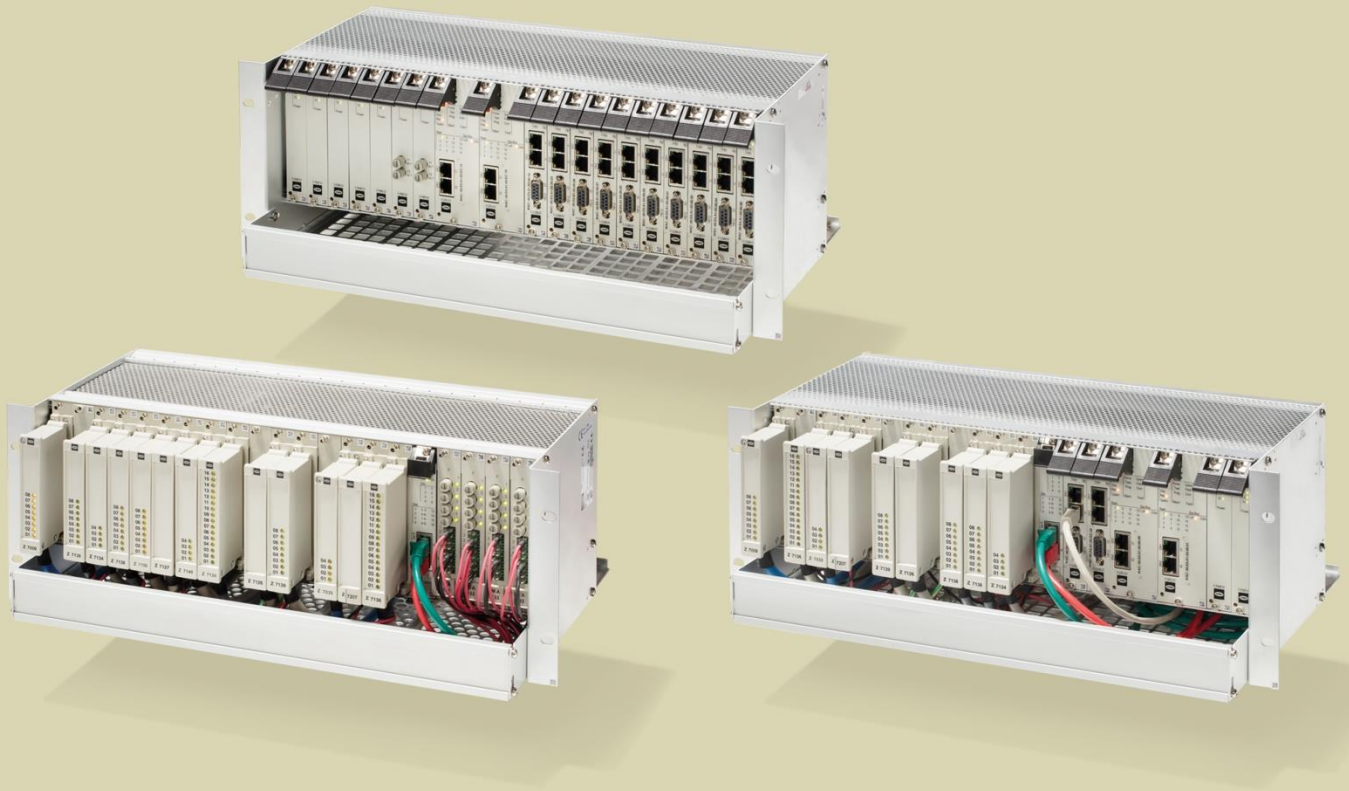
Handbuch

HIQuad®X

Sicherheitshandbuch



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
1.00	Erstausgabe		
2.00	Aktualisierte Ausgabe zu SILworX V11 Neu: Kapitel MultiForcen	X	X
3.00	Aktualisierte Ausgabe zu SILworX V12 Neu: Kapitel API-Sicherheitsmaßnahmen	X	X

Inhaltsverzeichnis

1 Einleitung

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

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 HIQuad X 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:

- HIQuad X Betriebssysteme gemäß Versionsliste.
- SILworX ab Version V12.

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

1.2 Zielgruppe

Dieses Dokument wendet sich an Planer, Projekteure, 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.
Kursiv	Parameter und Systemvariablen, Referenzen.
`Courier`	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 HIQuad X

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. 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 HIQuad X.

Das Automatisierungssystem ist ausgelegt für den Prozessmarkt zum Steuern und Regeln von verfahrenstechnischen Anlagen. Für die Programmierung, Konfiguration, Überwachung, Bedienung und Dokumentation des Systems HIQuad X wird das HIMA Programmierwerkzeug SILworX eingesetzt.

2.1.1 Anwendung im Ruhestromprinzip

Das HIQuad X 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 HIQuad X 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

HIQuad X 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 12.

2.1.4 Explosionsschutz

Das Automatisierungssystem HIQuad X ist geeignet zum Einbau in die Zone 2.

Die in Kapitel 13 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 HIQuad X Systeme in Automatisierungsanlagen und in Gesamtanlagen gewährleistet ist.

Die korrekte Programmierung der HIQuad X 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 11.3 und in den Handbüchern der Kommunikationsprotokolle aufgeführten Berechnungsgrundlagen sind anzuwenden.

2.3 ESD-Schutzmaßnahmen

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

HINWEIS

Schäden am HIQuad X 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 HIQuad X Systeme stehen außerdem noch folgende Dokumentationen zur Verfügung:

Name	Inhalt	Dokument-Nr.
HIQuad X Systemhandbuch	Hardwarebeschreibung des modularen Systems	HI 803 210 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 803 212 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 HIQuad X:

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

3.1 Sicherheit und Verfügbarkeit

Das System HIQuad X 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 HIQuad X 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 HIQuad X mit redundanten Prozessormodulen (F-CPU 01), redundanten Kommunikationsmodulen (F-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 wiederherzustellen.

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 HIQuad X 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} … 10^{-3}.

PFH = 10^{-8} … 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

Im HIQuad X System werden umfangreiche Selbst-Tests beim Start und im laufenden Betrieb durchgeführt.

Das Betriebssystem der Steuerungen 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.
- Die Spannungsversorgung.

Entdeckt das HIQuad X System bei den Selbst-Tests Modulfehler, so wird das betroffene Modul in den sicheren Zustand gebracht. Werden Modulfehler schon beim Starten eines Moduls entdeckt, geht das Modul erst gar nicht in Betrieb. Bei einem Kanalfehler wird nur der fehlerhafte Kanal abgeschaltet, sofern das E/A-Modul Kanalabschaltung unterstützt. Wenn schon bei der Initialisierung ein interner Kanalfehler festgestellt wird, dann geht der Kanal oder das Modul erst gar nicht in Betrieb.

In Mono-Systemen können im Fehlerfall entweder Teilfunktionen oder die gesamte Steuerung abgeschaltet werden. In redundanten Systemen führen redundanten Module oder redundante Kanäle die Funktion weiter aus, wenn in der Anlagenkonfiguration statt der Mono-Struktur eine Redundante Struktur implementiert ist.

Prozessormodule, E/A-Verarbeitungsmodule, Kommunikationsmodule und Power-Module sind mit LEDs ausgestattet, die entdeckte Fehler anzeigen. Damit ist im Störungsfall eine schnelle Fehlerdiagnose über einen gemeldeten Modulfehler oder einen Fehler in der externen Beschaltung möglich.

Das Programmierwerkzeug SILworX stellt außerdem Systemvariablen bereit, die Auswertungen der Modulzustände durch das Anwenderprogramm ermöglichen.

HIQuad X führt eine umfangreiche Diagnose des Systemverhaltens durch. Die Diagnosemeldungen und erkannten Fehler werden in den Diagnosespeichern des Prozessormoduls und des E/A-Verarbeitungsmoduls gespeichert. Module mit eigenem sicherheitsbezogenen Prozessorsystem führen eigene Diagnosen durch. Die Diagnosemeldungen können auch nach einer Systemstörung über das Programmierwerkzeug ausgelesen werden.

Weitere Informationen über die Auswertung der Diagnosemeldungen finden Sie im HIQuad X Systemhandbuch HI 803 210 D.

Bei einem sehr kleinen Teil der Bauelement-Ausfälle, welche die Sicherheit nicht beeinflussen, erzeugt das HIQuad X 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 HIQuad X 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 parametriert werden.
- Jedes E/A-Modul muss mit einer Leitungsschluss- und Leitungsbruch-Überwachung ausgestattet sein. Die Leistungsschluss- und Leitungsbruch-Überwachung muss parametriert 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.
- HIQuad X 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 803 210 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 $\mathbf{t}_{RR}$ wird durch den Parameter *Sicherheitszeit [ms]* in den Eigenschaften der Ressource $\mathbf{t}_{SR}$ wie folgt beeinflusst:

$$\mathbf{t}_{RR} \leq \mathbf{t}_{SR} + \mathbf{t}_{DO\ max.}$$

$\mathbf{t}_{SR}$ Parameter *Sicherheitszeit [ms]*

$\mathbf{t}_{DO\ max.}$ Maximale Abschaltzeit der Ausgangsmodule und dem Relaismodul F 3430 selbst, siehe Tabelle 2.

Modul	$\mathbf{t}_{DO\ max.}$
F 3330	13 ms ,nach IEC 61131-2 Typ 2
F 3331	18 ms, nach IEC 61131-2 Typ 2
F 3333	22 ms, nach IEC 61131-2 Typ 2
F 3334	21 ms, nach IEC 61131-2 Typ 2
F 3335	89 ms, nach IEC 61131-2 Typ 2
F 3349	7 ms, nach IEC 61131-2 Typ 2
F 3430	11 ms
F 6705	68 ms, Stromabfall von 20 mA auf 0/4 mA bei einer Last von 550 Ohm

Tabelle 2: Abschaltzeiten der Ausgangsmodule

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

- Physikalisch bedingte Verzögerungen, z. B. durch Schaltzeiten von externen Relais.
- Parametrierte Verzögerungen im Anwenderprogramm, z. B. durch Timer-Bausteine (TON, TOF).
- Verzögerungen durch µP-Module.

Wenn eines der µP-Module F 5220, F 6217, F 6220 und F 6221 mit eigenem Prozessorsystem verwendet wird, muss die Verzögerung dieser Module berücksichtigt werden:

$$t_{RR} \leq t_{SR} + t_{DO\ max.} + t_{D\ \mu P}$$

Wenn mehrere µP-Module verwendet werden, dann ist das Modul mit der längsten Verzögerung (Delay) ausschlaggebend, siehe Tabelle 3.

µP-Modul	$t_{D\ \mu P}$
F 5220	t_{SR} + 200 ms
F 6217	201 ms
F 6220	t_{SR} + 200 ms
F 6221	t_{SR} + 200 ms

Tabelle 3: Verzögerung (Delay) der µP-Module

Beispiel: F 6220, t_{SR} = 1000 ms, $t_{DO\ max.}$ = 0

$$t_{RR} \leq t_{SR} + t_{DO\ max.} + t_{D\ \mu P}$$

$$t_{RR} \leq t_{SR} + 0 + t_{SR} + 200\ ms$$

$$t_{RR} \leq 2 \times t_{SR} + 200\ ms$$

$$t_{RR} \leq 2 \times 1000\ ms + 200\ ms$$

$$t_{RR} \leq \underline{2200\ ms}$$

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 programmierten Verzögerungen durch das Anwenderprogramm.
- Anpassen des Parameters *Sicherheitszeit [ms]* t_{SR} bei Verwendung der µP-Module F 5220, F 6220 und F 6221.

Bei Verwendung der µP-Module F 5220, F 6220 und F 6221 gelten für den Parameter *Sicherheitszeit [ms]* die folgenden Bedingungen:

$$t_{SR} \geq \mathbf{4 \times t_{WD}}$$

$$t_{SR} \geq \mathbf{1000\ ms}$$

$$t_{WD} \geq \mathbf{50\ ms}$$

t_{WD} Watchdog-Zeit (Ressource)

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:

$t_{WD} \leq ½ \times t_{SR}$

t_{WD} Watchdog-Zeit (Ressource)

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

Bedingung für die Sicherheit plus Verfügbarkeit:

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

Die Watchdog-Zeit (Ressource) muss parametriert 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 ½ 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 der Steuerung (PES) folgende Bedingung einzuhalten:

$3 \times t_{WD} \leq t_{SR}$ **(Parameter** *Sicherheitszeit [ms]***)**

3.2.5 Watchdog-Zeit durch Test ermitteln

Die Watchdog-Zeit $\mathbf{t}_{WD}$ 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. safe**ethernet** 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. In den Ressource-Eigenschaften die *Maximale Systembus-Latenzzeit [µs]* auf die Standardeinstellung `System-Standardwerte` einstellen.
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 Zykluszeit im Control Panel ablesen und die Schwankungen und Lastspitzen nach Ablauf mehrerer Minuten notieren.
8. Nacheinander alle E/A-Verarbeitungsmodule (F-IOP 01) aus den Racks entfernen. Nachdem das letzte E/A-Verarbeitungsmodul entfernt wurde, die maximale Zykluszeit des Systems im Control Panel ablesen und notieren.
9. Die entfernten E/A-Verarbeitungsmodule in beliebiger Reihenfolge in die Racks stecken und warten, bis das System wieder im Normalbetrieb läuft.
10. Das Prozessormodul mit der höheren Steckplatz-Nummer aus dem Basis-Rack entfernen und danach die Zykluszeitstatistik im Control Panel zurücksetzen.
11. Das im vorherigen Schritt entfernte Prozessormodul wieder in das Basis-Rack stecken und warten, bis es sich mit dem verbliebenen Prozessormodul synchronisiert hat. Danach die maximale Zykluszeit im Control Panel ablesen und notieren.

i Das redundante Prozessormodul synchronisiert sich beim Hinzufügen automatisch mit der Konfiguration des vorhandenen Prozessormoduls. Die für die Synchronisation benötigte Zeit verlängert den Zyklus der Steuerung.

12. Die Schritte 10 und 11 mit dem Prozessormodul mit der niedrigeren Steckplatz-Nummer durchführen.

13. Die notierten Zeiten in die folgende Formel einsetzen:

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

t_{Sync} Maximale Synchronisationszeit der Prozessormodule. Den größeren Wert aus den Schritten 11 und 12 einsetzen.

$t_{Reserve}$ Sicherheitsreserve 12 ms.

t_{Komm} In den Ressource-Eigenschaften eingestellter Systemparameter *Max. Kom.Zeitscheibe [ms]*.

t_{Konfig} In den Ressource-Eigenschaften eingestellter Systemparameter *Maximale Dauer der Konfigurationsverbindung [ms].*

t_{Spitze} Maximale Lastspitze der Zykluszeit (t_{Spitze}). Den größere Wert aus den Schritten 7 und 8 einsetzen.

3.2.6 Typische Reaktionszeit

Die Reaktionszeit von zyklisch arbeitenden HIQuad X Steuerungen ist die doppelte Zykluszeit dieser Systeme im fehlerfreien Betrieb, wenn nicht durch Parametrierung oder durch die Logik des Anwenderprogramms eine Verzögerung erfolgt. Die zusätzlichen Verzögerungen der für eine Sicherheitsfunktion verwendeten E/A-Module müssen ebenfalls berücksichtigt werden, siehe Tabelle 2 und Tabelle 3.

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 803 212 D beschrieben.

3.4 Sicherheitsauflagen

Für den Einsatz des sicherheitsbezogenen Automatisierungssystems HIQuad X gelten die folgenden Sicherheitsauflagen.

3.4.1 Produktunabhängige Auflagen der Hardware

Personen, welche HIQuad X 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 HIQuad X 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 HIQuad X 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 HIQuad X 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 Überwachung der Temperatur

Die Temperatur der folgenden Module wird durch eingebaute Sensoren gemessen und kann im Programmierwerkzeug angezeigt und verwendet werden.

- F-CPU 01
- F-IOP 01
- F-PWR 01

i Die Temperatur kann im Anwenderprogramm z. B. als zusätzliches Abschaltkriterium verwendet werden, jedoch ist die Temperatur nicht sicherheitsbezogen erfasst.

Der Temperaturzustand darf als zusätzliches Abschaltkriterium benutzt werden.

Der Anwender hat durch geeignete Maßnahmen sicher zu stellen, dass die für das System spezifizierten Grenzen für die Umgebungstemperatur eingehalten werden.

3.4.8 Umgebungsbedingungen

Für den Einsatz des sicherheitsbezogenen Automatisierungssystems HIQuad X 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 4: 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

HIQuad X 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 HIQuad X erfüllt die in diesem Kapitel aufgelisteten Normen.

3.6.1 CE-Konformitätserklärung

Das Automatisierungssystem HIQuad X 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 HIQuad X für Anwendungen gemäß den Normen zur Funktionalen Sicherheit geprüft und zertifiziert. Das sicherheitsbezogene Automatisierungssystem HIQuad X trägt das folgende Prüfzeichen:

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

EG-Baumusterprüfbescheinigung
Sicherheitsbezogenes programmierbares System
HIQuad X

3.6.3 Normenspiegel

Das sicherheitsbezogene Automatisierungssystem HIQuad X 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 [1)]	PL e
EN 62061:2005 + AC:2010 + A1:2013 + A2:2015	SIL CL 3
EN 50156-1:2015	SIL 3
EN 12067-2:2004	---
EN 298:2012	---
EN 60079-0:2012 + A11:2013	---
EN 60079-11:2012	---
EN 60079-15:2010	---
NFPA 72:2016	---
NFPA 85:2015	---
NFPA 86:2015	---
EN 61131-2:2007	Zone B
EN 61131-6:2012	---
EN 61326-3-1:2017	---
EN IEC 61326-3-2:2018	---
EN 54-2:1997 + AC:1999 + A1:2006 [2)]	---
EN 50130-4:2011 + A1:2014 [2)]	---
EN 61000-6-7:2015	---

1) Ausnahme: Die F 3430 ist nicht nach EN ISO 13849-1 zertifiziert.

2) Ausnahme: Die F 3330 ist für Applikationen gemäß dieser Normen nicht einsetzbar.

Tabelle 5: Internationale Normen und Sicherheitsstufen

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

3.6.4 Prüfbedingungen

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

Norm	Inhalt
IEC/EN 61131-2 Zone B	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 61326-3-2	Elektrische Mess-, Steuer-, Regel- und Laborgeräte - EMV-Anforderungen Teil 3-2: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) - Industrielle Anwendungen in spezifizierter elektromagnetischer Umgebung.
EN 50130-4	Alarmanlagen, Teil 4: Elektromagnetische Verträglichkeit - Produktfamiliennorm: Anforderungen an die Störfestigkeit von Anlageteilen für Brandmeldeanlagen, Einbruch- und Überfallmeldeanlagen, Video-Überwachungsanlagen, Zutrittskontrollanlagen sowie Personen-Hilferufanlagen
EN 54-2	Brandmelderzentralen

Tabelle 6: Normen für EMV-, Klima- und Umweltanforderungen

Für sicherheitsbezogene Systeme werden erhöhte Pegel bei der Störbeeinflussung gefordert. HIQuad X 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 7: 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 8: Klimatische Prüfungen

3.6.4.2 Mechanische Prüfungen

Die wichtigsten Prüfungen und Grenzwerte für die mechanische 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, HIQuad X in Betrieb, 3 Schocks pro Achse und Richtung (18 Schocks).

Tabelle 9: 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: ▪ IEC 61131-2. ▪ SELV (Safety Extra Low Voltage). ▪ PELV (Protective Extra Low Voltage).
	Die Absicherung des HIQuad X Systems muss gemäß den Angaben in den Datenblättern erfolgen.
	Prüfung des Spannungsbereichs: 24 VDC, -20 … +25 % (19,2 … 30,0 VDC).
	Prüfung auf Unempfindlichkeit gegen Kurzzeitunterbrechung der externen Stromversorgung: DC, PS 2: 10 ms.
	Polaritätsumkehr der Versorgungsspannung.
	Pufferdauer, Beständigkeitsprüfung: Prüfung A, 300 h bei 60 C, Goldcap für Datum/Uhrzeit.

Tabelle 10: Nachprüfung der Gleichstromversorgungs-Eigenschaften

4 Prozessormodul (F-CPU 01)

Das sicherheitsbezogene Prozessormodul besteht aus zwei Mikroprozessoren mit je einem RAM-Speicher, welche gleichzeitig dieselben Programme, Betriebssysteme 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 viele weitere Selbst-Tests, wie die Überwachung des Programmablaufs (Watchdog) durch.

4.1 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-flüchtiger Speicher).
- Der Watchdog.
- Die E/A-Busse innerhalb der Steuerung.
- Die Spannungsversorgung.

4.2 Reaktionen auf Fehler im Prozessorsystem

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, Ausgänge werden energielos.

4.3 Austausch von Prozessormodulen

Vor dem Austausch von Prozessormodulen ist darauf zu achten, dass ein noch laufendes HIQuad X 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 das redundante 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.

Zu Einzelheiten über den Austausch von Prozessormodulen wird auf die Handbücher des Prozessormoduls, HI 803 214 D, und auf das Systemhandbuch HI 803 210 D verwiesen.

5 Kommunikationsmodul (F-COM 01)

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

- Das Prozessormodul steuert den sicherheitsbezogenen Datenaustausch mit den SIL 3-zertifizierten Übertragungsprotokollen safe**ethernet** und HIPRO-S V2. Das Kommunikationsmodul leitet die Daten an die verbundenen HIMA Steuerungen weiter. Durch das sicherheitsbezogene Protokoll safe**ethernet** 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 dem Kommunikationshandbuch HI 801 100 D zu entnehmen.

Näheres zu Kommunikation und Kommunikationsmodulen siehe folgende Dokumente:

- Kapitel 11.1 dieses Handbuchs.
- Handbuch des Kommunikationsmoduls HI 803 222 D.
- Kommunikationshandbuch HI 801 100 D.
- Systemhandbuch HI 803 210 D.

6 E/A-Verarbeitungsmodul (F-IOP 01)

Im HIQuad X System kommunizieren E/A-Verarbeitungsmodule über die beiden sicherheitsbezogenen Systembusse mit den Prozessormodulen im Basis-Rack. Zusätzlich verwaltet das E/A-Verarbeitungsmodul den internen E/A-Bus des Racks, in dem es sich befindet.

Über die Systembusse werden die Daten mit Hilfe eines sicherheitsbezogenen Protokolls übertragen. Es ist möglich, ein HIQuad X System, das **nur ein Prozessormodul** enthält, bei verminderter Verfügbarkeit mit nur einem Systembus zu betreiben.

E/A-Verarbeitungsmodule können nicht redundant verschaltet werden. Wird auf der E/A-Ebene Redundanz benötigt, ist ein redundantes Erweiterungs-Rack erforderlich. Die verschiedenen Konzepte des HIQuad X Systems sind dem Systemhandbuch HI 803 210 D zu entnehmen.

Das sicherheitsbezogene E/A-Verarbeitungsmodul ist mit einem 1oo2-Prozessorsystem (HICore 2) ausgestattet. Ein Hardware-Vergleicher führt ständig einen Abgleich der Daten der internen Mikroprozessoren und der Speicher durch. Das E/A-Verarbeitungsmodul meldet auftretende Differenzen und geht automatisch in den Zustand FEHLERSTOPP.

E/A-Verarbeitungsmodule überwachen die 5-V-Spannungsversorgung der Racks, auf denen sie gesteckt sind. Bei Unterschreitung der Mindestspannung schalten E/A-Verarbeitungsmodule die E/A-Ebene des eigenen Racks ab.

E/A-Verarbeitungsmodule testen und überwachen die E/A-Module in einem Rack und signalisiert deren Zustände. Zusätzlich stellen E/A-Verarbeitungsmodule das Watchdog-Signal für die Ausgangsmodule bereit.

E/A-Verarbeitungsmodule stellen dem Anwenderprogramm die Eingangswerte der E/A-Module eines Racks zur Verfügung. Die Ausgangswerte aus dem Anwenderprogramm werden an das E/A-Verarbeitungsmodul gesendet und von diesem in die Ausgangsmodule geschrieben. Die Ausgangsmodule steuern damit die Feldebene z. B. Aktoren an.

6.1 Selbst-Tests

Das Betriebssystem des E/A-Verarbeitungsmoduls 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.
- Die E/A-Busse.
- Die 5-V-Versorgungsspannung
- Die internen Spannungen.

6.2 Reaktionen im Fehlerfall

Bei Störung auf einem Systembus erfolgt die Kommunikation über den redundanten Systembus, sofern beide Systembusse eingerichtet wurden.

Bei Mono-Betrieb des Systems mit nur einem Prozessormodul ist die Verfügbarkeit des redundanten Systembusses nicht gegeben.

Bei Störungen auf dem E/A-Bus werden keine Prozessdaten übertragen. Dem System steht die E/A-Ebene nicht mehr zur Verfügung.

Das Modul signalisiert Fehler mit den LEDs auf der Frontplatte.

Bei Fehler werden alle im Erweiterungs-Rack gesteckten Ausgangsmodule über den zweiten Abschaltweg in den sicheren Zustand gebracht. Die Daten der Eingangsmodule werden nicht mehr versendet.

6.3 Reaktionen auf Fehler im Prozessorsystem

Das E/A-Verarbeitungsmodul meldet auftretende Differenzen des Hardware-Vergleichers und geht automatisch in den Zustand FEHLERSTOPP, dies gilt auch für den Ausfall des Hardware-Vergleichers.

Ein Hardware-Vergleicher innerhalb des E/A-Verarbeitungsmodul vergleicht ständig, ob die Daten des internen Mikroprozessors1 identisch sind mit den Daten des Mikroprozessors 2. Ist das nicht der Fall, oder finden die Test-Routinen einen Fehler im E/A-Verarbeitungsmodul, geht das E/A-Verarbeitungsmodul automatisch in FEHLERSTOPP.

6.4 Rack-ID

Die Rack-ID wird benötigt, um die einzelnen Racks innerhalb eines Systems eindeutig zu identifizieren. Die Rack-ID wird über einen 10-poligen DIP-Schalter auf dem E/A-Verarbeitungsmodul eingestellt. Jedem Rack ist eine eindeutige Rack-ID zuzuordnen, die mit der Konfiguration in SILworX übereinstimmen muss. Das Basis-Rack H51X hat die Rack-ID 0, da in das Rack kein E/A-Verarbeitungsmodul gesteckt wird. Die Rack-IDs und der DIP-Schalter sind im Handbuch des E/A-Verarbeitungsmoduls (HI 803 218 D) beschrieben.

Die Rack-ID ist der **Sicherheitsparameter** für die Adressierung der Racks und der in den Racks gesteckten Modulen.

6.5 Service-Mode

Das E/A-Verarbeitungsmodul ist mit einem Service-Mode ausgestattet. Dieser ermöglicht dem Anwender den Austausch von E/A-Modulen eines Racks im laufenden Betrieb, ohne dabei die gesamte E/A-Ebene eines Racks abzuschalten. Für den Austausch von E/A-Modulen im laufenden Betrieb muss der Service-Mode des E/A-Verarbeitungsmoduls aktiviert sein.

Bei aktiviertem Service-Mode werden E/A-Modul-Fehler, die ein Abschalten des betroffenen Racks fordern, unterdrückt. Das System meldet für das betroffene Rack eine Warnung. Diese Warnung wird über die Rack-Verbindungsanzeige der Prozessormodule signalisiert.

i Bei aktiviertem Service-Mode ist die Abschaltung über den E/A-Watchdog (2. Abschaltweg) blockiert! Die Ausgangsmodule können darüber nicht in den sicheren Zustand gebracht werden.

Der Service-Mode wird entweder über den Service-Taster (SERV) auf der Frontseite des E/A-Verarbeitungsmodules aktiviert/deaktiviert oder über ein PADT-Kommando.

Der Service-Mode wird 24 h nach Aktivierung automatisch beendet, sofern er nicht zuvor manuell beendet wurde.

Deaktiviert der Anwender den Service-Mode, bleibt der Service–Mode solange aktiv, bis die getauschten oder fehlerhafte E/A-Module initialisiert sind und kein Modul nach der Initialisierung einen Fehler meldet. Nach 24 h wird der Service-Mode durch das System deaktiviert.

Bei automatischer Deaktivierung des Service-Modes, 24 Stunden nach Aktivierung, werden keine E/A-Module neu initialisiert. Sind im Rack weiterhin Fehler vorhanden, die ein Abschalten des Racks erforderlich machen (z. B. fehlendes Ausgangsmodul), wird der E/A-Watchdog (2. Abschaltweg) abgeschaltet und alle Ausgangsmodule des Racks in den sicheren Zustand überführt.

Der SERV-Taster kann durch den Systemparameter *Service-Mode-Taster deaktivieren* gesperrt werden. Wenn der SERV-Taster durch das Anwenderprogramm gesperrt ist, dann kann der Service-Mode nur über ein PADT-Kommando gesteuert werden.

Austausch von E/A-Modulen

1. Den Service-Taster (SERV) auf dem E/A-Verarbeitungsmodul (F-IOP 01), das sich im Rack der zu tauschenden E/A-Modulen befindet, zwischen 2 s und 7 s drücken. Oder das E/A-Verarbeitungsmodul mit dem PADT-Kommando «*Service-Mode starten»* auswählen, um in den Service-Mode des Moduls zu wechseln.
   - ☑ Der Systemparameter *Service-Mode aktiv* ist TRUE.
   - ☑ Schrittresultat (optional). Die LEDs *Slot* und *Chn* blinken rot, wenn sich das E/A-Verarbeitungsmodul im Service-Mode befindet.
2. Befestigungsschrauben des zu tauschenden E/A-Moduls vollständig lösen.
3. Kabelstecker abschrauben oder E/A-Modul zusammen mit aufgestecktem Kabelstecker ziehen.
4. Neues E/A-Modul ohne Kabelstecker einstecken und verschrauben. Die Beschreibung im Systemhandbuch beachten!
5. Kabelstecker aufstecken und verschrauben.
6. Arbeitsschritte 2 … 5 für jedes weitere zu tauschende Modul wiederholen.
7. Service-Taster (SERV) auf dem E/A-Verarbeitungsmodul (F-IOP 01) zwischen 2 s und 7 s drücken oder den Service-Mode mit dem PADT-Kommando «Beenden des *Service-Mode einleiten»* deaktivieren.
   - ☑ Der Systemparameter Service-Mode aktiv ist FALSE.
   - ☑ Die LEDs des E/A-Verarbeitungsmoduls signalisieren reguläre Modul und Kanal-Diagnosen.

► Die E/A-Module sind getauscht und wieder in fehlerfreiem Betrieb.

Weitere Details zum Service-Mode sind dem Handbuch der F-IOP 01 (HI 803 218 D) zu entnehmen.

7 Eingangsmodule

Nachfolgende Tabelle gibt eine Übersicht über die Eingangsmodule des HIQuad X Systems:

Digitale Eingangsmodule [1)]	Kanäle	Sicherheitsbezogen	(Ex)i
F 3221	16	---	---
F 3224A	4	---	X
F 3236	16	X	---
F 3237	8	X	---
F 3238	8	X	X
F 3240	16	X	---
F 3248	16	X	---
Analoge Eingangsmodule [1)]	Kanäle	Sicherheitsbezogen	(Ex)i
F 6215	8	---	---
F 6217	8	X	---
F 6220	8	X	X
F 6221	8	X	X
Zählermodul [1)]	Kanäle	Sicherheitsbezogen	(Ex)i
F 5220	2	X	

[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 11: 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 F 5220, F 6217, F 6220 und F 6221 sind mit einem eigenen 1oo2-Prozessorsystem ausgestattet, das der erhöhten Komplexität der Module Rechnung trägt. Das 1oo2-Prozessorsystem dieser Module führt während des Betriebs automatisch sicherheitsbezogene Tests durch und übermittelt die sicheren Daten an das E/A-Verarbeitungsmodul.

Die sicherheitsbezogenen Eingangsmodule ohne Prozessorsystem werden während des Betriebes automatisch einem hochwertigen, zyklischen Selbst-Test unterzogen. Die Eingangsmodule enthalten Schaltungsteile, die einen Test der Modulfunktion über spezielle im Betriebssystem (E/A-Verarbeitungsmodul) integrierte Test-Routinen ermöglichen. Diese Test-Routinen stellen die korrekte Funktion des jeweiligen Eingangsmoduls sicher.

Werden bei den Selbst-Tests Fehler erkannt führt dies automatisch zu einer sicherheitsbezogenen Reaktion des E/A-Verarbeitungsmoduls und zu entsprechenden Fehlermeldungen. Die detaillierten Fehlermeldungen können im Anwenderprogramm durch das Auslesen der Fehlercodes ausgewertet werden.

In HIQuad X haben die Eingangsmodule das Verhalten automatischer Wiederanlauf. Sobald ein erkannter Fehler nicht mehr ansteht, verarbeiten die Eingangsmodule automatisch wieder eingehende Werte. Im Gegensatz dazu muss in HIQuad erst der ACK-Taster gedrückt werden. Das Verhalten automatischer Wiederanlauf kann in SILworX deaktiviert werden.

Für die ordnungsgemäße Funktion der Module sind die HIMA Kabelstecker zu verwenden.

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 parametriert sein (Standardwert = 0).

Zusätzlich zur Anzeige der LEDs *Slot* und *Chn* auf dem E/A-Verarbeitungsmodule werden Fehlermeldungen und Statusmeldungen erzeugt und auf dem Prozessormodul gespeichert. Mit dem PADT können diese aus dem Diagnose-Speicher ausgelesen werden.

Zur Erhöhung der Verfügbarkeit sind die sicherheitsbezogenen Eingangsmodule auch redundant einsetzbar. Redundante Eingangsmodule beeinträchtigen die Sicherheit des Systems nicht, siehe Kapitel 3.1.1.

Die Fehlermeldungen, die Statusmeldungen und die Systemvariablen können zur Programmierung von anwenderspezifischen Fehlerreaktionen verwendet werden. Einzelheiten sind dem Handbuch des jeweiligen Moduls zu entnehmen.

7.3 Sicherheit von Sensoren, Encoder 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 E/A-Störaustastung

Bei aktivierter Störaustastung reagiert das System nicht auf transiente Störungen. In diesem Fall schalten die Störungen die Ausgänge nicht sofort energielos und haben auch keine Auswirkung auf die Datenquellen.

Weitere Informationen zur Störaustastung finden Sie im Systemhandbuch HI 803 210 D.

Die Störaustastung wirkt nur innerhalb der Sicherheitszeit der Ressource und nur dann, wenn die Sicherheitszeit der Ressource ≥ 3 × Watchdog-Zeit der Ressource ist.

i Für die Eingangsmodule F 5220, F 6220 und F 6221 ist die Störaustastung immer aktiviert und kann nicht deaktiviert werden. Das Aktivierungsfeld in SILworX ist ausgegraut und ohne Funktion.

7.5 Sicherheitsbezogene digitale Eingangsmodule F 3236, F 3237, F 3238, F 3240 und F 3248

Die Eingangsmodule lesen die digitalen Signale an den Eingängen ein und liefern in jedem Zyklus des Prozessormoduls sichere Werte an das Anwenderprogramm.

7.5.1 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 einem Fehler wird für jeden Eingang der Initialwert verarbeitet.

Die Eingangsmodule für Näherungsschalter und für Kontaktgeber mit Leitungsüberwachung testen zusätzlich die Leitung bis zum Geber. An diese Module können sicherheitsbezogene Näherungsschalter angeschlossen werden. Durch die Selbst-Tests werden alle Anforderungen an die Erkennung der Schwellen sicherheitsbezogener Näherungsschalter erfüllt.

Die Überwachung des Geberstromes eines Kontaktgebers erfordert die Beschaltung mit zwei Widerständen gemäß Handbuch.

7.5.2 Redundanz von digitalen Eingängen

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

7.5.3 Surge auf digitalen Eingängen

Durch die kurze Zykluszeit der HIQuad X 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.
- Störaustastung im Anwenderprogramm programmieren. Ein Signal muss mindestens zwei Zyklen anstehen, bevor es ausgewertet wird. Die Fehlerreaktion erfolgt entsprechend verzögert.

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 803 210 D und der relevanten Normen.

7.6 Sicherheitsbezogenes Zählermodul F 5220

Das zweikanalige Zählermodul hat ein eigenes 1oo2-Prozessorsystem mit einem sicherheitsbezogenen Ausgang pro Kanal. Das Modul kann, abhängig von seiner Konfiguration, für die Erfassung folgender Prozesswerte eingesetzt werden:

- Impulszählung.
- Frequenzmessung oder Drehzahlmessung über eine einstellbare Torzeit.
- Grenzwertüberwachung durch zyklus-unabhängigen Ausgangsbetrieb mit Vergleichsfunktionen.
- Drehrichtungserkennung.

Das Zählermodul verarbeitet Impulse sicherheitsbezogen bis zu einer Frequenz von:

$$\mathbf{f_{max} = 2^{22} / (t_{SR} + 100\ ms)}$$

Die Sicherheitszeit der Ressource $\mathbf{t_{SR}}$ in der Betriebsart *Impulszählung* ist abhängig von der maximalen Frequenz $\mathbf{f_{max}}$ bis zu der die Zählereingänge sicherheitsbezogen betrieben werden dürfen:

$$\mathbf{t_{SR} = (2^{22} / f_{max}) - 100\ ms}$$

Bei Änderungen der Torzeit steht der korrekte Messwert erst nach drei Torzeiten am Ausgang zur Verfügung!

Das Zählermodul benötigt für den Betrieb das E/A-Watchdog-Signal nicht. Das Ausbleiben des E/A-Watchdog-Signals hat weder eine Auswirkung auf die Funktion des Zählermoduls noch auf deren Schaltausgänge.

Weitere Einzelheiten siehe Modulhandbuch HI 803 065 D.

7.6.1 Test-Routinen

Das Modul hat ein eigenes 1oo2-Prozessorsystem, das sicherheitsbezogene Selbst-Tests automatisch durchführt und die Daten dem Anwenderprogramm bereitstellt.

Stellen die Test-Routinen einen Modulfehler fest, werden die beiden sicherheitsbezogenen Ausgänge abgeschaltet. Bei einem Kanalfehler wird der dem Kanal zugeordnete sicherheitsbezogene Ausgang abgeschaltet.

7.6.2 Verhalten bei Leitungsbruch und Leitungsschluss

Wenn an einem Zählereingang ein Leitungsschluss oder Leitungsbruch festgestellt wird, dann schaltet das Modul den zugeordneten sicherheitsbezogenen Ausgang ab. Der Parameter *-> Prozesswert OK [BOOL]* wird auf FALSE gesetzt.

7.6.3 Redundanz von Zählereingängen

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

Eine Redundanzverknüpfung zweier Zählermodule muss über das Anwenderprogramm realisiert werden, da SILworX das Anlegen einer Redundanzgruppe für das Zählermodul nicht unterstützt.

7.6.4 Projektierungshinweise

Bei der Projektierung des Moduls sind die folgenden Punkte zu beachten:

- Die Störaustastung ist immer aktiv. Innerhalb der Störaustastung auftretende Impulse werden nicht gezählt. Für den sicherheitsbezogenen Betrieb muss der Parameter *Restart sperren [BOOL] ->* auf TRUE gesetzt werden.
- Testbetrieb wird im Hardware-Editor parametriert und ist ausschließlich während der Inbetriebnahme oder zu Testzwecken erlaubt.
  Im Regelbetrieb dürfen die folgenden, für den Testbetrieb vorgesehenen Parameter im Anwenderprogramm nicht verwenden werden:
  - *Testbetrieb [BOOL] ->*
  - *Maximalzeit Testbetrieb [ms]* > 0
  - *-> Restzeit Testbetrieb [s] [UDINT]*
  - *Force-Wert aktiv [BOOL] ->*
- Die Leitungsüberwachung wird nur in der Betriebsart *Näherungsschalter-Impulse* durchgeführt. Wird an den Zählereingängen ein Leitungsschluss oder Leitungsbruch erfasst, dann wird der entsprechende Parameter *-> LS [BOOL]* oder *-> LB [BOOL]* auf TRUE gesetzt.

7.7 Sicherheitsbezogenes analoges Eingangsmodul F 6217

Das Modul hat ein eigenes 1oo2-Prozessorsystem, das sicherheitsbezogene Selbst-Tests automatisch durchführt und die Daten dem Anwenderprogramm bereitstellt. Für jeden Kanal existiert der Analogwert als Rohwert (Datentyp DINT) und als skalierter Prozesswert (Datentyp REAL).

7.7.1 Test-Routinen

Das Modul schaltet über einen D/A-Wandler Testwerte auf und prüft diese über den A/D-Wandler, mit dem auch das Eingangssignal digitalisiert wird.

7.7.2 Redundanz von analogen Eingängen

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

Wenn zwei Eingänge redundant konfiguriert sind, dann wird der größere der beiden skalierten Werte in den redundanten Systemparameter *-> Prozesswert [REAL]* geschrieben. Voraussetzung dafür ist der fehlerfreie Betrieb beider Module. Im Fehlerfall wird nur der Wert des funktionsfähigen Moduls verarbeitet. Voraussetzung dafür ist eine für beide Eingänge identische Signalquelle, z. B. ein Messwert. Abweichung zwischen den beiden gemessenen Werten ist nur innerhalb der sicherheitstechnischen Messgenauigkeit erlaubt.

7.7.3 Projektierungshinweise

Für die sicherheitsbezogenen Verwendung müssen die Grenzwerte für Leitungsschluss und Leitungsbruch in SILworX pro Kanal eingestellt werden. HIMA empfiehlt, die voreingestellten NAMUR-Werte für Leitungsbruch (3,6 mA) und für Leitungsschluss (21 mA) beizubehalten.

Eine sicherheitsbezogene Auswertung ist nur innerhalb von 0 … 21 mA zulässig. Die Messgenauigkeit außerhalb dieses Bereiches kann nicht garantiert werden kann.

Der Parameter -> *Prozesswert [REAL]* übernimmt bei Verletzung der eingestellten Grenzwerte und bei internen Kanalfehlern automatisch den eingestellten Initialwert. Der Anwender muss im Anwenderprogramm sicherstellen, dass dieser Initialwert zum sicheren Zustand der jeweiligen Sicherheitsfunktion führt.

Die Verwendung des Parameters -> *Rohwert [1 mA = 10 000] [DINT]* ist nur unter folgenden Bedingungen zulässig:

1. Messbereich 0 … 21 mA
2. Zusätzliche Auswertung des Parameters -> *Prozesswert OK [BOOL]* im Anwenderprogramm. FALSE muss zum sicheren Zustand der jeweiligen Sicherheitsfunktion führen.
3. Auswertung der Grenzwerte für Leitungsbruch und Leitungsschluss, da der Parameter -> *Prozesswert OK [BOOL]* bei Verletzung der eingestellten Grenzen automatisch auf FALSE wechselt. Alternativ können die Grenzwerte auch im Anwenderprogramm ausgewertet werden.
4. Programmierung eines Ersatzwertes (Initialwert) im Anwenderprogramm, der zum sicheren Zustand der jeweiligen Sicherheitsfunktion führt.

7.8 Sicherheitsbezogenes analoges Eingangsmodul F 6220

Das analoge Eingangs-/Temperaturmodul hat 8 Kanäle zum Anschluss von Thermoelementen verschiedener Typen und einen Vergleichstemperatur-Eingang zum Anschluss eines Widerstandsthermometers Pt100.Die Kanäle sind in der Zündschutzart Eigensicherheit ausgeführt und sicher vom Ausgangs- und Versorgungsstromkreis getrennt. Das Modul ist mit einem eigenen 1oo2-Prozessorsystem ausgestattet.

Die Eingänge sind auch zur Messung von niedrigen Spannungen verwendbar, siehe Handbuch.

7.8.1 Test-Routinen

Das Modul hat ein eigenes 1oo2-Prozessorsystem, das sicherheitsbezogene Selbst-Tests automatisch durchführt und die Daten dem Anwenderprogramm bereitstellt. Jeder der 9 Kanäle (8 + 1) liefert sichere Eingangswerte und einen sicheren Fehlerstatus.

7.8.2 Redundanz von analogen Eingangsmodulen F 6220

Die redundante Verschaltung von analogen Eingängen zum Anschluss von Thermoelementen ist nicht zulässig. Bei Redundanz Verschaltung zweier Eingangsmodule muss jeder Eingangskanal mit einem eigenen Thermoelement verschaltet werden.

Eine redundante Verschaltung wird für die Verfügbarkeit der Eingänge verwendet.

Wenn zwei Eingänge redundant konfiguriert sind, dann wird der größere der beiden skalierten Werte in den redundanten Systemparameter *-> Prozesswert [REAL]* geschrieben. Voraussetzung dafür ist der fehlerfreie Betrieb beider Module. Im Fehlerfall wird nur der Wert des funktionsfähigen Moduls verarbeitet. Voraussetzung dafür ist eine für beide Eingänge identische Signalquelle, z. B. ein Messwert. Abweichung zwischen den beiden gemessenen Werten ist nur innerhalb der sicherheitstechnischen Messgenauigkeit erlaubt.

7.8.3 Projektierungshinweise

Für die sicherheitsbezogene Verwendung müssen, die in SILworX voreingestellten Grenzwerte für Leitungsschluss und Leitungsbruch gemäß ihrer Anwendung eingestellt werden. Die Grenzwerte müssen für jeden Kanal einzeln eingestellt werden.

Eine sicherheitsbezogene Auswertung in der Anwendung Spannungseingang ist nur innerhalb von -100 … +100 mV zulässig. Die Messgenauigkeit außerhalb des Bereichs kann nicht garantiert werden.

Eine sicherheitsbezogene Auswertung für Thermoelemente ist nur innerhalb deren überwachten Gebrauchsbereiche zulässig, siehe Datenblatt der F 6220. Die Messgenauigkeit außerhalb dieser Gebrauchsbereiche kann nicht garantiert werden. Zusätzlich muss der Referenztemperaturbereich des Pt100 (-40 … +80 °C) eingehalten werden.

Der Parameter *-> Prozesswert [REAL]* übernimmt bei Verletzung der eingestellten Grenzwerte und bei internen Kanalfehlern automatisch den eingestellten Initialwert. Der Anwender muss im Anwenderprogramm sicherstellen, dass dieser Initialwert zum sicheren Zustand der jeweiligen Sicherheitsfunktion führt.

Die Verwendung des Parameters *-> Rohwert [1 °C/ 1 mV = 10 000] [DINT]* ist nur unter folgenden Bedingungen zulässig:

1. Der Messbereich bei Spannungseingang oder bei den Thermoelementen wird eingehalten. Der Referenztemperaturbereich des Pt100 -40 … +80 °C wird eingehalten.
2. Zusätzliche Auswertung des Parameters *-> Prozesswert OK [BOOL]* im Anwenderprogramm. FALSE muss zum sicheren Zustand der jeweiligen Sicherheitsfunktion führen.
3. Auswertung der Grenzwerte für Leitungsbruch und Leitungsschluss, da der Parameter *-> Prozesswert OK [BOOL]* bei Verletzung der eingestellten Grenzen automatisch auf FALSE wechselt. Alternativ können die Grenzwerte auch im Anwenderprogramm ausgewertet werden.

4. Programmierung eines Ersatzwertes (Initialwert) im Anwenderprogramm, der zum sicheren Zustand der jeweiligen Sicherheitsfunktion führt.

Weiterhin sind die folgenden Punkte zu beachten:

- Nicht benutzte Eingänge sind kurzzuschließen.
- Die Referenztemperatur für den Betrieb gemäß SIL 3 ist direkt aus dem Anwenderprogramm heranzuziehen oder aus dem Vergleich zweier Module im Anwenderprogramm zu ermitteln.
- Die Temperatur der Thermoelemente ist für SIL 3 jeweils als Vergleich zweier Thermoelemente zu ermitteln.
- Es sind alle denkbaren Abweichungen zu betrachten und in der Auswertung der Messwerte zu berücksichtigen.

7.9 Sicherheitsbezogenes analoges Eingangsmodul F 6221

Das analoge Eingangsmodul hat 8 Kanäle zum direkten Anschluss von analogen Transmittern aus dem Ex-Bereich. Die Kanäle sind in der Zündschutzart Eigensicherheit ausgeführt und sicher vom Ausgangs- und Versorgungsstromkreis getrennt. Die Versorgung mit der Transmitter-Speisespannung kann durch das Speisemodul F 3325 oder eine andere Spannungsversorgung entsprechend den Datenblattvorgaben erfolgen. Diese Transmitter-Speisespannung ist zur Überwachung über das Modul F 6221 anzuschließen.

7.9.1 Test-Routinen

Das Modul hat ein eigenes 1oo2-Prozessorsystem, das sicherheitsbezogene Selbst-Tests automatisch durchführt und die Daten dem Anwenderprogramm bereitstellt. Jeder der 8 Kanäle liefert sichere Eingangswerte und einen sicheren Fehlerstatus.

7.9.2 Redundanz von analogen Eingängen

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

Wenn zwei Eingänge redundant konfiguriert sind, dann wird der größere der beiden skalierten Werte in den redundanten Systemparameter -> *Prozesswert [REAL]* geschrieben. Voraussetzung dafür ist der fehlerfreie Betrieb beider Module. Im Fehlerfall wird nur der Wert des funktionsfähigen Moduls verarbeitet. Voraussetzung dafür ist eine für beide Eingänge identische Signalquelle, z. B. ein Messwert. Abweichung zwischen den beiden gemessenen Werten ist nur innerhalb der sicherheitstechnischen Messgenauigkeit erlaubt.

7.9.3 Projektierungshinweise

Für die sicherheitsbezogenen Verwendung müssen die Grenzwerte für Leitungsschluss und Leitungsbruch in SILworX pro Kanal eingestellt werden. HIMA empfiehlt, die voreingestellten NAMUR-Werte für Leitungsbruch (3,6 mA) und für Leitungsschluss (21 mA) beizubehalten.

Eine sicherheitsbezogene Auswertung ist nur innerhalb des Messbereichs -2 … +22 mA zulässig. Die Messgenauigkeit außerhalb dieses Bereichs kann nicht garantiert werden.

Der Parameter -> *Prozesswert [REAL]* übernimmt bei Verletzung der eingestellten Grenzwerte und bei internen Kanalfehlern automatisch den eingestellten Initialwert. Der Anwender muss im Anwenderprogramm sicherstellen, dass dieser Initialwert zum sicheren Zustand der jeweiligen Sicherheitsfunktion führt.

Die Verwendung des Parameters -> *Rohwert [1 mA = 10 000] [DINT]* ist nur unter folgenden Bedingungen zulässig:

1. Messbereich -2 … 22 mA
2. Zusätzliche Auswertung des Parameters -> *Prozesswert OK [BOOL]* im Anwenderprogramm. FALSE muss zum sicheren Zustand der jeweiligen Sicherheitsfunktion führen.
3. Auswertung der Grenzwerte für Leitungsbruch und Leitungsschluss, da der Parameter -> *Prozesswert OK [BOOL]* bei Verletzung der eingestellten Grenzen automatisch auf FALSE wechselt. Alternativ können die Grenzwerte auch im Anwenderprogramm ausgewertet werden.
4. Programmierung eines Ersatzwertes (Initialwert) im Anwenderprogramm, der zum sicheren Zustand der jeweiligen Sicherheitsfunktion führt.

Weiterhin sind die folgenden Punkte zu beachten:

- Nicht benutzte Spannungseingänge 0 … 1 V sind auf der Klemmleiste kurzzuschließen.
- Nicht benutzte Stromeingänge sind durch den Shunt im Kabelstecker abgeschlossen.
- Nur die im Datenblatt der F 6221 aufgeführten Verwendungen sind zulässig.
- Die Ex-Schutzbestimmungen und Ex-Anschlussbedingungen sind einzuhalten.

7.10 Checkliste für sicherheitsbezogene Eingänge

HIMA empfiehlt, die verfügbaren Checklisten zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsbezogenen Eingängen einzusetzen. Die Checkliste ist als Planungsunterlage einsetzbar und dient gleichzeitig auch als Nachweis für eine sorgfältige 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 stellt HIMA die Checklisten im Download-Bereich https://www.hima.com/de/downloads/ zur Verfügung.

8 Ausgangsmodule

Nachfolgende Tabelle zeigt eine Übersicht der HIQuad X Ausgangsmodule:

Digitale Ausgangsmodule[1)]	Kanäle	Sicherheitsbezogen	Belastbarkeit
F 3322	16	---	≤ 0,5 A
F 3330	8	X	≤ 0,5 A
F 3331	8	X	≤ 0,5 A
F 3333	4	X	≤ 2 A
F 3334	4	X	≤ 2 A
F 3335	4 (Ex)i	X	22 V ≤ 0,053 A
F 3349	8	X	≤ 48 V ≤ 0,5 A
Relaismodule[1)]	Kanäle	Sicherheitsbezogen	Belastbarkeit
F 3422	8	---	≤ 60 V ≤ 2 A
F 3430	4	X	≤ 250 V ≤ 4 A
Analoge Ausgangsmodule[1)]	Kanäle	Sicherheitsbezogen	Belastbarkeit
F 6705	2	X	0 … 20 mA
F 6706	2	---	0 … 20 mA

[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 12: Übersicht Ausgangsmodule

8.1 Allgemein

Die sicherheitsbezogenen Ausgangsmodule schreiben einmal in jedem Zyklus die vom Anwenderprogramm erzeugten Werte auf die Ausgänge. Die Ausgangssignale werden zurückgelesen und mit den vorgegebenen Ausgangsdaten verglichen.

Zusätzlich werden Tests im Hintergrund über alle Ausgänge durchgeführt, bei denen eingeschaltete Kanäle kurzzeitig abgeschaltet und ausgeschaltete Kanäle kurzzeitig eingeschaltet werden. Die Testimpulse stehen bei den Modulen F 3330, F 3333, F 3335 und F 3430 250 µs lang an. Bei den Modulen F 3331 und F 3334 und F 3349 ist die Testimpulsdauer und das Testintervall einstellbar, siehe HIQuad X Modulhandbücher.

Mit diesen Tests wird die Schaltbarkeit der Ausgänge geprüft, ohne die Funktion der angeschlossenen Aktoren zu beeinflussen, falls die angeschlossenen Aktoren die Testdauer von 250 µs tolerieren. Ein Einfrieren (Verschweißen der Schalter) jedes Ausgangs wird erkannt, auch wenn das Ausgangssignal statisch ist.

In HIQuad X haben die Ausgangsmodule das Verhalten automatischer Wiederanlauf. Sobald ein erkannter Fehler nicht mehr ansteht, geben die Ausgangsmodule automatisch die im Anwenderprogramm erzeugten Werte wieder auf die Ausgänge. Im Gegensatz dazu muss in HIQuad erst der ACK-Taster gedrückt werden. Das Verhalten automatischer Wiederanlauf kann in SILworX deaktiviert werden.

Bei Ausgangsmodulen mit Leitungsüberwachung ist bei Anschluss von Induktivitäten oder Lampenlasten die Einstellung der Testimpulsdauer zu überprüfen und gegebenenfalls zu verlängern. Bei den Ausgängen ist der Wert «0» oder der geöffnete Relaiskontakt der sichere Zustand.

Für die ordnungsgemäße Funktion der Module sind die HIMA Kabelstecker zu verwenden.

8.2 Reaktion im Fehlerfall

Die Vorder- und Hintergrundtests der Ausgangsmodule liefern folgende Reaktionen im Fehlerfall:

- Ein Modulfehler führt immer zur Abschaltung des Moduls und dessen Ausgänge in den sicheren energielosen Zustand.
- Ein von der F-IOP nicht mehr ansprechbares Ausgangsmodul führt zur Abschaltung aller Ausgangsmodule eines Racks, da der sichere Zustand des Ausgangsmoduls nicht mehr überprüft werden kann. Um ein Ausgangsmodul im laufenden Betrieb auszutauschen, muss zuvor der Service-Mode auf dem E/A-Verarbeitungsmodul (F-IOP) aktiviert werden.
- Wenn an einem vom Anwenderprogramm ausgeschalteten Ausgang von digitalen Ausgangsmodulen ein High-Pegel statt dem zu erwarteten Low-Pegel anliegt, wird vom E/A-Verarbeitungsmodul ein Modulfehler signalisiert und das Ausgangsmodul in den sicheren energielosen Zustand gebracht.
- Wenn an einem vom Anwenderprogramm eingeschalteten Ausgang von digitalen Ausgangsmodulen ein Low-Pegel statt dem zu erwarteten High-Pegel anliegt, wird vom E/A-Verarbeitungsmodul ein Kanalfehler signalisiert.
- Wenn ein Hintergrundtest erkennt, dass ein Ausgang von digitalen Ausgangsmodulen mit High-Pegel nicht abgeschaltet werden kann, wird vom E/A-Verarbeitungsmodul eine Modulwarnung signalisiert. HIMA empfiehlt die Ursache für die Modulwarnung innerhalb von 24 h zu beheben, da danach alle Ausgangsmodule des betreffenden Racks in den sicheren Zustand gebracht werden. Wenn dagegen ein Ausgang beim Übergang von High-Pegel nach Low-Pegel nicht abgeschaltet werden kann, wird das Ausgangsmodul direkt in den energielosen Zustand gebracht.
- Wenn ein Hintergrundtest erkennt, dass ein Ausgang von digitalen Ausgangsmodulen mit Low-Pegel nicht eingeschaltet werden kann, wird vom E/A-Verarbeitungsmodul eine Modulwarnung signalisiert. Wenn die Modulwarnung nach Ablauf der Hintergrundtest-Zeit weiter ansteht, wird das Ausgangsmodul in den sicheren energielosen Zustand gebracht.
- Wenn an einem vom Anwenderprogramm eingeschalteten Kanal ein Leitungsschluss nach L- oder eine Überlast detektiert wird (F 3331 und F 3334), dann wird vom E/A-Verarbeitungsmodul dies als Modulfehler signalisiert und das Ausgangsmodul wird in den energielosen Zustand gebracht. Wenn zusätzlich der Systemparameter “LS/LB aktiv“ aktiviert ist und der Modus “LS/LB-Modus [UINT] ->“ auf 1 oder 2 gesetzt ist, wird die Systemvariable „LS“ bei dem Kanal, bei dem der Leitungsschluss detektiert wurde, auf TRUE gesetzt. Ausgabestand der Ausgangsmodule F 3334 beachten, siehe Kapitel 8.5.3 Hinweise zur Projektierung.
- Ein detektierter Leitungsschluss nach L- oder eine Überlast an einem Ausgang der F 3349, führt zur Abschaltung des Kanals. Der abgeschaltete Kanal wird nach ca. 4,5 Sekunden wieder zugeschaltet, wenn der Fehler nicht mehr ansteht.
- Die digitalen Ausgangsmodule F 3330 bis F 3335 unterstützen keine Abschaltung von einzelnen Kanälen.
- Im Stromquellenbetrieb wird das analoge Ausgangsmodul F 6705 bei allen auf dem Modul erkannten Fehlern in den sicheren, energielosen Zustand gebracht. Im Stromsenken-Betrieb ist der sichere, energielose Zustand nur durch Abschalten der externen Spannungsquelle erreichbar. Das Anwenderprogramm muss die Spannungsquelle für die Stromschleife sicher abschalten.
- Wenn ein Modul F 3330, F 3333, F 3335 oder F 3430 wegen eines Fehlers abgeschaltet wurde und für das Modul der automatische Wiederanlauf aktiviert ist, dann können Testimpulse von 1 ms im Abstand von 1 s ins Feld getrieben werden!
- Wenn ein Modul F 3331 oder F 3334 wegen eines Fehlers abgeschaltet wurde und für das Modul der automatische Wiederanlauf aktiviert ist, dann können Testimpulse im Abstand von 1 s ins Feld getrieben werden.
  Abhängig vom eingestellten Wert des Systemparameters Max. Testimpulsdauer [ms] ergibt sich:
  - Bei einem eingestellten Wert 0 ergibt sich eine Testimpulsdauer von max. 1 ms.
  - Bei einem eingestellten Wert 50 ergibt sich eine Testimpulsdauer von max. 50 ms.

- Wenn ein Modul F 3349 wegen eines Fehlers abgeschaltet wurde und für das Modul der automatische Wiederanlauf aktiviert ist, dann können Testimpulse von 100 µs im Abstand von 100 ms ins Feld getrieben werden!
- Wenn ein Modul F 6705 wegen eines Fehlers abgeschaltet wurde und für das Modul der automatische Wiederanlauf aktiviert ist, dann können Testimpulse von 16 ms im Abstand von 16 s ins Feld getrieben werden!

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 E/A-Störaustastung

Bei aktivierter Störaustastung reagiert das System nicht auf transiente Störungen. In diesem Fall schalten die Störungen die Ausgänge nicht sofort energielos und haben auch keine Auswirkung auf die Datenquellen.

Weitere Informationen zur Störaustastung finden Sie im Systemhandbuch HI 803 210 D.

Die Störaustastung wirkt nur innerhalb der Sicherheitszeit der Ressource und nur dann, wenn die Sicherheitszeit der Ressource ≥ 3 × Watchdog-Zeit der Ressource ist.

8.5 Sicherheitsbezogene digitale Ausgangsmodule F 3330, F 3331, F 3333, F 3334, F 3335, F 3349

Die Ausgangsmodule gewährleisten die Sicherheitsfunktion durch 3 in Reihe geschaltete testbare Schalter, wobei zwei davon als Sicherheitsschalter ausgeführt sind. Wenn eine Fehlfunktion der Ausgangsspannung oder der Sicherheitsschalter detektiert wird, dann schalten die Sicherheitsschalter alle Ausgänge in den energielosen Zustand.

Jeder Sicherheitsschalter ist einzeln über den E/A-Bus abschaltbar. Wenn ein Ausgangsmodul im Fehlerfall nicht über den E/A-Bus abgeschaltet werden kann, dann wir das Ausgangsmodul über den zweiten unabhängig Abschaltweg (E/A-Watchdog) in den energielosen Zustand gebracht.

Diese integrierte Sicherheitsfunktion schaltet bei Modulfehler alle Kanäle sicher ab (energieloser Zustand).

8.5.1 Test-Routinen

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

- Rücklesen der Ausgangssignale. Die Schaltschwelle für einen rückgelesenen Low-Pegel ist ≤ 6,5 V, gilt nicht für die F 3349.
- Prüfen der integrierten zweifachen Sicherheitsabschaltung.
- Testen der Rücklese-Einheiten, gilt nur für die F 3349.
- Aufschalten von Testmustern im Rahmen der Hintergrundtests mit Testintervall und maximaler Testimpulsdauer.
- Lesen der Leitungsüberwachung (LS/LB) der eingeschalteten Kanäle, sofern vorhanden.
- Lesen der Leitungsüberwachung (LS/LB) aller Kanäle, sofern vorhanden, im Rahmen des Testmustertests.

8.5.2 Redundanz von digitalen Ausgängen

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

8.5.3 Hinweise zur Projektierung

Die Leitungsbruch-Überwachung erfordert eine Mindestlast von mindestens 10 mA.

Bei redundanten Kanälen ist die erforderliche Mindestlast doppelt so hoch (20 mA).

Das Ausgangsmodul F 3334 detektiert ab dem Hardware-Ausgabestand AS03 keinen Leitungsschluss mehr. Es ist unzulässig, die Systemvariable *-> LS [BOOL]* ab Ausgabestand AS03 auszuwerten.

Vor dem Löschen der Module F 3330, F 3331, F 3333 und F 3334 aus der Projektkonfiguration sind die Ausgänge in den sicheren (abgeschalteten) Zustand zu bringen, z. B. ist für Ausgänge, die auf High-Pegel geforct sind, das Forcen zu beenden.

8.6 Sicherheitsbezogenes Relaismodul F 3430

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.

8.6.1 Test-Routinen

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

- Rücklesen des Ausgangssignals der diversitären 3fach-Relaisschalter.
- Prüfen der integrierten zweifachen Sicherheitsabschaltung.
- Aufschalten von Testmustern und Test auf Übersprechen (Walking-Bit-Test) im Rahmen der Hintergrundtests.

8.6.2 Verhalten bei externem Kurzschluss

Bei externen Kurzschlüssen spricht die Sicherung für den relevanten Kanal an. Eine Fehlermeldung erfolgt nicht.

8.6.3 Redundanz von Relaisausgängen

Die redundante Verschaltung von Relaisausgängen ist zulässig. Eine redundante Verschaltung wird für die Verfügbarkeit der Ausgänge verwendet.

8.6.4 Hinweise zur Projektierung

Relais sind elektromechanische Bauelemente und haben konstruktionsbedingt eine begrenzte Lebensdauer. Die Lebensdauer der Relais richtet sich nach der Schaltleistung der Kontakte (Strom/Spannung) und der Anzahl der Schaltspiele.

Die Lebensdauer beträgt bei Nennbetriebsbedingungen 300 000 Schaltspiele bei 30 VDC und 4 A.

Zur Einhaltung der Anforderungen gemäß IEC 61508 (PFD/PFH, siehe Kapitel 3.1.1) gilt ein Offline-Proof-Test-Intervall von 5 Jahren bei SIL-3-Anwendungen und von 20 Jahren bei SIL 2-Anwendungen.

Die notwendigen Prüfungen werden bei HIMA durchgeführt.

8.7 Sicherheitsbezogene analoges Ausgangsmodul F 6705

Die analogen Ausgänge geben die im Anwenderprogramm ermittelten Werte an Aktoren weiter.

Das analoge Ausgangsmodul F 6705 ist im Stromquellen- und im Stromsenken-Betrieb einsetzbar. Im Stromquellen-Betrieb ist der energielose Zustand (Ausgangsstrom = 0 mA) der sichere Zustand.

Damit im Fehlerfall die Eingangsvariablen den Wert 0 an das Anwenderprogramm liefern, müssen die Initialwerte auf 0 gesetzt werden.

Im Stromsenken-Betrieb ist der sichere Zustand nur mit zusätzlichen Maßnahmen erreichbar. Das Anwenderprogramm muss die Versorgungsspannung für die Stromschleife sicher abschalten.

8.7.1 Test-Routinen für analoge Ausgänge

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

- Rücklesen des Ausgangssignale.
- Testen des D/A-Wandlers auf Linearität.
- Testen auf Übersprechen zwischen den Ausgängen.
- Prüfen der integrierten zweifachen Sicherheitsabschaltung.

8.7.2 Verhalten bei externem Kurzschluss oder Überlast

Ein externer Leitungsbruch ist nicht von internen Fehlern unterscheidbar und schaltet das Modul ab.

8.7.3 Redundanz von analogen Ausgängen

Die redundante Verschaltung von analogen Ausgängen ist zulässig. Eine analoge Verschaltung wird für die Verfügbarkeit der Ausgänge verwendet. Für die redundante Verschaltung der Ausgänge, siehe das Modulhandbuch der F 6705 (HI 803 070 D).

8.8 Austausch von Ausgangsmodulen

Wenn Ausgangsmodule im Fehlerfall oder im Wartungsfalle getauscht werden, dann muss vorher der Service-Mode auf dem E/A-Verarbeitungsmodul (F-IOP) aktiviert werden, siehe Kapitel 6.5. Zusätzlich muss der Systemparameter *Service-Mode-Taster-deaktivieren* deaktiviert sein.

8.9 Checkliste für sicherheitsbezogene Ausgänge

HIMA empfiehlt, die Checklisten zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsbezogenen Ausgängen einzusetzen. Die Checkliste ist als Planungsunterlage einsetzbar und dient gleichzeitig auch als Nachweis für eine sorgfältige durchgeführte Planung. Die Checklisten stehen auf der HIMA-Webseite im Microsoft® Word®-Format zur Verfügung.

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. Damit kann auch eine Dokumentation über den Zusammenhang zwischen externer Verdrahtung und Anwenderprogramm erfolgen.

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

9 Software

Die Software für das sicherheitsbezogene Automatisierungssystem HIQuad X 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.

9.1 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 HIQuad X 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.

9.2 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.

9.3 Sicherheitstechnische Aspekte für die Programmierung

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

9.3.1 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!

9.3.2 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.

9.3.3 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.

9.3.4 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.

9.4 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 Systemhandbuch HI 803 210 D.**
- **Die in Tabelle 13 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.

9.4.1 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.

Parameter	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 zuweisen, sonst ist das Projekt nicht ablauffähig!	Eindeutiger Wert innerhalb des Netzwerks der Steuerungen. Das sind alle Steuerungen, die potentiell miteinander verbunden sind.
Sicherheitszeit [ms]	J	Sicherheitszeit der Ressource in Millisekunden, siehe Kapitel *Sicherheitsrelevante Zeiten* im Sicherheitshandbuch. Wertebereich: 20 … 22 500 ms. Standardwert: 600 ms (online änderbar)	Applikations-spezifisch
Watchdog-Zeit [ms]	J	Watchdog-Zeit in Millisekunden, siehe Kapitel *Sicherheitsrelevante Zeiten* im Sicherheitshandbuch. Wertebereich: 6 … 7500 ms. Standardwert: 200 ms (online änderbar)	Applikations-spezifisch
Sollzykluszeit [ms]	N	Gewünschte oder maximale Zykluszeit, siehe *Sollzykluszeit-Modus.* *Wertebereich*: 0 … 7500 ms. Standardwert: 0 ms (online änderbar) Die Sollzykluszeit darf höchstens so groß sein wie die eingestellte *Watchdog-Zeit [ms]* abzüglich des kleinsten einstellbarer Werts der *Watchdog-Zeit [ms]* (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 *Sollzykluszeit [ms]*, 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. 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 benötige Ausführungszeit von Anwenderprogrammen ab und verlängert so den Zyklus. Standardwert: Mode 1	Applikations-spezifisch
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.	Applikations-spezifisch

Parameter	S [1)]	Beschreibung	Einstellung für sicheren Betrieb
Optimierte Nutzung Kom.-Zeitscheibe	N	Der Systemparameter verkürzt die Antwortzeiten für die Kommunikation über das oder die Prozessormodule. i Es kann sich die zeitliche Ausnutzung der *Max. Kom.-Zeitscheibe [ms]* und somit der Systemparameter *Max. Dauer Konfigurationsverbindungen [ms]* ändern, so dass diese stärker beansprucht werden können, z. B. beim Reload.	---
Max. Dauer Konfigurations-verbindungen [ms]	N	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.	Applikations-spezifisch
Maximale Systembus-Latenzzeit [µs]	N	Maximale Verzögerung einer Nachricht zwischen einem E/A-Verarbeitungsmodul und einem Prozessormodul. Einstellung: System-Standardwerte oder 100 … 50 000 µs Standardwert: *System-Standardwerte* i Für die Einstellung der maximalen Systembuslatenz auf einen Wert ≠ *System-Standardwerte* ist eine Lizenz erforderlich.	---
Online-Einstellungen erlauben	J	TRUE: **Alle** unter FALSE genannten Schalter/Parameter sind online mit dem PADT änderbar. Dies gilt nur, wenn die Systemvariable *Read-only in RUN* den Wert FALSE hat. Standartwert: TRUE. FALSE: Folgende Parameter sind **nicht** online änderbar: ▪ *System-ID* ▪ *Autostart* ▪ *Globales Forcen erlaubt* ▪ *Globales MultiForcen erlaubt* ▪ *Globale Force-Timeout-Reaktion* ▪ *Laden erlaubt* ▪ *Reload erlaubt* ▪ *Start erlaubt* Wenn *Reload erlaubt* = TRUE ist, sind folgende Parameter online änderbar: ▪ *Watchdog-Zeit (der Ressource)* ▪ *Sicherheitszeit* ▪ *Sollzykluszeit* ▪ *Sollzykluszeit-Modus* Bei gestoppter Steuerung und durch einen Reload ist es möglich, *Online-Einstellungen erlauben* = TRUE zu setzen.	HIMA empfiehlt die Einstellung FALSE.

Parameter	S [1)]	Beschreibung		Einstellung für sicheren Betrieb
Autostart	J	TRUE:	Wenn die Steuerung an die Versorgungsspannung angeschlossen wird, starten die Anwenderprogramme automatisch. Standartwert: 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. Standartwert: TRUE.	Applikations-spezifisch
		FALSE:	Kein Start erlaubt.	
Laden erlaubt	J	TRUE:	Download der Konfiguration erlaubt. Standartwert: TRUE.	Applikations-spezifisch
		FALSE:	Kein Start erlaubt.	
Reload erlaubt	J	TRUE:	Reload der Konfiguration erlaubt. Standartwert: 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. Standartwert: 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: ▪ 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. Standartwert: FALSE (online änderbar).	

Parameter	S [1)]	Beschreibung	Einstellung für sicheren Betrieb
Minimale Konfigurations-version	N	Mit dieser Einstellung ist es möglich, Code zu generieren, der entsprechend den Projektanforderungen zu alten oder zu neuen Versionen des HIQuad X Betriebssystems kompatibel ist. Als Standardwert wird die installierte SILworX Version angezeigt. HIQuad X wird erst ab SILworX V10 unterstützt. Die Einstellung auf eine SILworX Version vor V10 wird für HIQuad X abgelehnt. Im Logbuch erscheint eine Fehlermeldung! Weitere Details siehe Kapitel Parameter *Minimale Konfigurationsversion*.	Applikations-spezifisch
Schneller Hochlauf	J	Für HIQuad X nicht anwendbar.	---
[1)] Systemparameter wird vom Betriebssystem sicherheitsbezogen behandelt, ja (J) oder nein (N).			

Tabelle 13: Die Systemparameter der Ressource

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

Mit den Einstellungen im Systemparamater *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.

HIQuad X 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	Ist ein CPU-Zyklus kürzer als die definierte Sollzykluszeit, wird der CPU-Zyklus bis zur Sollzykluszeit verlängert. Ist der CPU-Zyklus länger als die Sollzykluszeit, setzt die CPU den Zyklus ohne Verzögerung fort. i Ein Reload oder eine Aufsynchronisation wird abgelehnt, wenn die Reservezeit (Sollzykluszeit minus tatsächliche Zykluszeit) nicht ausreicht.
fest-tolerant	Wie *fest*, jedoch mit den folgenden Unterschieden: 1. Wenn erforderlich wird bei der Aufsynchronisation die Sollzykluszeit für einen CPU-Zyklus nicht eingehalten, um die Aufsynchronisation erfolgreich durchführen zu können. 2. Wenn erforderlich wird beim Reload die Sollzykluszeit für 1 bis n (n = Anzahl der geänderten Anwenderprogramme) CPU-Zyklen nicht eingehalten, um den Reload erfolgreich durchführen zu können. Die Standardeinstellung ist *fest-tolerant*! i Nach dem 1. Reload-Aktivierungszyklus gelten Watchdog-Zeit, Sollzykluszeit und Sollzykluszeit-Modus gemäß der neuen Konfiguration. Höchstens jeder fünfte Zyklus kann während des Reload verlängert werden. Ein einziger Zyklus kann während der Synchronisation verlängert werden.
dynamisch	Die CPU führt jeden CPU-Zyklus so schnell wie möglich aus. Dies entspricht einer eingestellten Sollzykluszeit von 0 ms. i Ein Reload oder eine Aufsynchronisation wird abgelehnt, wenn die Reservezeit (Sollzykluszeit minus tatsächliche Zykluszeit) nicht ausreicht. Höchstens jeder fünfte Zyklus kann während des Reload verlängert werden. Ein einziger Zyklus kann während der Synchronisation verlängert werden.
dynamsich-tolerant	Wie *dynamisch*, jedoch mit den folgenden Unterschieden: 1. Wenn erforderlich wird bei der Aufsynchronisation die Sollzykluszeit für einen CPU-Zyklus automatisch erhöht, um die Aufsynchronisation erfolgreich durchführen zu können. 2. Wenn erforderlich wird beim Reload die Sollzykluszeit für 1 bis n (n = Anzahl der geänderten Anwenderprogramme) CPU-Zyklen automatisch erhöht, um den Reload erfolgreich durchführen zu können. i Nach dem 1. Reload-Aktivierungszyklus gelten Watchdog-Zeit, Sollzykluszeit und Sollzykluszeit-Modus gemäß der neuen Konfiguration. Ein Reload oder eine Aufsynchronisation wird abgelehnt, wenn die Reservezeit (Sollzykluszeit minus tatsächliche Zykluszeit) nicht ausreicht.

Tabelle 14: Einstellungen Sollzykluszeit-Modus

9.4.1.2 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.

9.4.1.3 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 (F-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 HIQuad X 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.

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

Der Systemparameter *Max. Dauer Konfigurationsverbindungen [ms]* entspricht dem erforderlichen Zeitbudget $\mathbf{t}_{Konfig}$ 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 $\mathbf{t}_{Konfig}$ so zu dimensionieren, dass alle Tasks in einem CPU-Zyklus abgearbeitet werden können.

Für die Prozessormodule F-CPU 01 wird $\mathbf{t}_{Konfig}$ wie folgt berechnet:

F-CPU 01: $\mathbf{t}_{Konfig} = (\mathbf{n}_{Com} + \mathbf{n}_{PADT}) * 1\ ms + \mathbf{n}_{RIO} * 0{,}25\ ms + 4\ ms + 4 * (\mathbf{t}_{Latenz} * 2 + 0{,}8\ ms)$

$t_{Konfig:}$	Systemparameter *Max. Dauer Konfigurationsverbindungen [ms]*
$n_{COM:}$	Anzahl Module mit Ethernet-Schnittstellen (F-CPU, F-COM)
$n_{PADT:}$	5, maximale Anzahl PADT-Verbindungen
$n_{RIO:}$	Anzahl konfigurierter Remote I/Os
$t_{Latenz:}$	Aktive *maximale Systembus-Latenzzeit einsetzen, siehe nachfolgende Beschreibungen.* 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.

Ist für den Parameter *Maximale Systembus-Latenzzeit [µs]* die Einstellung System-Standardwerte ausgewählt, so ist der Wert 2,2 ms in die obere Formel einzusetzen. Ist für t_{Latenz} ein Wert von 100 … 50 000 µs manuell eingetragen, dann ist dieser Wert in die obere Formel einzusetzen.

TIPP Die aktuelle Systembus-Latenzzeit wird im Control Panel angezeigt!

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

i Wenn $\mathbf{t}_{Konfig}$ 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 $\mathbf{t}_{Konfig}$ 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 $\mathbf{t}_{Konfig}$ im Control Panel auch online eingestellt werden.

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

9.4.1.5 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.
- Für HIQuad X ist die *Minimale Konfigurationsversion* auf *SILworX V10* oder höher einzustellen.

9.4.1.6 Systemvariablen 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 des 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
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 *Lesen* 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)] Sicherheitsbezogener Systemparameter ja/nein (J/N)			

Tabelle 15: Systemvariablen des Racks

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

9.4.2 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 drei Systemvariablen *Read-only in RUN*, *Reload-Deaktivierung* und *Force-Deaktivierung,* siehe Tabelle 15.

Wenn alle drei Systemvariablen TRUE sind, dann ist kein Zugriff auf die Steuerung mehr möglich. In diesem Fall kann die Steuerung nur durch Neustart aller Prozessormodule 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 Variable vom Typ BOOL definieren, Initialwert auf FALSE setzen.
2. Globale Variable den drei Systemvariablen *Read-only in RUN*, *Reload-Deaktivierung* und *Force-Deaktivierung* 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 und weiteren Bedienfunktionen können auf unterschiedliche Schlüssel und Personen verteilt werden.

9.5 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.

9.5.1 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 9.5.3.

⚠ 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.

9.5.2 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.

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

9.5.3 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 HIQuad X 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!

9.5.4 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.

9.5.5 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.

Näheres zum Forcen im Systemhandbuch HI 803 210 D und in der SILworX Online-Hilfe.

9.5.5.1 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.

9.5.5.2 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.

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

9.6 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.

9.7 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 Installationsverzeichnisses befindet sich die API-Dokumentation in HTLM-Format und ein C# Anwendungsbeispiel.

10 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.

10.1 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 HIQuad X).
- 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!

10.1.1 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.

10.1.1.1 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.

10.1.2 Schritte der Programmierung

Die Programmierung von HIQuad X 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.

10.1.3 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.

10.1.4 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 *Codegenerierung Kompatibilität* auf *SILworX V2* 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 parametrierten maximaler Anzahl von CPU-Zyklen. Nicht änderbar!		
Klassifikation	N	Einstufung des Anwenderprogramms in *sicherheitsgerichtet* oder *standard*, dient nur zur Dokumentation und hat keinen Einfluss auf die Funktion des Programms. Die Standardeinstellung ist sicherheitsgerichtet		Applikations-spezifisch
Online-Einstellungen erlauben	J	Wenn *Online-Einstellungen erlauben* ausgeschaltet ist, können die Einstellungen der anderen Programmschalter nicht per Online-Zugriff (Control Panel) verändert werden. Wirkt nur, wenn *Online-Einstellungen erlauben* 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: ▪ Nur Forcen beenden. ▪ Programm stoppen. Die Standardeinstellung ist *Nur Forcen beenden.*		
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 *ab SILworX V7*.		

[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 sicherheitsbezogen Betrieb aufgenommen wird!

Tabelle 16: Systemparameter des Anwenderprogramms

10.1.5 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.

10.1.6 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.

10.1.7 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.

10.1.8 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.

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!

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.

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.

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.

10.1.9 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.

10.1.10 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.

Testmodus erlaubt	Beschreibung
Deaktiviert	Testmodus deaktiviert (Standardeinstellung).
Aktiviert	Testmodus aktiviert.

Tabelle 17: 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!

10.1.11 Online-Änderung von Systemparametern

Es ist möglich, die Systemparameter der Tabelle 18 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 geforderten 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 18: Online änderbare Parameter

10.1.12 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.

10.1.13 Multitasking

Multitasking bezeichnet die Fähigkeit des HIQuad X 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$_{\text{Anwenderprogramm}}$ **= Watchdog-Zeit**$_{\text{Prozessormodul}}$ **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* parametriert 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 803 210 D.

10.1.14 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 HIQuad X, die bereits baumustergeprüft sind.

10.2 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 und dient gleichzeitig auch als Nachweis für eine sorgfältige durchgeführte Planung.

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

11 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.

11.1 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!

Für HIQuad X stehen die im Kommunikationshandbuch aufgelisteten Standardprotokolle zur Verfügung.

11.2 Sicherheitsbezogenes Protokoll safe**ethernet**

Die sicherheitsbezogene Kommunikation über safe**ethernet** ist bis SIL 3 zertifiziert.

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

Weitere Einzelheiten zu safe**ethernet** 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 HIQuad X die sicherheitsbezogene Kommunikation. Die Input-Variablen dieser safe**ethernet** Verbindung verhalten sich gemäß dem eingestellten Parameter *Freeze-Daten bei Verbindungsverlust [ms]*. Für sicherheitsbezogene Funktionen, die über safe**ethernet** 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 ≥ 1,5 x Sollzykluszeit**
2. **ReceiveTMO ≥ 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.

11.3 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 Störaustastung 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 safe**ethernet** 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 HIQuad X Steuerung	Für weitere Informationen zur Reaktionszeit der HIQuad X Steuerung (Ressource) t_{RR}, siehe Kapitel *Sicherheitsrelevante Zeiten*.
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 safe**ethernet** Parameter und Bedingungen

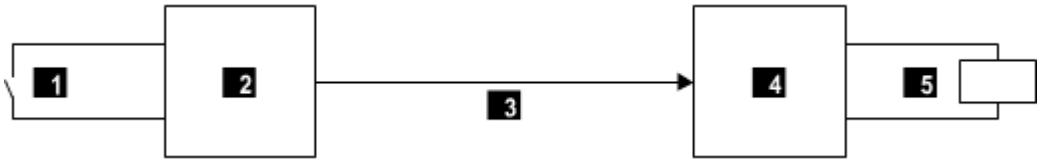
Für die folgenden Berechnungen der zulässigen maximalen Reaktionszeiten gelten folgende Bedingungen:

- Die Signale, die mit safe**ethernet** übertragenen 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.

11.3.1 Berechnung der maximalen Reaktionszeit zweier HIQuad X Steuerungen

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



1 Eingang
2 HIQuad X Steuerung 1
3 Sicherheitsbezogenes Protokoll
4 HIQuad X Steuerung 2
5 Ausgang

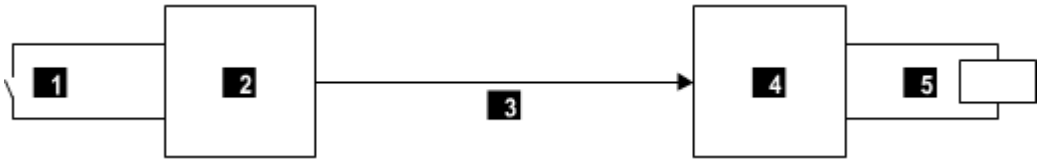
Bild 1: Reaktionszeit bei Verbindung zweier HIQuad X Steuerungen

$$\mathbf{T_R = t_1 + t_2 + t_3}$$

T_R Worst Case Reaction Time
t_1 Reaktionszeit der HIQuad X Steuerung 1
t_2 *ReceiveTMO*
t_3 Reaktionszeit der HIQuad X Steuerung 2

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

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



1 Eingang
2 HIQuad X Steuerung
3 Sicherheitsbezogenes Protokoll
4 HIMatrix Steuerung
5 Ausgang

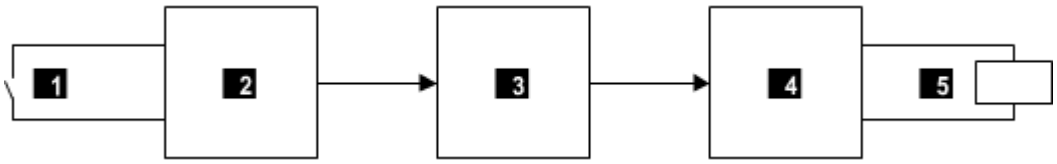
Bild 2: Reaktionszeit bei Verbindung einer HIQuad X mit einer HIMatrix Steuerung

$$\mathbf{T_R = t_1 + t_2 + t_3}$$

T_R Worst Case Reaction Time
t_1 Reaktionszeit der HIQuad X Steuerung
t_2 *ReceiveTMO*
t_3 2 * Watchdog-Zeit der HIMatrix Steuerung

11.3.3 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:



1 Eingang
2 Remote I/O 1
3 HIQuad X Steuerung
4 Remote I/O 2
5 Ausgang

Bild 3: Reaktionszeit mit zwei HIMatrix Steuerungen/Remote I/Os und einer HIQuad X Steuerung

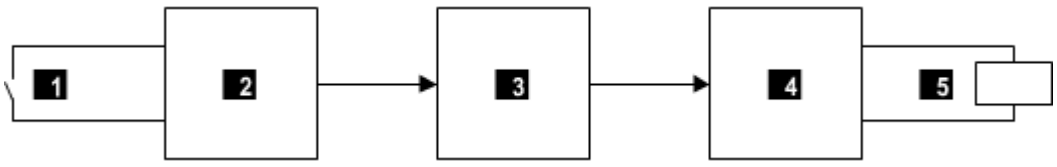
$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

T_R	Worst Case Reaction Time
t_1	2 * Watchdog-Zeit der HIMatrix Steuerung/Remote I/O 1
t_2	*ReceiveTMO1*
t_3	Reaktionszeit der HIQuad X 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.

11.3.4 Berechnung der max. Reaktionszeit mit zwei HIQuad X und einer HIMatrix Steuerung

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



1 Eingang
2 HIQuad X Steuerung 1
3 HIMatrix Steuerung
4 HIQuad X Steuerung 2
5 Ausgang

Bild 4: Reaktionszeit mit zwei HIQuad X Steuerungen und einer HIMatrix Steuerung

$$T_R = t_{RR1} + t_1 + t_2 + t_3 + t_{RR2}$$

T_R Worst Case Reaction Time
t_{RR1} Reaktionszeit der HIQuad X Steuerung 1
t_1 *ReceiveTMO1*
t_2 2 * Watchdog-Zeit des HIMatrix Steuerung
t_3 *ReceiveTMO2*
t_{RR2} Reaktionszeit der HIQuad X Steuerung 2

i Die beiden HIQuad X Steuerungen 1 und 2 können auch identisch sein.
Die HIMatrix Steuerung kann auch eine HIQuad X Steuerung sein.

11.4 Sicherheitsbezogenes Protokoll HIPRO-S V2

Das HIPRO-S V2 Protokoll wird zur sicherheitsbezogenen Kommunikation gemäß SIL 3 zwischen HIQuad Steuerungen und HIQuad X, HIMax oder HIMatrix Steuerungen verwendet.

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

- 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 HIQuad X Steuerungen verwendet werden. Verbindungen zwischen HIQuad X Steuerungen untereinander und mit weiteren HIMA Steuerungen (HIMax. HIMatrix) müssen mit safe**ethernet** aufgebaut werden!

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

12 Einsatz in Brandmelderzentralen

Die HIQuad X Systeme sind für Brandmelderzentralen nach DIN EN 54-2 und NFPA 72 einsetzbar, wenn für die Eingänge und Ausgänge Leitungsüberwachung parametriert 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 Brandmeldezentrale den Störungsmeldezustand innerhalb von 100 s nach Empfang der Störungsmeldung im HIQuad X System einnehmen.

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

- Die digitalen Eingänge der Eingangsmodule F 3237 und F 3238 mit Leitungsüberwachung.
- Die analogen Eingänge der Eingangsmodule F 6217 und F 6221 mit Leitungsüberwachung.

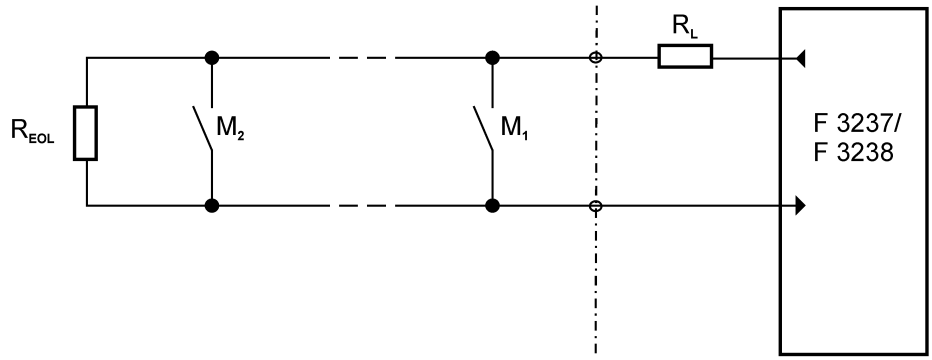
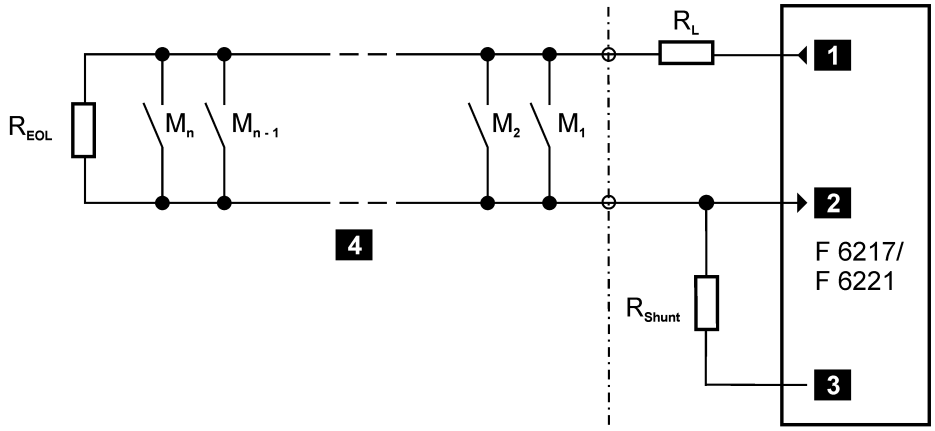


Bild 5: Verschaltung von Brandmeldern mit digitalen Eingängen



1 Sensor-Versorgung
2 Analoger Eingang
3 Bezugspotenzial
4 Meldeschleife

M: Brandmelder R_{EOL}: Abschlusswiderstand am letzten Sensor der Schleife.
R_{Shunt}: Messwiderstand R_L: Begrenzung des maximal zulässigen Stromes der Schleife.

Bild 6: Verschaltung von Brandmeldern mit analogen Eingängen

Für die Applikation 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.

Zusätzlich ist auf die Einhaltung der spezifizierten Stromwerte der Module F 3237 und F 3238 (siehe Datenblätter) zu achten. Dies gilt insbesondere, wenn die Brandmelder keine mechanischen Kontakte haben, sondern elektronische Ausgänge.

Die Alarmausgänge zur Ansteuerung von z. B. Lampen, Sirenen und Hupen werden im Arbeitsstromprinzip betrieben. Diese Ausgänge sind auf Leitungsbruch und Leitungsschluss zu überwachen.

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 Ausgangsmodule oder zu Übertragungseinrichtungen für Störungsmeldungen muss im Ruhestromprinzip erfolgen.

Die Übertragung von Brandmeldungen von HIMA System zu HIMA System ist mit den vorhandenen Kommunikationsstandards wie Ethernet (OPC) realisierbar. Die Überwachung der Kommunikation ist Bestandteil des Anwenderprogramms. 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.

HIQuad X Systeme, die als Brandmelderzentralen 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 HIQuad X 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 EN 54-2 und NFPA 72 ist eine Erdschlussüberwachung einzusetzen.

13 Einsatz von HIQuad X in Zone 2

HIQuad X 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 803 210 D zu beachten.

HIQuad X 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 HIQuad X Komponenten in Zone 2

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

Die HIQuad X Komponenten sind für Temperaturbereich 0 °C ≤ Ta ≤ +60 °C zugelassen und haben die folgenden Ex-Kennzeichnungen:

 II 3G Ex nA IIC T4 Gc

 II 3G Ex nA nC IIC T4 Gc

0 °C ≤ Ta ≤ +60 °C

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 HIQuad X Komponenten

Besondere Bedingungen

1. HIQuad X 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 HIQuad X Komponenten sind für den Betrieb mit maximalem Verschmutzungsgrad 2 ausgelegt.
4. Das verwendete Gehäuse muss die entstehende Verlustleistung sicher abführen können.
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.
7. Die Racks müssen zwangsbelüftet sein.

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.

Anhang

Glossar

Begriff	Beschreibung
AI	Analog Input: Analoger Eingang
AO	Analog Output: Analoger Ausgang
ARP	Address Resolution Protocol: Netzwerkprotokoll zur Zuordnung von Netzwerkadressen zu Hardwareadressen
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
EUC	Equipment under Control: Überwachte Steuerung
FAT	Factory Acceptance Test: Abnahme eines Produkts beim Hersteller
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 Racks (Nummer)
rückwirkungsfrei	Rückwirkungsfrei meint in diesem Zusammenhang, dass sichere und nicht sichere Module, sofern als rückwirkungsfrei gekennzeichnet, in einen Rack betrieben werden dürfen. Das nicht sichere Modul hat im Sinne der funktionalen Sicherheit keine Rückwirkung auf die sicheren Module.
R/W	Read/Write: Spaltenüberschrift für Art von Systemvariable
SAT	Site Acceptance Test: Abnahme einer Steuerung an ihrem Aufstellungsort
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 Verschlüsslungsprotokoll
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
w_S	Scheitelwert der Gesamt-Wechselspannungskomponente

Abbildungsverzeichnis

Tabellenverzeichnis

Index

HANDBUCH
HIQuad X Sicherheitshandbuch

HI 803 208 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 HIQuad X:

www.hima.com/de/produkte-services/hiquad-x

www.hima.com