Handbuch

HIMax®

Sicherheitshandbuch

Bahnanwendungen

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

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

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

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

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

Kontakt

HIMA Paul Hildebrandt GmbH

Postfach 1261

68777 Brühl

Tel.: +49 6202 709-0

Fax: +49 6202 709-107

E-Mail: info@hima.com

Revisions-index	Änderungen	Art der Änderung	
		technisch	redaktionell
8.00	Aktualisierte Ausgabe zu SILworX V8 Geändert: Sicherheitszeiten, Normen, Prüfbedingungen Hinzugefügt: Module X-CPU 31, X-DI 32 03 und X-DO 24 02, Kapitel Cyber Security	X	X
9.00	Hinzugefügt: Modul X-AI 32 01	X	X
10.00	Aktualisierte Ausgabe zu SILworX 10 Geändert: Sicherheitsrelevante Zeitparameter, Automation Security (Cyber Security)	X	X
11.00	Aktualisierte Ausgabe zu SILworX V11	X	X

Inhaltsverzeichnis

1 Einleitung 7

1.1 Gültigkeit und Aktualität 7

1.2 Zielgruppe 7

1.3 Darstellungskonventionen 8

1.3.1 Sicherheitshinweise 8

1.3.2 Gebrauchshinweise 9

1.4 Safety Lifecycle Services 10

2 Einsatz des Systems HIMax 11

2.1 Bestimmungsgemäße Verwendung 11

2.1.1 Anwendung im Ruhestromprinzip 11

2.1.2 Anwendung im Arbeitsstromprinzip 11

2.2 Nichtbestimmungsgemäße Verwendung 11

2.3 Aufgaben der Maschinen- und Anlagenhersteller sowie des Betreibers 12

2.3.1 Anschluss von Kommunikationspartnern 12

2.3.2 Verwendung der sicherheitsbezogenen Kommunikation 12

2.4 ESD-Schutzmaßnahmen 12

2.5 Weitere Systemdokumentationen 13

3 Sicherheitskonzept für den Einsatz der PES 14

3.1 Sicherheit und Verfügbarkeit 14

3.1.1 HR-Berechnungen 14

3.1.2 Selbst-Test und Fehlerdiagnose 15

3.1.3 PADT 15

3.1.4 Redundanz 15

3.1.5 Aufbau von Sicherheitssystemen nach dem Arbeitsstromprinzip 16

3.1.5.1 Erkennen ausgefallener Komponenten 16

3.1.5.2 Sicherheitsfunktion im Arbeitsstromprinzip 16

3.1.5.3 Redundanz von Komponenten 16

3.2 Sicherheitsrelevante Zeiten 17

3.2.1 Prozess-Sicherheitszeit 17

3.2.2 Parameter «Sicherheitszeit [ms]» Ressource 17

3.2.3 Watchdog-Zeit (Ressource) 18

3.2.4 Abschätzung der Watchdog-Zeit 18

3.2.5 Watchdog-Zeit durch Test ermitteln 19

3.3 Sicherheitsauflagen 21

3.3.1 Produktunabhängige Auflagen der Hardware 21

3.3.2 Produktabhängige Auflagen der Hardware 21

3.3.3 Produktunabhängige Auflagen der Programmierung 21

3.3.4 Auflagen für die Verwendung des Programmierwerkzeugs 22

3.3.5 Kommunikation 22

3.3.6 Auflagen für Bahnanwendungen 22

3.4 Automation Security 23

3.4.1 Produkteigenschaften 23

3.4.2 Risikoanalyse und Planung 24

3.5 Prüfbedingungen 25

3.6 Zusätzliche Prüfbedingungen für Bahnanwendungen 25
3.6.1 Höhenbereich 25
3.6.2 Klimatische Bedingungen 26
3.6.2.1 Einsatz in der Signaltechnik 26
3.6.2.2 Einsatz auf Bahnfahrzeugen 26
3.6.3 Mechanische Bedingungen 26
3.6.3.1 Einsatz in der Signaltechnik 26
3.6.3.2 Einsatz auf Bahnfahrzeugen 26
3.6.4 EMV-Bedingungen 26
3.6.4.1 Einsatz in der Signaltechnik 27
3.6.4.2 Einsatz auf Bahnfahrzeugen 28
3.6.5 Erschwerte Bedingungen 28
3.6.6 Versorgungsspannung 29
3.6.6.1 Bedingungen an die Versorgungsspannung auf Bahnfahrzeugen 29
4 Prozessormodul 30
4.1 Prozessormodul X-CPU 01 30
4.2 Prozessormodul X-CPU 31 30
4.3 Selbst-Tests 30
4.4 Reaktionen auf Fehler im Prozessormodul 30
4.5 Austausch von Prozessormodulen 31
5 Systembusmodul 32
5.1 Rack-ID 32
5.2 Attribut *Responsible* 32
6 Kommunikationsmodul 35
7 Eingangsmodule 36
7.1 Allgemeines 36
7.2 Reaktion im Fehlerfall 36
7.3 Sicherheit von Sensoren, Encodern und Transmittern 36
7.4 Sicherheitsbezogene digitale Eingangsmodule 37
7.4.1 Test-Routinen 37
7.4.2 Redundanz von digitalen Eingängen 37
7.4.3 Surge auf digitalen Eingängen 37
7.5 Sicherheitsbezogene analoge Eingangsmodule 38
7.5.1 Test-Routinen 38
7.5.2 Redundanz von analogen Eingängen 38
7.5.3 Zustand von LL, L, N, H, HH bei X-AI 32 01 38
7.6 Checklisten Eingänge 38
8 Ausgangsmodule 39
8.1 Allgemeines 39
8.2 Reaktion im Fehlerfall 39
8.3 Sicherheit von Aktoren 39
8.4 Sicherheitsbezogene digitale Ausgangsmodule 39
8.4.1 Test-Routinen 40
8.4.2 Ausgangs-Störaustastung 40

8.4.3 Verhalten bei externem Kurzschluss oder Überlast 40
8.4.4 Redundanz von digitalen Ausgängen 40

8.5 Sicherheitsbezogene Relaismodule 40

8.5.1 Test-Routinen 41
8.5.2 Redundanz von Relaisausgängen 41

8.6 Checklisten Ausgänge 41

9 Software 42

9.1 Sicherheitstechnische Aspekte von Betriebssystemen 42

9.2 Arbeitsweise und Funktionen von Betriebssystemen 42

9.3 Sicherheitstechnische Aspekte für die Programmierung 43

9.3.1 Sicherheitskonzept von SILworX 43
9.3.2 Überprüfung der Konfiguration und der Anwenderprogramme 43
9.3.3 Archivierung eines Projekts 44
9.3.4 Identifizierung von Konfiguration und Programmen 44

9.4 Parameter der Ressource 44

9.4.1 Systemparameter der Ressource 45
9.4.1.1 Verwendung der Parameter *Sollzykluszeit* und *Sollzykluszeit-Modus* 49
9.4.1.2 Maximale Kommunikationszeitscheibe 50
9.4.1.3 Ermitteln der maximalen Dauer der Kommunikationszeitscheibe 50
9.4.1.4 Berechnung der *Max. Dauer Konfigurationsverbindungen [ms]* t_{Konfig} 51
9.4.1.5 52
9.4.1.6 Parameter *Minimale Konfigurationsversion* 52
9.4.1.7 Systemvariable des Racks 53
9.4.2 Abschließen und Aufschließen der Steuerung 54

9.5 Forcen 54

9.5.1 Verwendung von Forcen 55
9.5.2 Per Reload geänderte Zuweisung einer Datenquelle 55
9.5.3 Zeitbegrenzung 56
9.5.4 Einschränkung des Forcens 56
9.5.5 MultiForcen 57
9.5.5.1 Ziele von MultiForcen 57
9.5.5.2 Globales MultiForcen 58

9.6 Sicherer Versionsvergleich 58

10 Sicherheitstechnische Aspekte für Anwenderprogramme 59

10.1 Sicherheitsbezogener Einsatz 59

10.1.1 Basis der Programmierung 59
10.1.1.1 E/A-Konzept 60
10.1.2 Schritte der Programmierung 60
10.1.3 Funktionen der Anwenderprogramme 60
10.1.4 Systemparameter der Anwenderprogramme 61
10.1.5 Hinweise zum Parameter *Codegenerierung Kompatibilität* 62
10.1.6 Code-Erzeugung 63
10.1.7 Laden und Starten des Anwenderprogramms 63
10.1.8 Reload 63
10.1.9 Online-Test 64
10.1.10 Testmodus 65
10.1.11 Online-Änderung von Systemparametern 65
10.1.12 Projekt-Dokumentation für sicherheitsbezogene Anwendungen 66

10.1.13 Multitasking 67
10.1.14 Abnahme durch Genehmigungsbehörden 67
10.2 Checkliste zur Erstellung eines Anwenderprogramms 67
11 Konfiguration der Kommunikation 68
11.1 Standardprotokolle 68
11.2 Sicherheitsbezogenes Protokoll safeethernet 68
11.3 Maximale Reaktionszeit für safeethernet 70
11.3.1 Berechnung der max. Reaktionszeit zweier HIMax Steuerungen 71
11.3.2 Berechnung der max. Reaktionszeit in Verbindung mit einer HIMatrix Steuerung 71
11.3.3 Berechnung der max. Reaktionszeit mit zwei HIMatrix Steuerungen oder Remote I/Os 72
11.3.4 Berechnung der max. Reaktionszeit mit zwei HIMax und einer HIMatrix Steuerung 72
11.4 Sicherheitsbezogenes Protokoll PROFIsafe 73
Anhang 74
Glossar 74
Abbildungsverzeichnis 75
Tabellenverzeichnis 76
Index 77

1 Einleitung

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

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

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

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

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

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

- Die in den Beschreibungen vorgesehenen Einsatzfälle wurden eingehalten.
- Die spezifizierten Umgebungsbedingungen wurden eingehalten.
- Es sind nur zugelassene Fremdgeräte angeschlossen.

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

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

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

1.1 Gültigkeit und Aktualität

Dieses Sicherheitshandbuch ist für folgende Versionen erstellt:

- HIMax Betriebssysteme gemäß Versionsliste.
- SILworX ab Version 11.

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

1.2 Zielgruppe

Dieses Dokument wendet sich an Planer, 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 HIMax

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

2.1 Bestimmungsgemäße Verwendung

Das Kapitel beschreibt die bestimmungsgemäße Verwendung des sicherheitsbezogenen Automatisierungssystems HIMax.

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

Das sicherheitsbezogene System HIMax ist einsetzbar bis zum Sicherheits-Integritätslevel SIL 4 gemäß EN 50126, EN 50128 und EN 50129.

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

2.1.1 Anwendung im Ruhestromprinzip

Das HIMax System ist für das Ruhestromprinzip konzipiert.

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

2.1.2 Anwendung im Arbeitsstromprinzip

Das HIMax System kann in Arbeitsstrom-Anwendungen eingesetzt werden.

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

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

2.2 Nichtbestimmungsgemäße Verwendung

Bei der Übertragung von (sicherheitsrelevanten) Daten sind IT-Sicherheitsregeln zu beachten. Bei Übertragung über öffentliche Netze (z. B. Internet) sind Zusatzmaßnahmen zur Erhöhung der Sicherheit (z. B. VPN-Tunnel, Firewall, etc.) einzusetzen.

2.3 Aufgaben der Maschinen- und Anlagenhersteller sowie des Betreibers

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

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

2.3.1 Anschluss von Kommunikationspartnern

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

2.3.2 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 10.1.14 und im Kommunikationshandbuch HI 801 100 D aufgeführten Berechnungsgrundlagen sind anzuwenden.

2.4 ESD-Schutzmaßnahmen

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

HINWEIS

Schäden am HIMax System durch elektrostatische Entladung!

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

2.5 Weitere Systemdokumentationen

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

Dokument	Inhalt	Dokument-Nr.
HIMax Sicherheitshandbuch	Sicherheitsfunktionen des HIMax Systems	HI 801 002 D
HIMax Systemhandbuch	Hardwarebeschreibung des modularen Systems	HI 801 000 D
Zertifikate	Prüfergebnisse	
Versionsliste	TÜV-zertifizierte Versionen des Betriebssystems	
Handbücher der Komponenten	Beschreibung der einzelnen Komponenten	
Wartungshandbuch	Beschreibung wichtiger Tätigkeiten zum Betrieb und Wartung	HI 801 170 D
Kommunikationshandbuch	Beschreibung der safe**ethernet** Kommunikation und Auflistung 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	SILworX Bedienung	

Tabelle 1: Übersicht Systemdokumentation

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

3 Sicherheitskonzept für den Einsatz der PES

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

- Sicherheit und Verfügbarkeit.
- Für Sicherheit wichtige Zeiten.
- Sicherheitsauflagen.
- Automation Security.
- Zusätzliche Prüfbedingungen für Bahnanwendungen.

3.1 Sicherheit und Verfügbarkeit

Die HIMax Systeme sind für Prozess-Steuerungen, Schutzsysteme, Brennersteuerungen und Maschinensteuerungen zertifiziert.

Das sicherheitsbezogene System HIMax ist einsetzbar bis zum Sicherheits-Integritätslevel SIL 4 gemäß EN 50126, EN 50128 und EN 50129.

Vom sicherheitsbezogenen Automatisierungssystem HIMax geht kein unmittelbares Risiko aus.

⚠ WARNUNG

Personenschaden durch falsch angeschlossene oder falsch programmierte sicherheitsbezogene Automatisierungssysteme!

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

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

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

HIMA empfiehlt dringend, ausgefallene Module nach möglichst kurzer Zeit zu ersetzen.

Ein Ersatzmodul, das an der Stelle eines ausgefallenen Moduls eingesetzt ist, nimmt ohne Bedienaktion seinen Betrieb auf. Es übernimmt die Funktion des ausgefallenen Moduls, sofern es vom gleichen Typ oder einem zugelassenen Ersatztyp ist.

3.1.1 HR-Berechnungen

Für die HIMax Systeme wurden gemäß IEC 61508 die HR-Berechnungen durchgeführt.

Die Werte für HR werden auf Anfrage von HIMA mitgeteilt.

Die Sicherheitsfunktionen, bestehend aus einem sicherheitsbezogenen Loop (Eingang, Verarbeitungseinheit, Ausgang und sicherer Kommunikation zwischen HIMA Systemen), erfüllen in allen Kombinationen die oben beschriebenen Anforderungen.

3.1.2 Selbst-Test und Fehlerdiagnose

Das Betriebssystem der Module führt beim Start und im laufenden Betrieb umfangreiche Selbst-Tests durch. Getestet werden dabei vor allem:

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

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

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

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

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

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

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

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

3.1.3 PADT

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

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

3.1.4 Redundanz

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

Die Redundanz von Komponenten beeinträchtigt nicht die Sicherheit des Systems.. Auch bei redundanten Systemkomponenten ist SIL 4 gewährleistet.

3.1.5 Aufbau von Sicherheitssystemen nach dem Arbeitsstromprinzip

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

1. Der sichere 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 Modul muss mit einer Leitungsschluss- und Leitungsbruch-Überwachung ausgestattet sein. Die Leitungsschluss- 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.
- HIMax Module.
- Sensoren und Aktoren.

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

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

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

3.2 Sicherheitsrelevante Zeiten

Folgende Zeitparameter 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:

$\mathbf{t}_{RR} \leq \mathbf{t}_{SR}$

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

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

- Physikalische bedingte Verzögerungen, z. B. Schaltzeiten von externen Relais.
- Parametrierte Verzögerungen im Anwenderprogramm, z. B. durch Timer-Bausteine (TON, TOF).
- Verzögerung von Ausgangssignalen durch die Ausgangs-Störaustastung, siehe Kapitel 8.4.2.

Der Parameter *Sicherheitszeit [ms]* $\mathbf{t}_{SR}$ in den Eigenschaften der Ressource ist im Bereich von 20 … 22 500 ms in SILworX einstellbar.

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

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

3.2.3 Watchdog-Zeit (Ressource)

Die Watchdog-Zeit $\mathbf{t_{WD}}$ 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:

$\mathbf{t_{WD}} \quad \mathbf{\leq} \quad \mathbf{½ \times t_{SR}}$

$\mathbf{t_{WD}}$ Watchdog-Zeit (Ressource)

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

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 eingestellte Watchdog-Zeit größer als ½ mal die Sicherheitszeit der Ressource ist.

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

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

HINWEIS

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

Einstellungen vor jeder Online-Änderung genau prüfen!

3.2.4 Abschätzung der Watchdog-Zeit

HIMA empfiehlt für eine ausreichende Verfügbarkeit dringend folgende Einstellung:

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

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

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

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

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

3.2.5 Watchdog-Zeit durch Test ermitteln

Bei zeitkritischen Anwendungen oder Systemen mit mehr als einer Steuerung (PES) ist es notwendig, die Watchdog-Zeit $\mathbf{t}_{WD}$ während der Inbetriebnahme zu ermitteln. Dies muss im RUN-Betrieb unter Volllast geschehen. Dazu müssen alle projektierten Module gesteckt und alle konfigurierten Kommunikationsverbindungen (z. B. safe**ethernet** und weitere Protokolle) in Betrieb sein.

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

Test durchführen

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

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

7. Die maximale Ausführungsdauer der Anwenderprogramme (AP) im Control Panel ablesen und die Schwankungen und Lastspitzen nach Ablauf mehrere Minuten notieren.
   Danach $\mathbf{t}_{Spitze}$ berechnen:
   $\mathbf{t}_{Spitze}$ = Ausführungsdauer (max.) **–** Ausführungsdauer (min.), für jedes AP ausrechnen und diese Werte für alle AP addieren.
8. Nacheinander jedes Prozessormodul entfernen und wieder in den Basisträger einfügen. Jeweils vor dem Entfernen eines Prozessormoduls warten, bis sich das gerade eingefügte Prozessormodul synchronisiert hat.

i

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

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

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

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

10. Die notierten Zeiten in die folgende Formel einsetzen:

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

t_{Sync} Ermittelte Zeit für die Synchronisation eines Prozessormoduls.

$t_{Reserve}$ Sicherheitsreserve 12 ms.

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

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

$\mathbf{t_{Latenz}}$ Eingestellter Systemparameter *Maximale Systembus-Latenzzeit [µs]* x 4.

t_{Spitze} Summe aller in Schritt 7 errechneten AP-Lastspitzen.

3.3 Sicherheitsauflagen

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

3.3.1 Produktunabhängige Auflagen der Hardware

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

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

3.3.2 Produktabhängige Auflagen der Hardware

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

- An ein System müssen Geräte angeschlossen werden, die eine sichere elektrische Trennung zum Netz aufweisen.
- Für die Bearbeitung sicherheitsbezogener Aufgaben sind nur sicherheitsbezogene Module einzusetzen.
- Die im Systemhandbuch genannten Einsatzbedingungen sind einzuhalten, insbesondere hinsichtlich Versorgungsspannung und Belüftung.
- Zur Einhaltung der Schutzmaßnahmen in Bezug auf elektrische Sicherheit und Erdung muss der Hersteller der spezifischen Anwendung geeignete Trennungsmaßnahmen zwischen Innen- und Außenanlage entsprechend EN 50122 vorsehen. Die HIMax Systeme müssen dadurch gegen Einflüsse von Teilen der Außenanlage im Oberleitungs- und Stromabnehmerbereich und gegen Bahnrückströme gesichert werden. Es sind für den Bahnbereich zugelassene Energieversorgungseinrichtungen zu verwenden.

3.3.3 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.

3.3.4 Auflagen für die Verwendung des Programmierwerkzeugs

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

- Durch doppelte Kompilierung in SILworX mit Vergleich der beiden Konfigurations-CRCs wird sichergestellt, dass die Kompilierung korrekt erfolgte.
- 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 eine Erprobung erfolgen.
- Die Fehlerreaktion des Systems bei Fehlern in den fehlersicheren Eingangs- und Ausgangsmodulen muss gemäß den anlagenspezifischen sicherheitstechnischen Gegebenheiten durch das Anwenderprogramm festgelegt werden.
- Das Programmierwerkzeug SILworX hat eine Funktion, die nach einer Änderung des Anwenderprogramms oder der Systemkonfiguration nur die Änderungen anzeigt. Eine Analyse der Änderungen (Änderungsauswirkungsanalyse ÄAA) hat den notwendigen Testumfang zu definieren. Diese ÄAA hat die erwarteten Änderungen auf Basis der durchgeführten Modifikationen, die Ausgabe der Vergleichsfunktion von SILworX und notwendige Regressionstests zu berücksichtigen.

3.3.5 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 nicht die zulässige maximale Reaktionszeit überschreitet. Die im Kapitel 11.2 aufgeführten Berechnungsgrundlagen sind anzuwenden.
- Die Datenübertragung in Übertragungssystemen der Kategorie 1 und Kategorie 2 gemäß EN 50159 ist ohne zusätzliche Maßnahmen möglich.
- Die Anwendung in Übertragungssystemen der Kategorie 3 gemäß EN 50159 ist möglich, wenn zusätzliche Maßnahmen zur Gewährleistung der Sicherheit des Übertragungskanals getroffen werden (z. B. durch Firewalls oder Verschlüsselung).
- Die Standard-Protokolle dürfen nicht für die Übertragung von sicherheitsrelevanten Daten eingesetzt werden.
- An alle Kommunikationsschnittstellen dürfen nur Geräte angeschlossen werden, die eine sichere elektrische Trennung gewährleisten.

3.3.6 Auflagen für Bahnanwendungen

Folgende Auflagen sind beim Einsatz des HIMax Systems in Bahnanwendungen zu beachten:

- Das HIMax System kann in einer Umgebung mit Verschmutzungsgrad 2 und Überspannungskategorie 2 gemäß EN 50124-1 eingesetzt und betrieben werden.
- Für Bahnanwendungen sind die relevanten Normen anzuwenden.
- Die digitalen Ausgänge besitzen eine Leitungsschluss-Überwachung. Maßnahmen beim Ansprechen der Überwachung müssen durch das Anwenderprogramm erfolgen.
- Der Temperaturzustand (Betriebstemperatur) der HIMax Systeme ist durch das Anwenderprogramm auszuwerten. Sicherheitsbezogene Maßnahmen müssen ebenfalls durch das Anwenderprogramm erfolgen. Weitere Informationen finden Sie im HIMax Systemhandbuch HI 801 000 D, Kapitel *Überwachung der Temperatur*.
- Fehlermeldungen müssen durch das Anwenderprogramm ausgewertet werden. Fehler werden durch Statusbits signalisiert und stehen somit dem Anwenderprogramm zur Verfügung. Zusätzlich werden Fehler im Diagnosespeicher der Steuerung eingetragen und können mit dem Programmierwerkzeug ausgelesen werden. Weitere Informationen finden Sie im HIMax Systemhandbuch HI 801 000 D, Kapitel *Diagnose*).
- Eine Erdschlusserkennung ist extern zu konfigurieren.

3.4 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 (X-OPC DA, X-OPC AE).
- Optionale Kommunikationsverbindungen zu externen Systemen.

3.4.1 Produkteigenschaften

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

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

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

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

⚠ WARNUNG

Personenschaden durch unbefugte Manipulationen an Steuerungen möglich!

Steuerungen sind gegen unbefugte Zugriffe zu schützen:

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

3.4.2 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 Anwenders!**

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

3.5 Prüfbedingungen

Die Normen, nach denen das HIMax System für den industriellen Einsatz geprüft und zertifiziert ist, können dem Sicherheitshandbuch HI 801 002 D entnommen werden.

3.6 Zusätzliche Prüfbedingungen für Bahnanwendungen

Nachfolgende Tabelle zeigt die HIMax Komponenten, die für den Einsatz in Bahnanwendungen zugelassen sind:

Bezeichnung	Beschreibung
X-CPU 01	Prozessormodul
X-CPU 31	Prozessormodul
X-SB 01	Systembusmodul
X-COM 01	Kommunikationsmodul
X-AI 32 01	Analoges Eingangsmodul (32 Kanäle)
X-DI 32 01	Digitales Eingangsmodul (32 Kanäle)
X-DI 32 02	Digitales Eingangsmodul (32 Kanäle), für Näherungsschalter (NAMUR)
X-DI 32 03	Digitales Eingangsmodul (32 Kanäle), 48 VDC
X-DI 64 01	Digitales Eingangsmodul (64 Kanäle)
X-DO 12 01	Relaismodul (12 Kanäle)
X-DO 24 02	Digitales Ausgangsmodul (24 Kanäle), 48 VDC
X-DO 32 01	Digitales Ausgangsmodul (32 Kanäle)
X-BASE PLATE	HIMax Basisträger

Tabelle 2: Zugelassene HIMax Komponenten

3.6.1 Höhenbereich

Für die HIMax Komponenten gelten für den Höhenbereich folgende Klassen:

- Für den Einsatz in der Signaltechnik gemäß EN 50125-3: AX bis 2000 m.
- Für den Einsatz auf Bahnfahrzeugen gemäß EN 50125-1: AX bis 2000 m.

3.6.2 Klimatische Bedingungen

Die HIMax Komponenten wurden gemäß EN 50125-3 und EN 50155 geprüft.

3.6.2.1 Einsatz in der Signaltechnik

Für den Temperaturbereich 0 … +60 °C lassen sich gemäß der EN 50125-3 folgende Klimaklassen ableiten:

- Im Container mit Temperaturüberwachung: T1, T2 und TX.
- Im nicht klimatisierten Gebäude: T1.
- Im klimatisierten Gebäude: T1, T2 und TX.

3.6.2.2 Einsatz auf Bahnfahrzeugen

Für den Einsatz auf Bahnfahrzeugen können die HIMax Module keiner Temperaturklasse gemäß EN 50155 zugeordnet werden.

i Der Anwender muss durch geeignete Maßnahmen in der Anwendung sicherstellen, dass der Temperaturbereich der HIMax von 0 … 60 °C eingehalten wird.

Für die erweiterte Betriebstemperatur beim Einschalten gilt für das HIMax System die Klasse ST0, wie im Kapitel 4.3.3 der EN 50155 definiert.

Für die schnelle Temperaturänderung gilt für das HIMax System die Temperaturänderungsklasse H1, wie im Kapitel 4.3.4 der EN 50155 definiert.

Da die Platinen in den Modulen des HIMax Systems mit einem Schutzüberzug beschichtet sind, besitzen diese die Schutzlackierungsklasse PC2, wie im Kapitel 10.7 der EN 50155 definiert.

3.6.3 Mechanische Bedingungen

Die HIMax Komponenten wurden gemäß EN 50125-3 und EN 50155 geprüft.

3.6.3.1 Einsatz in der Signaltechnik

Die wichtigsten Prüfungen und Grenzwerte für mechanische Bedingungen sind in nachstehender Tabelle aufgelistet:

Prüfnorm	Mechanische Prüfungen
EN 50125-3	Unempfindlichkeitsprüfung gegen Schwingungen: 2,3 m/s^2 zwischen 5 … 2000 Hz, Prüfling in Betrieb
	Unempfindlichkeitsprüfung gegen Schocken: 20 m/s^2, 11 ms, Prüfling in Betrieb

Tabelle 3: Mechanische Bedingungen für Einsatz in der Signaltechnik

3.6.3.2 Einsatz auf Bahnfahrzeugen

Die in Tabelle 2 aufgeführten HIMax Komponenten wurden gemäß der EN 50155 mechanisch geprüft. Die Prüfung erfolgte gemäß EN 61373, Kategorie 1, Klasse B.

Das HIMax System verfügt über keine Sockel für integrierte Schaltungen und/oder Randsteckverbinder. Aus diesem Grund wird die Klasse K2, wie im Kapitel 10.1.5 der EN 50155 definiert, eingehalten.

3.6.4 EMV-Bedingungen

Die in Tabelle 2 aufgeführten HIMax Komponenten wurden gemäß den EMV-Anforderungen der EN 50121-4 und EN 50121-3-2 positiv getestet.

3.6.4.1 Einsatz in der Signaltechnik

Die wichtigsten Prüfungen und Grenzwerte für EMV-Bedingungen sind in nachstehender Tabelle aufgelistet:

Prüfnorm	Art der Prüfung	Prüfungen der Störfestigkeit	
EN 61000-4-2	ESD-Prüfung	6 kV Kontakt-, 8 kV Luftentladung	
EN 61000-4-3	EM-Feld	80 MHz … 1 GHz:	10 V/m
		800 MHz … 1 GHz:	20 V/m
		1,4 GHz … 2 GHz:	10 V/m
		2 GHz … 2,7 GHz:	5 V/m
		5,1 GHz … 6 GHz:	3 V/m
EN 61000-4-4	Burst-Prüfung	Versorgungsspannung:	2 kV
		E/A-Leitungen:	2 kV
		Erdanschluss:	1 kV
EN 61000-4-5	Surge	Versorgungsspannung:	2 kV CM
			1 kV DM
		E/A-Leitungen:	2 kV CM
			1 kV DM
EN 61000-4-6	Einströmung	Versorgungsspannung:	10 V
		E/A-Leitungen:	10 V
		Erdanschluss:	10 V
EN 61000-4-8	Magnetfeld mit Netzfrequenz	16 2/3 Hz, 50 Hz, 60 Hz:	100 A/m
		DC:	300 A/m

Tabelle 4: EMV-Bedingungen für Einsatz in der Signaltechnik gemäß EN 50121-4

i Werden die Module X-DI 32 03, X-DI 64 01, X-DO 24 02 und X-DO 32 01 eingesetzt, sind zur Einhaltung der Funkstörspannung folgende Maßnahmen erforderlich:

- Klappferrit WE 742 715 5 mit 7 Windungen auf der 24-V-Versorgungsspannung des Systems.
- Klappferrit WE 742 715 5 mit 4 Windungen auf der 48-V-Versorgungsspannung der X-DO 24 02.
- Klappferrit WE 742 715 5 mit 4 Windungen auf der 48-V-Versorgungsspannung der X-DI 32 03.

i Wird das Modul X-DO 24 02 mit einer externen 24-V-Versorgungsspannung aus einem DC-Netz versorgt, so muss das Netzfilter H 7013 in unmittelbarer Nähe des Versorgungsspannungsanschlusses des Moduls eingebaut sein. Bei 48 VDC ist das entsprechende Netzfilter H 7021 einzusetzen.

3.6.4.2 Einsatz auf Bahnfahrzeugen

Die wichtigsten Prüfungen und Grenzwerte für EMV-Bedingungen sind in nachstehender Tabelle aufgelistet:

Prüfnorm	Art der Prüfung	Prüfungen der Störfestigkeit	
EN 61000-4-2	ESD-Prüfung	6 kV Kontakt-, 8 kV Luftentladung	
EN 61000-4-3	EM-Feld	80 MHz … 1 GHz: 1,4 GHz … 2GHz: 2 GHz … 2,7 GHz: 5,1 GHz … 6 GHz:	20 V/m 10 V/m 5 V/m 3 V/m
EN 61000-4-4	Burst-Prüfung	Versorgungsspannung: E/A-Leitungen:	2 kV 2 kV
EN 61000-4-5	Surge	Versorgungsspannung:	2 kV CM 1 kV DM
EN 61000-4-6	Einströmung	Versorgungsspannung: E/A-Leitungen:	10 V 10 V

Tabelle 5: EMV-Bedingungen für Einsatz auf Bahnfahrzeugen gemäß EN 50121-3-2

3.6.5 Erschwerte Bedingungen

Das HIMax System muss zum Schutz gegen Umwelteinflüsse der Klassen 4C3, 4B1 und 4S2 in einem geschlossenen Schrank geeigneter Schutzart, z. B. IP54, eingebaut werden.

3.6.6 Versorgungsspannung

Die wichtigsten Prüfungen und Grenzwerte für die Versorgungsspannung der HIMax Komponenten sind in nachstehender Tabelle aufgelistet:

IEC/EN 61131-2	Nachprüfung der Eigenschaften der Gleichstromversorgung
	Die Spannungsversorgung muss alternativ folgende Normen erfüllen: IEC/EN 61131-2 oder SELV (Safety Extra Low Voltage) oder PELV (Protective Extra Low Voltage)
	Die Absicherung der HIMax Geräte muss gemäß den Angaben der Handbücher X-BASE PLATE, HI 801 024 D und HI 801 370 D, erfolgen.
	Prüfung des Spannungsbereiches: 24 VDC, -20 … +25 % (19,2 … 30,0 V)
	Prüfung auf Unempfindlichkeit gegen Kurzzeitunterbrechung der externen Stromversorgung: DC, PS 2: 2 ms
	Polaritätsumkehr der Versorgungsspannung: Hinweis im entsprechenden Kapitel des Systemhandbuchs oder im Datenblatt der Stromversorgung.
	Pufferdauer, Beständigkeitsprüfung: Prüfung B, 1000 h

Tabelle 6: Nachprüfung der Eigenschaften der Gleichstromversorgung

3.6.6.1 Bedingungen an die Versorgungsspannung auf Bahnfahrzeugen

Die Versorgung des HIMax Systems aus einer Akkumulatorbatterie erfolgt mit einer Nennspannung von 24 V.

Für die Versorgungsspannung der HIMax gilt: 24 VDC, -15 … +20 %, 5 % Welligkeit.

Damit ergeben sich die folgenden Toleranzen:

- Niedrigste Dauerspannung: 19,2 V (0,8 UN).
- Höchste Dauerspannung: 30 V (1,25 UN).

Die in Tabelle 2 aufgeführten HIMax Komponenten wurden gemäß EN 50155, Kapitel 5.1 getestet.

Der Anwender muss durch externe Maßnahmen sicherstellen, dass eine niedrigste Dauerspannung von 0,8 UN eingehalten wird, da sonst einzelne Module oder das ganze System einen Reboot durchführen.

Spannungsschwankungen über 1,25 UN gemäß EN 50155, Kapitel 5.1.1.3, müssen mittels externer Maßnahmen durch den Anwender abgefangen werden.

HIMax Systeme sind für Unterbrechungen bis zu 2 ms ausgelegt. Damit erfüllt die HIMax die Anforderungen der Klasse S1 gemäß EN 50155, Kapitel 5.1.1.4.

Das HIMax System erfüllt die Bedingungen für den Gleichspannungswelligkeitsfaktor gemäß EN 50155, Kapitel 5.1.1.6.

Die Bedingungen gemäß EN 50155, Kapitel 5.1.3, für das Umschalten zwischen 2 Versorgungsspannungen werden nicht erfüllt. Es sind externe Maßnahmen durch den Anwender erforderlich.

4 Prozessormodul

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

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

4.1 Prozessormodul X-CPU 01

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

4.2 Prozessormodul X-CPU 31

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

4.3 Selbst-Tests

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

Getestet werden hauptsächlich:

- Die Mikroprozessoren.
- Die redundanten Speicher.
- Die nicht-flüchtigen Speicher.
- Der Watchdog.
- Der Hardware-Vergleicher.

4.4 Reaktionen auf Fehler im Prozessormodul

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

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

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

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

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

4.5 Austausch von Prozessormodulen

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

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

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

HINWEIS

Unterbrechung des sicherheitsbezogenen Betriebs möglich!

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

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

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

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

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

5 Systembusmodul

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

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

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

5.1 Rack-ID

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

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

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

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

5.2 Attribut *Responsible*

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

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

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

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

⚠ WARNUNG

Personenschaden möglich!

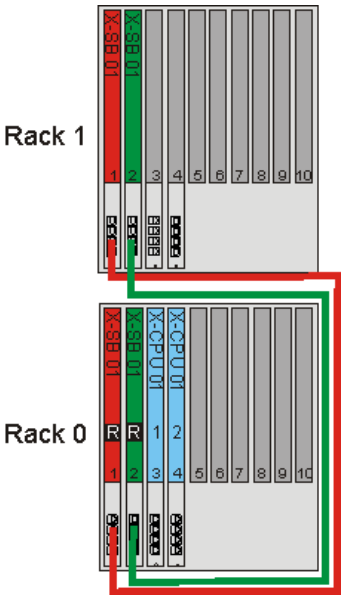
Die Parametrierung muss mit Hilfe von SILworX verifiziert werden.

Dabei ist unbedingt folgende Vorgehensweise einzuhalten:

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

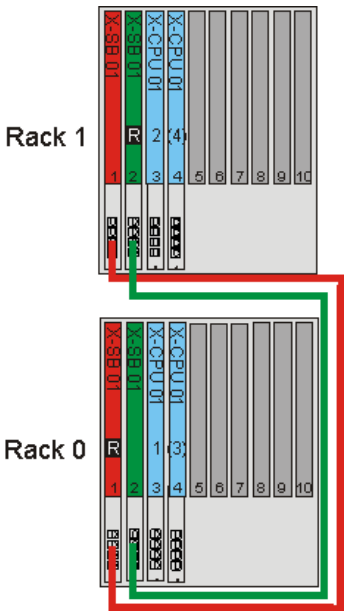
Empfohlene Konfigurationen:

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



R Systembusmodul ist responsible

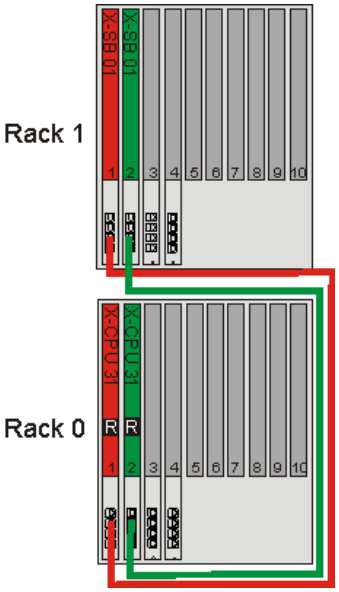
Bild 1: Empfohlene Konfiguration: alle Prozessormodule auf Rack 0



R Systembusmodul ist responsible

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

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



R Prozessormodul ist responsible

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

6 Kommunikationsmodul

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

- Das Prozessormodul steuert den sicherheitsbezogenen Datenverkehr durch das sicherheitsbezogene Übertragungsprotokoll safe**ethernet**. 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 Standardprotokolle sind z. B.:
  - Modbus
  - PROFIBUS Master/Slave
  - Send/Receive TCP
  - PROFINET-IO
  - SNTP

Weitere Informationen zu Kommunikation und Kommunikationsmodulen finden Sie in folgenden Dokumenten:

- Kapitel 11.1 dieses Handbuchs
- Handbuch des Kommunikationsmoduls HI 801 010 D
- Kommunikationshandbuch HI 801 100 D
- Systemhandbuch HI 801 000 D

7 Eingangsmodule

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

Digitale Eingangsmodule [1)]	Kanäle	Sicherheitsbezogen	Anmerkung
X-DI 32 01	32	SIL 4	
X-DI 32 02	32	SIL 4	Näherungsschalter (NAMUR)
X-DI 32 03	32	SIL 4	48 VDC
X-DI 64 01	64	SIL 4	
Analoge Eingangsmodule [1)]	Kanäle	Sicherheitsbezogen	Anmerkung
X-AI 32 01	32	SIL 4	

[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 7: Übersicht Eingangsmodule

7.1 Allgemeines

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!

Zu den Diagnose-LEDs der Module erzeugen die Steuerungen Fehler- und Statusmeldungen, die gespeichert werden. Das PADT kann diese im Diagnose-Speicher gespeicherten Meldungen auslesen.

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

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

Weitere Informationen zu den Eingangsmodulen finden Sie in den Modulhandbüchern.

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). Das Modul aktiviert die LED *Error*.

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

7.3 Sicherheit von Sensoren, Encodern und Transmittern

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

7.4 Sicherheitsbezogene digitale Eingangsmodule

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

7.4.1 Test-Routinen

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

7.4.2 Redundanz von digitalen Eingängen

Digitale Eingänge redundant zu verschalten, ist zulässig. Die redundante Verschaltung dient der Erhöhung der Verfügbarkeit der Eingänge.

7.4.3 Surge auf digitalen Eingängen

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

Bei Verwendung abgeschirmter Kabel für digitale Eingänge sind keine weiteren Maßnahmen zur Vorsorge für 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 801 000 D und der relevanten Normen.

7.5 Sicherheitsbezogene analoge Eingangsmodule

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

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

7.5.1 Test-Routinen

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

7.5.2 Redundanz von analogen Eingängen

Analoge Eingänge redundant zu verschalten, ist zulässig. Die redundante Verschaltung dient normalerweise der Erhöhung der Verfügbarkeit.

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

Für sicherheitsbezogene Anwendungen des Modules X-AI 32 01 gilt:

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

Im Fehlerfall liefern die Zustandsvariablen den Wert FALSE.

7.6 Checklisten Eingänge

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

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

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

8 Ausgangsmodule

Digitale Ausgangsmodule	Kanäle	Sicherheitsbezogen	Anmerkung
X-DO 24 02	24	SIL 4	48 VDC, ≤ 0,5 A
X-DO 32 01	32	SIL 4	24 VDC, ≤ 0,5 A
Relais-Modul [1)]			
X-DO 12 01	12	SIL 4	230 VAC/VDC
[1)] Sicher elektrisch getrennt.			

Tabelle 8: Übersicht Ausgangsmodule

8.1 Allgemeines

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

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

Mit der Verwendung des jeweiligen Fehlercodes gibt es zusätzliche Möglichkeiten, Fehlerreaktionen im Anwenderprogramm zu programmieren.

Weitere Informationen zu den Ausgangsmodulen finden Sie in den Modulhandbüchern.

8.2 Reaktion im Fehlerfall

Wenn die Test-Routinen bei Ausgängen einen Fehler feststellen, schaltet die Steuerung im Fehlerfall den jeweiligen Ausgang ab, also in den sicheren Zustand. Das Modul aktiviert die LED *Error*.

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

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

8.3 Sicherheit von Aktoren

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

8.4 Sicherheitsbezogene digitale Ausgangsmodule

In den sicherheitsbezogenen Ausgangskanälen sind zusätzlich zur Einzelkanalabschaltung drei testbare Schalter in Serie integriert. Somit ist die Anforderung für SIL 4 nach einem sicheren, unabhängigen zweiten Abschaltweg erfüllt. Diese integrierte Sicherheitsabschaltung schaltet im Fehlerfall die einzelnen Kanäle des defekten Ausgangsmoduls sicher ab (energieloser Zustand).

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

8.4.1 Test-Routinen

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

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

8.4.2 Ausgangs-Störaustastung

Ist die Ausgangs-Störaustastung aktiviert, verzögert das Ausgangsmodul die Abschaltreaktion eines Kanals.

Bei aktivierter Ausgangs-Störaustastung ist zu berücksichtigen, dass bei Unterdrückung einer transienten Störung sich die Reaktion auf den Wert *Sicherheitszeit – Watchdog-Zeit* verlängern kann.

In allen Fällen wird der Fehler zusätzlich mit der LED *Error* auf der Frontplatte angezeigt.

8.4.3 Verhalten bei externem Kurzschluss oder Überlast

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

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

8.4.4 Redundanz von digitalen Ausgängen

Digitale Ausgänge redundant zu verschalten, ist zulässig. Eine redundante Verschaltung dient der Erhöhung der Verfügbarkeit.

8.5 Sicherheitsbezogene Relaismodule

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

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

Beim Modul sind die Ausgänge mit zwei Sicherheitsrelais mit zwangsgeführten Kontakten ausgestattet. Damit können die Ausgänge für Sicherheitsabschaltungen entsprechend SIL 4 verwendet werden.

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

8.5.1 Test-Routinen

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

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

8.5.2 Redundanz von Relaisausgängen

Digitale Relaisausgänge redundant zu verschalten ist zulässig. Die redundante Verschaltung dient der Erhöhung der Verfügbarkeit der Relaisausgänge.

8.6 Checklisten Ausgänge

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

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

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

9 Software

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

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

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

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

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

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

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 einige 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 Kapitel 5.1 und das Systemhandbuch HI 801 000 D.**
- **Responsible-Attribut von Systembusmodulen oder Prozessormodulen, siehe Kapitel 5.1.**
- **Die in der Tabelle 9 hervorgehobenen 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.

Systemparameter	S [1)]	Beschreibung	Einstellung für sicheren Betrieb
Name	N	Name der Ressource	Beliebig
System-ID [SRS]	J	System-ID der Ressource Wertebereich: 1 … 65 535 Standardwert: 60 000 Es ist notwendig, der System-ID einen anderen Wert als den Standardwert zu zuweisen, sonst ist das Projekt nicht ablauffähig!	Eindeutiger Wert innerhalb des Netzwerks der Steuerungen. Das sind alle Steuerungen, die potenziell miteinander verbunden sind.
Sicherheitszeit [ms]	J	Sicherheitszeit der Ressource in Millisekunden, siehe Kapitel *Sicherheitsrelevante Zeiten* im Sicherheitshandbuch. Wertebereich: 20 … 22 500 ms. Standardwert: 600 ms (online änderbar)	Applikationsspezifisch
Watchdog-Zeit [ms]	J	Watchdog-Zeit in Millisekunden, siehe Kapitel *Sicherheitsrelevante Zeiten* im Sicherheitshandbuch. Wertebereich: 6 … 7500 ms Standardwert: 200 ms (online änderbar)	Applikationsspezifisch
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 einstellbaren 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.	Applikationsspezifisch
Sollzykluszeit-Modus	N	Verwendung der *Sollzykluszeit [ms],* siehe nachfolgende Kapitel. Die Standardeinstellung ist fest-tolerant (online änderbar).	Applikationsspezifisch
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	Applikationsspezifisch
Max. Kom.-Zeitscheibe [ms]	N	Höchstwert in ms der Zeitscheibe, die innerhalb des Zyklus der Ressource für Kommunikation verwendet wird, siehe Kommunikationshandbuch HI 801 100 D. Wertebereich: 2 … 5000 ms Standardwert: 60 ms	---

Systemparameter	S [1)]	Beschreibung		Einstellung für sicheren Betrieb
Optimierte Nutzung der Kom.-Zeitscheibe	N	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 Konfigurationsverbindungen [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.		Applikationsspezifisch
Maximale Systembus-Latenzzeit [µs]	N	Maximale Verzögerung einer Nachricht zwischen einem E/A-Modul und einem Prozessormodul. 100 … 50 000 µs, Standardwert: *System-Standardwerte* i Für die Einstellung der maximalen Systembuslatenz auf einen Wert ≠ *System-Standardwerte* ist eine Lizenz erforderlich.		Applikationsspezifisch
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. Standardwert: TRUE.	HIMA empfiehlt die Einstellung FALSE.
		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.		

Systemparameter	S [1)]	Beschreibung		Einstellung für sicheren Betrieb
Autostart	J	TRUE:	Wenn die Steuerung an die Versorgungsspannung angeschlossen wird, starten die Anwenderprogramme automatisch. Standardwert: TRUE.	Applikationsspezifisch
		FALSE:	Kein automatischer Start nach Zuschalten der Versorgungsspannung.	
		Einstellungen in den Programm-Eigenschaften der Ressource beachten!		
Start erlaubt	J	TRUE:	Kaltstart oder Warmstart durch PADT im Zustand RUN oder STOPP erlaubt. Standardwert: TRUE.	Applikationsspezifisch
		FALSE:	Kein Start erlaubt.	
Laden erlaubt	J	TRUE:	Download der Konfiguration erlaubt. Standardwert: TRUE.	Applikationsspezifisch
		FALSE:	Kein Start erlaubt.	
Reload erlaubt	J	TRUE:	Reload der Konfiguration erlaubt. Standardwert: TRUE.	Applikationsspezifisch
		FALSE:	Reload der Konfiguration nicht erlaubt. Ein laufender Reload-Prozess wird beim Umschalten auf FALSE nicht abgebrochen.	
Globales Forcen erlaubt	J	TRUE:	Globales Forcen für diese Ressource erlaubt. Standardwert: TRUE.	Applikationsspezifisch
		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.		Applikationsspezifisch
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.	Applikationsspezifisch
		FALSE:	Anwender mit MultiForcen-Zugriff können keine globale Variablen forcen. Standardwert: FALSE (online änderbar).	

Systemparameter	S [1)]	Beschreibung		Einstellung für sicheren Betrieb
Minimale Konfigu-rations-version	N	Mit dieser Einstellung ist es möglich, Code zu generieren, der entsprechend den Projektanforderungen zu alten oder zu neuen Versionen des HIMax Betriebssystems kompatibel ist. Standardwert: SILworX V11 bei neuen Projekten.		Applikations-spezifisch
		SILworX V2	Codegenerierung erfolgt wie bei SILworX V2 für HIMax vor V3.	
		SILworX V3	Codegenerierung wie SILworX V3 für HIMax V3.	
		SILworX V4	Codegenerierung wie SILworX V4 für HIMax V4.	
		SILworX V5	Codegenerierung wie SILworX V5 für HIMax V5.	
		SILworX V6	Codegenerierung wie SILworX V6.48 für HI-Max V6.	
		SILworX V6b	Codegenerierung wie SILworX V6.114 für HIMax V6.	
		SILworX V7	Codegenerierung wie SILworX V7 für HIMax V7.	
		SILworX V8	Codegenerierung wie SILworX V8 für HIMax V8.	
		SILworX V9	Codegenerierung wie SILworX V9 für HIMax V9.	
		SILworX V10	Codegenerierung wie SILworX V10 für HIMax V10.	
		SILworX V11	Codegenerierung wie SILworX V11 für HIMax V11.	
Schneller Hoch-lauf	N	Für HIMax nicht anwendbar.		---
[1)] Systemparameter wird vom Betriebssystem sicherheitsbezogen behandelt, ja (J) oder nein (N).				

Tabelle 9: 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.

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

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

Einstellung	Beschreibung
fest	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 10: 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. Auch wenn die Protokollverarbeitung innerhalb der Dauer einer Kommunikationszeitscheibe nicht beendet werden konnte, führt die CPU dennoch die sicherheitsrelevanten Überwachungen für alle Protokolle in einem CPU-Zyklus aus.

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

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

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

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

Ermitteln der tatsächlichen Dauer der maximalen Kommunikationszeitscheibe

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

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

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 Betriebssysteme HIMax CPU ≤ V3 wird $\mathbf{t}_{Konfig}$ von SILworX mit 6 ms vorgegeben. Jedoch darf die Verarbeitungsdauer der genannten Tasks in einem CPU-Zyklus die Vorgabe überschreiten.

Für die Betriebssysteme HIMax CPU ≥ V4 wird $\mathbf{t}_{Konfig}$ wie folgt berechnet:

X-CPU 01: $\mathbf{t}_{Konfig} = (\mathbf{n}_{Com} + \mathbf{n}_{PADT} + \mathbf{n}_{RIO}) * 0{,}25\ ms + 4\ ms + 4 * (\mathbf{t}_{Latenz} * 2 + 0{,}31\ ms)$

X-CPU 31: $\mathbf{t}_{Konfig} = (\mathbf{n}_{Com} + \mathbf{n}_{PADT}) * 1\ ms + \mathbf{n}_{RIO} * 0{,}25\ ms + 4\ ms + 4 * (\mathbf{t}_{Latenz} * 2 + 0{,}8\ ms)$

t_{Konfig}:	Systemparameter *Max. Dauer Konfigurationsverbindungen [ms]*
n_{COM}:	Anzahl Module mit Ethernet-Schnittstellen (X-SB, X-CPU, X-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.

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

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

Bei der Codegenerierung und bei der Projektkonvertierung wird im Logbuch des PADTs ein Hinweis ausgegeben, wenn $\mathbf{t}_{Konfig}$ 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

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

[1)] Maximale Systembus-Latenzzeit einschließlich maximaler zusätzlicher Verzögerung durch die Netzwerk-Infrastruktur

Tabelle 11: Standardwerte der maximalen Systembus-Latenzzeit

9.4.1.6 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.

9.4.1.7 Systemvariable des Racks

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

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

Tabelle 12: Systemvariable der Hardware

Diesen Systemvariablen lassen sich globale Variable 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 Systemvariablen *Read-only in RUN*, *Reload-Deaktivierung*, *Force-Deaktivierung* und *MultiForcen gesperrt*.

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

Beispiel: Steuerung abschließbar machen

1. Globale Variablen vom Typ BOOL definieren, Initialwerte auf FALSE setzen.
2. Globale Variablen den oben genannten Systemvariablen als Ausgangsvariable zuweisen.
3. Globale Variable dem Kanalwert eines digitalen Eingangs zuweisen.
4. Schlüsselschalter an den digitalen Eingang anschließen.
5. Programm kompilieren, auf die Steuerung laden und starten.

► Der Besitzer eines passenden Schlüsselschalters kann die Steuerung ab- und aufschließen. Bei einem Fehler im entsprechenden digitalen Eingangsmodul wird die Steuerung automatisch aufgeschlossen.

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

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 HIMax 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.

Weitere Informationen zum Forcen finden Sie im Systemhandbuch HI 801 000 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 4-Qualität und dient als Nachweis gegenüber Prüfstellen.

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

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

10 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 HIMax).
- 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 HIMax Systemen für sicherheitstechnische Anwendungen ist in folgenden Schritten durchzuführen:

1. Steuerungsfunktionen spezifizieren.
2. Anwenderprogramme schreiben.
3. Anwenderprogramme mit dem C-Code-Generator kompilieren.
   - Die Anwenderprogramme sind fehlerfrei erzeugt und lauffähig.
4. Anwenderprogramme verifizieren und validieren.
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 *ab SILworX V7* bei allen neuen Projekten.		

[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 13: 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 vollständigen Eingabe des Anwenderprogramms und der E/A-Belegung der Steuerung wird der Code erzeugt. Dabei wird der Konfigurations-CRC, die Prüfsumme über die Konfigurationsdateien, gebildet.

Dieser ist eine Signatur über die gesamte Konfiguration und wird als Hex-Code im 32-Bit-Format ausgegeben. Alle konfigurierbaren oder veränderbaren Elemente wie Logik, Variablen, Schaltereinstellungen fließen darin ein.

i Vor dem Laden des Anwenderprogramms für den sicherheitsbezogenen Betrieb muss der Anwender dieses unbedingt zweimal kompilieren. Die beiden erzeugten Versionen müssen dieselben Prüfsummen haben.

In der Standardeinstellung kompiliert SILworX die Ressource-Konfiguration automatisch zweimal und vergleicht die Prüfsummen.

Das Ergebnis des CRC-Vergleichs ist im Logbuch zu sehen.

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

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

Für Fehlersuche kann das Anwenderprogramm beim Online-Test in Einzelschritten, d. h., Zyklus für Zyklus, ausgeführt werden. Jeder Zyklus wird durch ein Kommando vom PADT ausgelöst. In der Zeit zwischen zwei Zyklen sind die von diesem Anwenderprogramm beschriebenen globalen Variablen **eingefroren**. Dadurch reagieren die zugeordneten physikalischen Ausgänge und Kommunikationsdaten nicht mehr auf Prozessänderungen!

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 14: Anwenderprogramm-Parameter *Testmodus erlaubt*

HINWEIS

Störung des sicherheitsbezogenen Betriebs möglich!

Ist das Anwenderprogramm im Testmodus angehalten, kann es nicht auf Eingänge sicherheitsbezogen reagieren und Ausgänge ansteuern! Die Werte der Ausgänge können sich in diesem Zustand nicht ändern.

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 15 online in der Steuerung zu ändern.

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

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

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

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

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

Tabelle 15: 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 HIMax Systems, bis zu 32 Anwenderprogramme innerhalb des Prozessormoduls abzuarbeiten.

Die einzelnen Anwenderprogramme lassen sich unabhängig voneinander starten und stoppen.

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

$\text{Watchdog-Zeit}_{\text{Anwenderprogramm}}$ = $\text{Watchdog-Zeit}_{\text{Prozessormodul}}$ 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 801 000 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 HIMax, 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, dient aber gleichzeitig auch als Nachweis für eine sorgfältig durchgeführte Planung.

Die aktuellen Checklisten können über die E-Mail-Adresse documentation@hima.com angefragt werden. Für registrierte Kunden 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!

Die folgenden Standardprotokolle stehen zur Verfügung:

- Auf den Ethernet-Schnittstellen des Kommunikationsmoduls:
  - Modbus-TCP (Master/Slave)
  - Modbus redundant (Slave).
  - SNTP
  - Send/Receive TCP
  - PROFINET-IO (Controller, Device).
- Auf den Feldbus-Schnittstellen (RS 485) des Kommunikationsmoduls je nach Ausführung des Geräts:
  - Modbus (Master/Slave).
  - Modbus redundant (Slave).
  - PROFIBUS-DP (Master/Slave).

11.2 Sicherheitsbezogenes Protokoll safe**ethernet**

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

Weitere Informationen zu safe**ethernet** finden Sie im Kommunikationshandbuch HI 801 100 D.

HINWEIS

Unbeabsichtigter Übergang in den sicheren Zustand möglich!

***ReceiveTMO* ist ein sicherheitsbezogener Parameter!**

ReceiveTMO ist die Überwachungszeit auf PES 1, innerhalb der eine korrekte Antwort von PES 2 empfangen werden muss.

i ReceiveTMO gilt ebenso in umgekehrter Richtung von PES 2 nach PES 1!

Trifft innerhalb der *ReceiveTMO* keine korrekte Antwort des Kommunikationspartners ein, schließt HIMax 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 * *Sollzykluszeit*
2. ReceiveTMO ≤ 5 * *Sollzykluszeit* + 4 * 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 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 HIMax Steuerung	Für weitere Informationen zur Reaktionszeit der HIMax 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 16: Beschreibung safe**ethernet** Parameter und Bedingungen

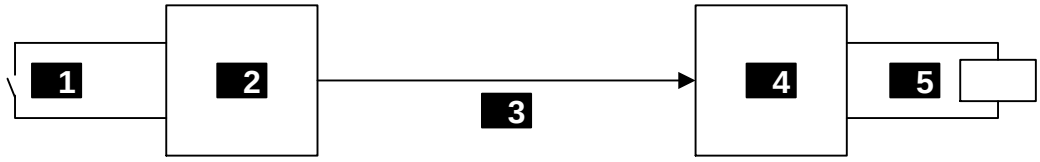
Für die folgenden Berechnungen der zulässigen maximalen Reaktionszeiten gelten folgende Bedingungen:

- 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 max. Reaktionszeit zweier HIMax Steuerungen

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



1 Eingang
2 HIMax Steuerung 1
3 Sicherheitsbezogenes Protokoll
4 HIMax Steuerung 2
5 Ausgang

Bild 4: Reaktionszeit bei Verbindung zweier HIMax Steuerungen

$T_R = t_1 + t_2 + t_3$

T_R Worst Case Reaction Time

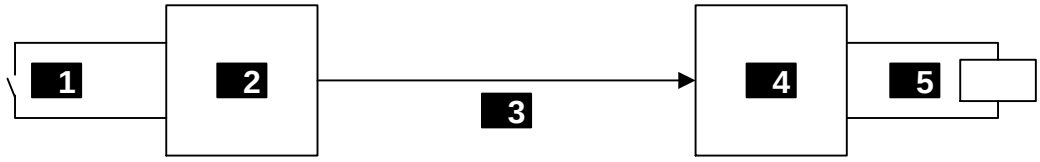
t_1 Sicherheitszeit der HIMax Steuerung 1

t_2 *ReceiveTMO*

t_3 Sicherheitszeit der HIMax Steuerung 2

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 HIMax Steuerung bis zur Reaktion des Ausgangs (Out) der HIMatrix Steuerung wie folgt berechnen:



1 Eingang
2 HIMax Steuerung
3 Sicherheitsbezogenes Protokoll
4 HIMatrix Steuerung
5 Ausgang

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

$T_R = t_1 + t_2 + t_3$

T_R Worst Case Reaction Time

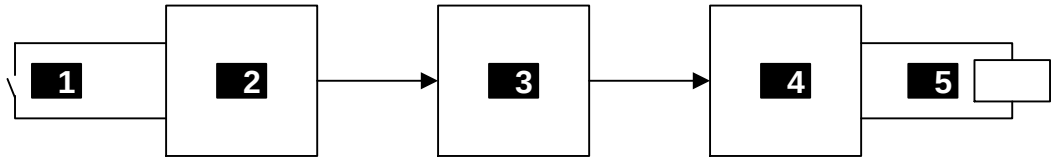
t_1 Sicherheitszeit der HIMax Steuerung

t_2 *ReceiveTMO*

t_3 2 * Watchdog-Zeit der HIMatrix Steuerung

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 HIMax Steuerung
4 Remote I/O 2
5 Ausgang

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

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

T_R Worst Case Reaction Time

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

t_2 *ReceiveTMO1*

t_3 2 * Watchdog-Zeit der HIMax Steuerung

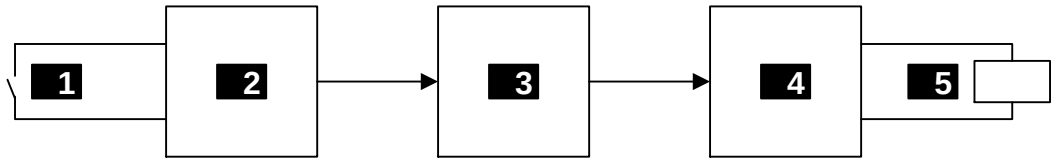
t_4 *ReceiveTMO2*

t_5 2 * Watchdog-Zeit der HIMatrix Steuerung 2 oder 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 HIMax und einer HIMatrix Steuerung

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



1 Eingang
2 HIMax Steuerung 1
3 HIMatrix Steuerung
4 HIMax Steuerung 2
5 Ausgang

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

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

T_R	Worst Case Reaction Time
t_1	Sicherheitszeit des HIMax Steuerung 1
t_2	*ReceiveTMO1*
t_3	2 * Watchdog-Zeit des HIMatrix Steuerung
t_4	*ReceiveTMO2*
t_5	Sicherheitszeit der HIMax Steuerung 2

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

11.4 Sicherheitsbezogenes Protokoll PROFIsafe

Auflagen zur Einsatz des PROFIsafe Protokolls sind im Kommunikationshandbuch HI 801 100 D gegeben. Die Auflagen sind zu beachten.

Formeln zur Berechnung der Reaktionszeit sind ebenfalls dem Kommunikationshandbuch zu entnehmen.

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
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
PE	Protective Earth: Schutzerde
PELV	Protective Extra Low Voltage: Funktionskleinspannung mit sicherer Trennung
PES	Programmierbares Elektronisches System
R	Read: Auslesen einer Variablen
Rack-ID	Identifikation eines Basisträgers (Nummer)
rückwirkungsfrei	Eingänge sind für rückwirkungsfreien Betrieb ausgelegt und können in Schaltungen mit Sicherheitsfunktionen eingesetzt werden.
R/W	Read/Write (Spaltenüberschrift für Art von Systemvariable)
SB	Systembus (-modul)
SELV	Safety Extra Low Voltage: Schutzkleinspannung
SFF	Safe Failure Fraction: Anteil der sicher beherrschbaren Fehler
SIL	Safety Integrity Level (nach IEC 61508)
SILworX	Programmierwerkzeug
SNTP	Simple Network Time Protocol (RFC 1769)
SRS	System.Rack.Slot: Adressierung eines Moduls
SW	Software
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

Bild 1: Empfohlene Konfiguration: alle Prozessormodule auf Rack 0 33
Bild 2: Empfohlene Konfiguration: Prozessormodule X-CPU 01 auf Rack 0 und Rack 1 33
Bild 3: Konfiguration mit Prozessormodulen X-CPU 31 auf Rack 0, Steckplätze 1 und 2 34
Bild 4: Reaktionszeit bei Verbindung zweier HIMax Steuerungen 71
Bild 5: Reaktionszeit bei Verbindung einer HIMax mit einer HIMatrix Steuerung 71
Bild 6: Reaktionszeit mit zwei Remote I/Os und einer HIMax Steuerung 72
Bild 7: Reaktionszeit mit zwei HIMax Steuerungen und einer HIMatrix Steuerung 72

Tabellenverzeichnis

Tabelle 1: Übersicht Systemdokumentation 13
Tabelle 2: Zugelassene HIMax Komponenten 25
Tabelle 3: Mechanische Bedingungen für Einsatz in der Signaltechnik 26
Tabelle 4: EMV-Bedingungen für Einsatz in der Signaltechnik gemäß EN 50121-4 27
Tabelle 5: EMV-Bedingungen für Einsatz auf Bahnfahrzeugen gemäß EN 50121-3-2 28
Tabelle 6: Nachprüfung der Eigenschaften der Gleichstromversorgung 29
Tabelle 7: Übersicht Eingangsmodule 36
Tabelle 8: Übersicht Ausgangsmodule 39
Tabelle 9: Die Systemparameter der Ressource 48
Tabelle 10: Einstellungen Sollzykluszeit-Modus 49
Tabelle 11: Standardwerte der maximalen Systembus-Latenzzeit 52
Tabelle 12: Systemvariable der Hardware 53
Tabelle 13: Systemparameter des Anwenderprogramms 62
Tabelle 14: Anwenderprogramm-Parameter *Testmodus erlaubt* 65
Tabelle 15: Online änderbare Parameter 66
Tabelle 16: Beschreibung safeethernet Parameter und Bedingungen 70

Index

Arbeitsstromprinzip 11
Ausgangs-Störaustastung 40
Automation Security 23
CRC 63
ESD-Schutz 12
Fehlerreaktion
  Eingänge 36
Fehlerreaktionen
  Ausgänge 39
Funktionstest der Steuerung 43
Hardware-Editor 53
Kommunikationszeitscheibe 50
LED Ess 31
Multitasking 67
Online-Test-Feld 64
PADT 15
Prozess-Sicherheitszeit 17
Prüfbedingungen 25
  Bahnanwendungen 25
  EMV 26
  klimatisch 26
  mechanisch 26
Rack-ID 32
Redundanz 15
Responsible 32
Ruhestromprinzip 11
Selbst-Test 15
Sicherheitskonzept 43
Sicherheitszeit 17
Steuerung abschließbar machen 54
Surge 37
Watchdog-Zeit
  Abschätzung 19
  Ressource 18

HANDBUCH
Sicherheitshandbuch für Bahnanwendungen

HI 801 326 D

Für weitere Informationen kontaktieren Sie:

HIMA Rail Segment Team
Telefon: +49 6202 709-411

Oder schreiben Sie unserem Rail-Expertenteam:
rail@hima.com

Erfahren Sie online mehr über HIMA-Lösungen
für Bahnanwendungen:

www.hima.com/de/branchen-loesungen/bahn/

HIMA SMART SAFETY.

www.hima.com