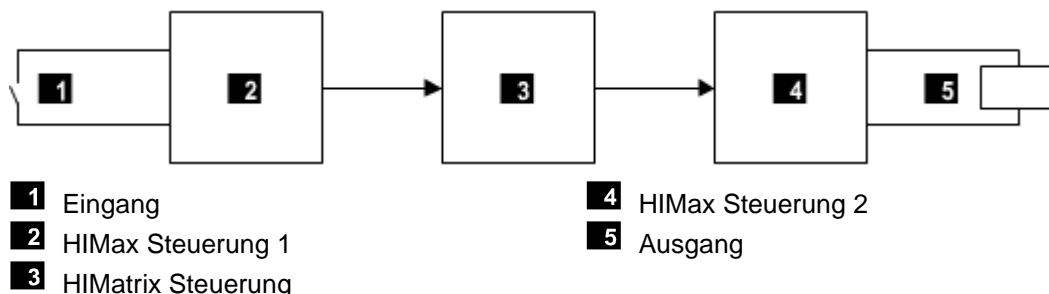


Bild 7: Reaktionszeit mit zwei HIMax Steuerungen und einer HIMatrix Steuerung

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

T_R	Worst Case Reaction Time
t_1	Sicherheitszeit der HIMax Steuerung 1
t_2	<i>ReceiveTMO1</i>
t_3	2 * Watchdog-Zeit des HIMatrix Steuerung
t_4	<i>ReceiveTMO2</i>
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.

12.4 Sicherheitsbezogenes Protokoll HIPRO-S V2

Das HIPRO-S V2 Protokoll wird zur sicherheitsbezogenen Kommunikation gemäß SIL 3 zwischen HIMax Steuerungen und HIQuad X, HIQuad oder HIMatrix Steuerungen verwendet. Voraussetzung für den Einsatz von HIPRO-S V2 sind die folgenden Betriebssysteme:

- Für HIMax Steuerungen eine Betriebssystem-Version ab V8.
- Für HIQuad X Steuerungen.
- Für HIQuad Steuerungen mit Betriebssystem-Ausgabe ab BS41q/51q V7.0-8 (08.xx).
- Für HIMatrix 03 Steuerungen mit Betriebssystem-Version ab V12 (CPU) / V16.10 (COM).

Das HIPRO-S V2 Protokoll darf nur für Verbindungen zwischen HIQuad Steuerungen oder zu HIMax Steuerungen verwendet werden. Verbindungen zwischen HIMax Steuerungen untereinander und mit HIMatrix Steuerungen müssen mit **safeethernet** aufgebaut werden!

Für weitere Informationen, siehe HIPRO-S V2 Handbuch HI 800 722 D.

12.5 Sicherheitsbezogenes Protokoll PROFIsafe

Das PROFIsafe Protokoll wird zur sicherheitsbezogenen Kommunikation gemäß SIL 3 zwischen HIMax Steuerungen und HIQuad X, HIQuad oder HIMatrix Steuerungen verwendet.

Für weitere Informationen siehe Kommunikationshandbuch HI 801 100 D.

13 Einsatz in Brandmelderzentralen

Die HIMax Systeme sind für Brandmelderzentralen nach DIN EN 54-2 und NFPA 72 einsetzbar, wenn für die Eingänge und Ausgänge Leitungsüberwachung parametrierbar ist.

Hierzu ist es erforderlich, dass das Anwenderprogramm die Funktionalitäten für Brandmelderzentralen nach den genannten Normen erfüllt.

DIN EN 54-2 fordert 10 s als maximale Zykluszeit für Brandmelderzentralen. Dieser maximale Wert kann mit den HIMA Systemen leicht erfüllt werden, da die Zykluszeiten dieser Systeme im Bereich von Millisekunden liegen. Dies gilt ebenso für die gegebenenfalls geforderte Sicherheitszeit von 1 s (Fehlerreaktionszeit).

Nach DIN EN 54-2 muss die Brandmelderzentrale den Störungsmeldezustand innerhalb von 100 s nach Empfang der Störungsmeldung im HIMax System einnehmen.

Der Anschluss der Brandmelder erfolgt im Arbeitsstromprinzip mit Leitungsüberwachung auf Leitungsschluss und Leitungsbruch. Hierzu sind folgende Eingänge und Ausgänge verwendbar:

- Die digitalen und analogen Eingänge der Eingangsmodule mit Leitungsüberwachung.
- Die digitalen Ausgänge der Ausgangsmodule mit Leitungsüberwachung

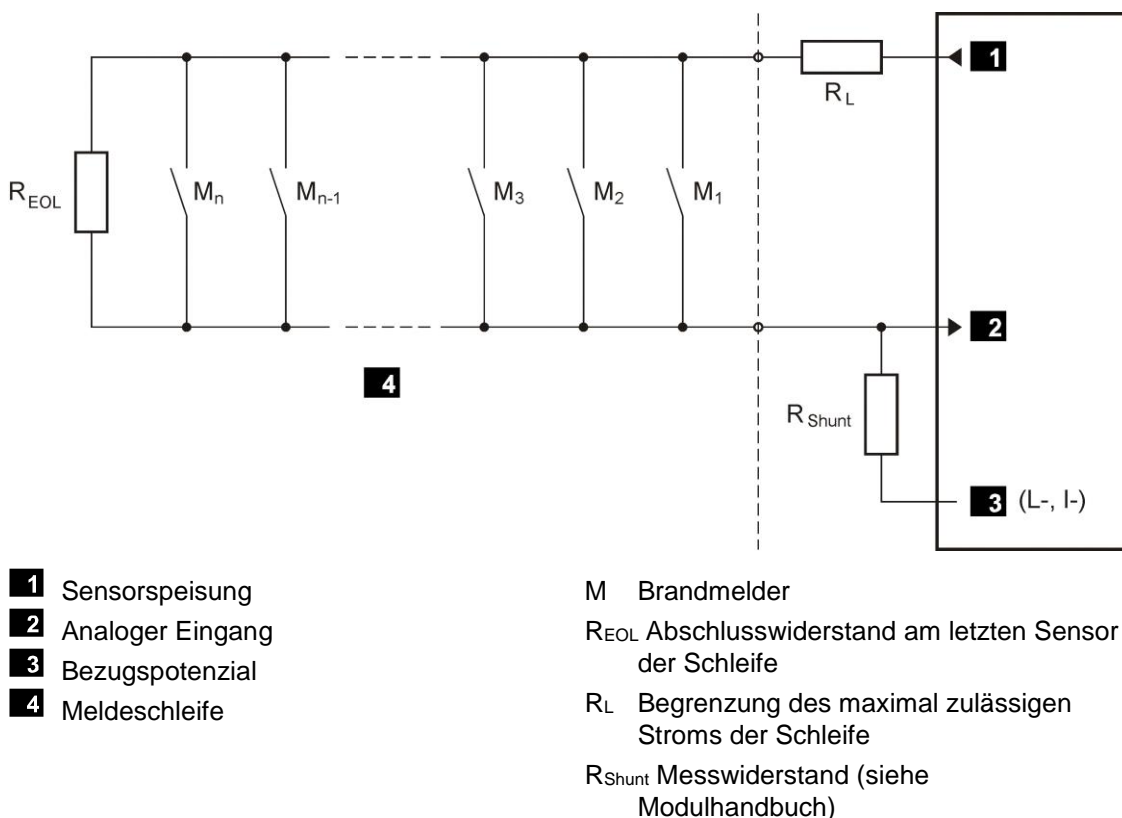


Bild 8: Verschaltung von Brandmeldern

Für die Anwendung sind die Widerstände R_{EOL} , R_L und R_{Shunt} abhängig von den eingesetzten Sensoren und der Anzahl der Sensoren pro Meldeschleife zu berechnen. Die dafür notwendigen Daten sind dem jeweiligen Datenblatt des Sensorherstellers zu entnehmen.

Die Alarmausgänge zur Ansteuerung von z. B. Lampen, Sirenen und Hupen werden im Arbeitsstromprinzip betrieben. Diese Ausgänge sind auf Leitungsbruch und Leitungsschluss zu überwachen. Dazu ist die Leitungsüberwachung der Ausgangsmodule zu konfigurieren und im Anwenderprogramm zu verarbeiten.

Ein entsprechend angepasstes Anwenderprogramm kann die Ansteuerung von z. B. Visualisierungssystemen, Leuchtmeldetableaus, LED-Anzeigen, alphanumerischen Displays und akustischen Alarmen realisieren.

Die Weiterleitung von Störungsmeldungen über Eingangs- und Ausgangskanäle oder zu Übertragungseinrichtungen für Störungsmeldungen muss im Ruhestromprinzip erfolgen.

Die Übertragung von Brandmeldungen von einem HIMax System zu einem Fremdsystem kann mit dem vorhandenen Kommunikationsstandard Ethernet (OPC) realisiert werden. HIMA empfiehlt, die Kommunikation redundant auszuführen, damit bei Störung einer Komponente einer Übertragungsstrecke (z. B. Leitung, Hardwarefehler) die Kommunikation weiterhin gewährleistet ist. Der Ausfall der Komponente muss gemeldet werden und die defekte Komponente soll während des Betriebs getauscht oder repariert werden können.

HIMax Systeme, die als Brandmelderzentrale eingesetzt werden, müssen eine redundante Stromversorgung haben. Zusätzlich müssen Vorkehrungen gegen einen Ausfall der Energieversorgung getroffen werden, z. B. Einsatz einer batteriebetriebenen Hupe. Die Umschaltung zwischen Netzversorgung und der Ersatzstromversorgung muss einen unterbrechungsfreien Betrieb gewährleisten. Spannungseinbrüche bis zu einer Dauer von 10 ms sind zulässig.

Bei Störungen des Systems beschreibt das Betriebssystem die im Anwenderprogramm zugewiesenen Systemvariablen. Somit ist eine Fehlersignalisierung auf die vom System erkannten Fehler programmierbar. Das HIMax System schaltet im Fehlerfall sicherheitsbezogene Eingänge und Ausgänge ab, mit folgenden Auswirkungen:

- Verarbeitung des Low-Pegels in allen Kanälen der fehlerhaften Eingänge.
- Abschaltung aller Kanäle der fehlerhaften Ausgänge.

Bei Brandmelderanlagen nach DIN EN 54-2 und NFPA 72 ist eine Erdschlussüberwachung einzusetzen.

14 ATEX-konformer Einsatz als Sicherheits-, Kontroll- und Regelvorrichtung

Die folgenden HIMax Komponenten sind geeignet für den bestimmungsgemäßen Einsatz zur Detektion und Messung von brennbaren Gasen:

- X-BASE PLATE
- X-SB 01
- X-CPU 01, X-CPU 31
- X-AI 32 01, X-AI 32 02
- X-DO 24 01, X-DO 32 01

Die genannten HIMax Komponenten sind nach folgenden Normen geprüft:

- EN 50271:2010
- EN 50495:2010
- IEC / EN 60079-0:2012 + A11:2013
- IEC / EN 60079-29-1:2008

Die genannten Komponenten erfüllen die Anforderungen der Richtlinie 2014/34/EU und sind Sicherheits-, Kontroll- und Regelvorrichtungen gemäß ATEX Richtlinie.

Die genannten Komponenten sind geeignet zur Überwachung von Zündgefährdungen in explosionsgefährdeten Bereichen als zugehörige Betriebsmittel, oder als ortsfeste Gaswarnzentralen zur Detektion und Messung von brennbaren Gasen.

Die Hardware und Software der Komponenten ist auf Einhaltung der Anforderungen gemäß EN 60079-29-1 und EN 50271 geprüft.

An den 4 ... 20 mA Signaleingängen sind Gassensoren anzuschließen, die den Anforderungen der EN 60079-29-1 genügen. Die Anschaltung der Gassensoren muss unter Beachtung der Dokumentationen und der EU-Baumusterprüfbescheinigungen durchgeführt werden.

Die Erstellung des sicherheitsrelevanten Applikationsprogramms muss unter Beachtung des Sicherheitshandbuchs mit dem Programmierwerkzeug SILworX erfolgen.

Die sicherheitstechnische Funktion ist durch Verifikation und Validation nachzuweisen.

Für die herzustellende Sicherheitseinrichtung oder Gaswarnanlage ist eine zugehörige Sicherheitsinformation und Betriebsanleitung nach 2014/34/EU, Anhang II, Absatz 1.0.6 zu erstellen. In einem weiteren Konformitätsbewertungsverfahren ist für die Sicherheitseinrichtung oder Gaswarnanlage eine vollständige EU-Baumusterprüfbescheinigung zu erstellen, unter Berücksichtigung der oben aufgeführten Punkte.

15 Einsatz von HIMax in Zone 2

HIMax Komponenten sind zum Einbau in den explosionsgefährdeten Bereich der Zone 2 geeignet. Dazu sind, neben den besonderen Bedingungen, die Montage- und Installationsangaben in den Modulhandbüchern und dem Systemhandbuch HI 801 000 D zu beachten.

HIMax Komponenten erfüllen die Anforderungen folgender Normen:

Norm	Beschreibung
IEC 60079-0	Explosionsgefährdete Bereiche – Teil 0: Betriebsmittel Allgemeine Anforderungen
EN 60079-0	
IEC 60079-15	Explosionsgefährdete Atmosphäre – Teil 15: Geräteschutz durch Zündschutzart «n»
EN 60079-15	

Tabelle 20: Normen für HIMax Komponenten in Zone 2

Die aktuelle Konformitätserklärung für die HIMax Komponenten ist auf den HIMA Webseiten www.hima.com/de zu finden.

Die HIMax Komponenten sind für Temperaturbereich $0\text{ °C} \leq T_a \leq +60\text{ °C}$ zugelassen und haben die folgenden Ex-Kennzeichnungen, siehe Tabelle 22:


Kennzeichnung	Beschreibung
	Ex-Kennzeichen nach Richtlinie 2014/34/EU
II	Gerätegruppe, für alle explosionsgefährdeten Bereiche außer schlagwettergefährdete Grubenbaue.
3G	Gerätekategorie, Bereich mit normalerweise keinem, oder nur kurzfristig auftretendem brennbarem Gasgemisch.
Ex	Ex-Kennzeichen nach Norm
nA	Zündschutzart für nicht funkende Einrichtung
nC	Zündschutzart für funkende, abgedichtete Einrichtung
IIC	Zündgruppe des Gases, typisches Gas ist Wasserstoff
T4	Temperaturklasse T4, mit einer maximalen Oberflächentemperatur von 135 °C
Gc	Geräteschutzniveau, entspricht der ATEX-Gerätekategorie 3G

Tabelle 21: Beschreibung Ex-Kennzeichnung HIMax Komponenten

Besondere Bedingungen

1. HiMax Komponenten sind in ein Gehäuse einzubauen, das die Anforderungen der IEC 60079-0/EN 60079-0 oder IEC 60079-15/EN 60079-15 mit einer Schutzart IP54 oder besser erfüllt.
2. Das Gehäuse muss mit einem Warnhinweis versehen sein:

WARNUNG: Arbeiten nur im spannungslosen Zustand zulässig

Ausnahme:

Wenn sichergestellt ist, dass keine explosionsfähige Atmosphäre vorhanden ist, darf auch unter Spannung gearbeitet werden.

3. Die HiMax Komponenten sind für den Betrieb mit maximalem Verschmutzungsgrad 2 ausgelegt.
4. Das verwendete Gehäuse muss die entstehende Verlustleistung sicher abführen können. Die Verlustleistung der HiMax Komponenten ist der Tabelle 22 zu entnehmen.
5. Die Versorgungsspannungen sind aus Netzgeräten mit sicherer Trennung zu entnehmen. Nur Netzgeräte in den Ausführungen PELV oder SELV einsetzen.
6. Die in den Modulhandbüchern aufgeführten Bedingungen sind zu beachten.

Anwendbare Normen:

IEC 60079-14	Explosionsgefährdete Bereiche – Teil 14: Projektierung, Auswahl und Errichtung elektrischer Anlagen.
EN 60079-14	

Anforderungen für die Zündschutzart «n» sind zu beachten.

Komponente	Ex-Kennzeichnung	Max. Verlustleistung
CB / FTA für X-AI 32 01	 II 3G Ex nA IIC T4 Gc	3 W
CB / FTA für X-DI 32 02	 II 3G Ex nA IIC T4 Gc	3 W
CB / FTA für X-DI 32 05	 II 3G Ex nA IIC T4 Gc	3 W
CB / FTA für X-AI 32 02	 II 3G Ex nA IIC T4 Gc	3 W
X-AI 16 51	 II 3G Ex nA IIC T4 Gc	11 W
X-AI 32 01	 II 3G Ex nA IIC T4 Gc	21 W
X-AI 32 02	 II 3G Ex nA IIC T4 Gc	21 W
X-AI 32 51	 II 3G Ex nA IIC T4 Gc	14 W
X-AO 16 01	 II 3G Ex nA IIC T4 Gc	38 W
X-AO 16 51	 II 3G Ex nA IIC T4 Gc	13 W
X-BASE PLATE	 II 3G Ex nA IIC T4 Gc	15 W
X-CI 24 01	 II 3G Ex nA IIC T4 Gc	21 W
X-CI 24 51	 II 3G Ex nA IIC T4 Gc	12 W
X-COM 01	 II 3G Ex nA IIC T4 Gc	9 W
X-CPU 01	 II 3G Ex nA IIC T4 Gc	41 W
X-CPU 31	 II 3G Ex nA IIC T4 Gc	21 W
X-DI 16 01	 II 3G Ex nA IIC T4 Gc	33 W
X-DI 32 01	 II 3G Ex nA IIC T4 Gc	15 W
X-DI 32 02	 II 3G Ex nA IIC T4 Gc	23 W
X-DI 32 03	 II 3G Ex nA IIC T4 Gc	17 W
X-DI 32 04	 II 3G Ex nA IIC T4 Gc	15 W
X-DI 32 05	 II 3G Ex nA IIC T4 Gc	23 W
X-DI 32 51	 II 3G Ex nA IIC T4 Gc	13 W
X-DI 32 52	 II 3G Ex nA IIC T4 Gc	10 W
X-DI 64 01	 II 3G Ex nA IIC T4 Gc	21 W
X-DI 64 51	 II 3G Ex nA IIC T4 Gc	15 W
X-DO 12 01	 II 3G Ex nA nC IIC T4 Gc	51 W
X-DO 12 02	 II 3G Ex nA IIC T4 Gc	38 W
X-DO 12 51	 II 3G Ex nA nC IIC T4 Gc	32 W
X-DO 24 01	 II 3G Ex nA IIC T4 Gc	29 W
X-DO 24 02	 II 3G Ex nA IIC T4 Gc	34 W
X-DO 32 01	 II 3G Ex nA IIC T4 Gc	34 W
X-DO 32 51	 II 3G Ex nA IIC T4 Gc	31 W
X-FAN 10 01	 II 3G Ex nA nC IIC T4 Gc	28 W
X-FAN 10 03	 II 3G Ex nA nC IIC T4 Gc	7 W











Komponente	Ex-Kennzeichnung	Max. Verlustleistung
X-FAN 15 01	 II 3G Ex nA nC IIC T4 Gc	41 W
X-FAN 15 02	 II 3G Ex nA nC IIC T4 Gc	41 W
X-FAN 15 03	 II 3G Ex nA nC IIC T4 Gc	9 W
X-FAN 15 04	 II 3G Ex nA nC IIC T4 Gc	9 W
X-FAN 18 01	 II 3G Ex nA nC IIC T4 Gc	55 W
X-FAN 18 03	 II 3G Ex nA nC IIC T4 Gc	12 W
X-FTA 005 02L (X-DO 12 01)	 II 3G Ex nA IIC T4 Gc	7 W
X-HART 32 01	 II 3G Ex nA IIC T4 Gc	9 W
X-MIO 7/6 01	 II 3G Ex nA nC IIC T4 Gc	45 W
X-SB 01	 II 3G Ex nA IIC T4 Gc	21 W

Tabelle 22: Kennzeichnung und Verlustleistung von HIMax Komponenten

Anhang

Glossar

Begriff	Beschreibung
AI	Analog Input: Analoger Eingang
AO	Analog Output: Analoger Ausgang
ARP	Address Resolution Protocol: Netzwerkprotokoll zur Zuordnung von Netzwerkadressen zu Hardware-Adressen
COM	Kommunikation (Modul)
CRC	Cyclic Redundancy Check: Prüfsumme
DI	Digital Input: Digitaler Eingang
DO	Digital Output: Digitaler Ausgang
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Normen
ESD	Electrostatic Discharge: Elektrostatische Entladung
FB	Feldbus
FBS	Funktionsbausteinsprache
HW	Hardware
ICMP	Internet Control Message Protocol: Netzwerkprotokoll für Status- und Fehlermeldungen
IEC	Internationale Normen für die Elektrotechnik
LS/LB	Leitungsschluss/Leitungsbruch
MAC	Media Access Control: Hardware-Adresse eines Netzwerkanschlusses
PADT	Programming and Debugging Tool (nach IEC 61131-3): PC mit SILworX
PELV	Protective Extra Low Voltage: Funktionskleinspannung mit sicherer Trennung
PES	Programmable Electronic System: Programmierbares Elektronisches System
R	Read: Auslesen einer Variablen
Rack-ID	Identifikation eines Basisträgers (Nummer)
rückwirkungsfrei	Eingänge sind für rückwirkungsfreien Betrieb ausgelegt und können in Schaltungen mit Sicherheitsfunktionen eingesetzt werden.
R/W	Read/Write: Spaltenüberschrift für Art von Systemvariable
SB	Systembus (-modul)
SELV	Safety Extra Low Voltage: Schutzkleinspannung
SFF	Safe Failure Fraction: Anteil der sicher beherrschbaren Fehler
SIL	Safety Integrity Level (nach IEC 61508)
SILworX	Programmierwerkzeug
SNTP	Simple Network Time Protocol (RFC 1769)
SRS	System.Rack.Slot: Adressierung eines Moduls
SSL	Secure Sockets Layer, siehe TLS
SW	Software
TLS	Transport Layer Security: Hybrides Verschlüsselungsprotokoll
TMO	Timeout
W	Write: Variable wird mit Wert versorgt, z. B. vom Anwenderprogramm
WD	Watchdog: Funktionsüberwachung für Systeme. Signal für fehlerfreien Prozess
WDZ	Watchdog-Zeit
ws	Scheitelwert der Gesamt-Wechselspannungskomponente

Abbildungsverzeichnis

Bild 1:	Empfohlene Konfiguration: alle Prozessormodule auf Rack 0	36
Bild 2:	Empfohlene Konfiguration: Prozessormodule X-CPU 01 auf Rack 0 und Rack 1	36
Bild 3:	Konfiguration mit Prozessormodulen X-CPU 31 auf Rack 0, Steckplätze 1 und 2	37
Bild 4:	Reaktionszeit bei Verbindung zweier HIMax Steuerungen	79
Bild 5:	Reaktionszeit bei Verbindung einer HIMax mit einer HIMatrix Steuerung	79
Bild 6:	Reaktionszeit mit zwei HIMatrix Steuerungen/Remote I/Os und einer HIMax Steuerung	80
Bild 7:	Reaktionszeit mit zwei HIMax Steuerungen und einer HIMatrix Steuerung	80
Bild 8:	Verschaltung von Brandmeldern	82

Tabellenverzeichnis

Tabelle 1: Übersicht Systemdokumentation	13
Tabelle 2: Umgebungsbedingungen	25
Tabelle 3: Internationale Normen und Sicherheitsstufen	29
Tabelle 4: Normen für EMV-, Klima- und Umweltaanforderungen	30
Tabelle 5: Prüfungen der Störaussendung	30
Tabelle 6: Klimatische Prüfungen	31
Tabelle 7: Mechanische Prüfungen	31
Tabelle 8: Nachprüfung der Gleichstromversorgungs-Eigenschaften	32
Tabelle 9: Übersicht Eingangsmodule	39
Tabelle 10: Übersicht Ausgangsmodule	43
Tabelle 11: Die Systemparameter der Ressource	54
Tabelle 12: Einstellungen Sollzykluszeit-Modus	55
Tabelle 13: Standardwerte der maximalen Systembus-Latenzzeit	58
Tabelle 14: Systemvariable der Hardware	59
Tabelle 15: Systemparameter des Anwenderprogramms	70
Tabelle 16: Anwenderprogramm-Parameter <i>Testmodus erlaubt</i>	73
Tabelle 17: Online änderbare Parameter	74
Tabelle 18: Verfügbare Protokolle und Übertragungsmedium	76
Tabelle 19: Beschreibung safeethernet Parameter und Bedingungen	78
Tabelle 20: Normen für HIMax Komponenten in Zone 2	85
Tabelle 21: Beschreibung Ex-Kennzeichnung HIMax Komponenten	85
Tabelle 22: Kennzeichnung und Verlustleistung von HIMax Komponenten	88

Index

Arbeitsstromprinzip	11	klimatisch	31
Ausgangs-Störaustastung	44, 45	mechanisch	31
Automation Security	26	Rack-ID	35
Besondere Bedingungen	86	Reaktionszeit	21
Brandmelder	82	Redundanz	16
Brandmelderzentralen	82	Responsible	35
CRC	71	Ruhestromprinzip	11
ESD-Schutz	12	Schadgase	32
Fehlerreaktion		Selbst-Test	16
Ausgänge	43	Sicherheitsfunktion	47
Eingänge	40	Sicherheitskonzept	50
Funktionstest der Steuerung	50	Sicherheitszeit	18
Hardware-Editor	59	Steuerung abschließbar machen	60
Kommunikationszeitscheibe	56	Surge	40
LED Ess	34	Versorgungsspannung	32
Leistungsüberwachung	82	Wartung	24
Multitasking	75	Watchdog-Zeit	
Online-Test-Feld	72	Abschätzung	20
PADT	16	Ressource	19
Prozess-Sicherheitszeit	18	Wiederholungsprüfung	22
Prüfbedingungen	30	Zone 2	85
EMV	31		


HANDBUCH
HIMax Sicherheitshandbuch
HI 801 002 D

Für weitere Informationen kontaktieren Sie:

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

Telefon +49 6202 709-0
Fax +49 6202 709-107
E-Mail info@hima.com

Erfahren Sie online mehr über HIMax:

 www.hima.com/de/produkte-services/himax/



www.hima.com