Handbuch

HIMatrix®F

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
3.02	Geändert: Kapitel 3.5.2: Temperaturklassen, Kapitel 3.5.4: Angaben zu externen Filtern	X	X
3.03	Eingefügt: F60 DO 8 01	X	X
3.04	Geändert: Kapitel 3.5.2.2: Temperaturklassen	X	X
4.00	Aktualisierte Ausgabe zu SILworX V11 Eingefügt: Standardmodule, MultiForcen	X	X

Inhaltsverzeichnis

1 Einleitung

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

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 HIMatrix 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:

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

Für die Anwendung früherer Versionen von HIMatrix 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 HIMatrix

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 HIMatrix.

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 HIMatrix wird das HIMA Programmierwerkzeug SILworX eingesetzt.

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

2.1.1 Anwendung im Ruhestromprinzip

Das HIMatrix 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).

Als sicherer Zustand im Fehlerfall wird damit bei Eingangs- und Ausgangssignalen der spannungs- oder stromlose Zustand eingenommen.

2.1.2 Anwendung im Arbeitsstromprinzip

Das HIMatrix 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

Die Übertragung der sicherheitsrelevanten Daten über öffentliche Netze (z. B. Internet) ist zulässig mit Zusatzmaßnahmen zur Erhöhung der Sicherheit (z. B. VPN-Tunnel, Firewall, etc.).

Mit den Feldbus-Schnittstellen ist keine sicherheitsbezogene Kommunikation möglich.

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 HIMatrix Systeme in Automatisierungsanlagen und in Gesamtanlagen gewährleistet ist.

Die korrekte Programmierung der HIMatrix 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 9 und im Kommunikationshandbuch HI 801 100 D aufgeführten Berechnungsgrundlagen sind anzuwenden.

2.4 ESD-Schutzmaßnahmen

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

HINWEIS

Schäden am HIMatrix 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 HIMatrix Systeme stehen außerdem noch folgende Dokumente zur Verfügung:

Name	Inhalt	Dokument-Nr.
HIMatrix Sicherheitshandbuch	Sicherheitsfunktionen des HIMatrix Systems	HI 800 022 D
HIMatrix Systemhandbuch	Hardwarebeschreibung des Systems	HI 800 140 D
HIMatrix F60 Systemhandbuch	Hardwarebeschreibung des modularen Systems F60	HI 800 190 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 800 672 D
Kommunikationshandbuch	Beschreibung der **safe**ethernet Kommunikation und der verfügbaren Protokolle	HI 801 100 D
Automation Security Handbuch	Beschreibung von Automation Security Aspekten bei HIMA Systemen	HI 801 372 D
SILworX Erste Schritte Handbuch	Einführung in die Bedienung von SILworX bei Planung, Inbetriebnahme, Test und Betrieb	HI 801 102 D
SILworX Online-Hilfe (OLH)	SILworX Bedienung	

Tabelle 1: Übersicht Systemdokumentation

Alle aktuellen Handbücher können über die E-Mail-Adresse documentation@hima.com angefragt werden. Für registrierte Kunden 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 HIMatrix:

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

3.1 Sicherheit und Verfügbarkeit

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

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

Vom sicherheitsbezogenen Automatisierungssystem HIMatrix selbst geht kein unmittelbares Risiko aus.

⚠ WARNUNG

Personenschaden möglich durch falsch angeschlossene oder falsch programmierte sicherheitsbezogene Automatisierungssysteme!

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

3.1.1 HR-Berechnungen

Für das System HIMatrix 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. Diese Anforderungen werden von den Steuerungen, den Remote I/Os und den F60 Modulen erfüllt.

3.1.2 Selbst-Test und Fehlerdiagnose

Das Betriebssystem der Steuerungen führt beim Start und im laufenden Betrieb umfangreiche Selbsttests durch.

Getestet werden hauptsächlich:

- Die Prozessoren.
- Die Speicherbereiche (RAM, nichtflüchtiger Speicher).
- Der Watchdog.
- Die einzelnen E/A-Kanäle.
- Die Spannungsversorgung.

Werden bei diesen Tests Fehler festgestellt, dann schaltet das Betriebssystem die defekte Steuerung, das defekte Modul, die defekte Remote I/O oder den defekten E/A-Kanal ab.

Bei einem System ohne Redundanz bedeutet dies, dass Teilfunktionen oder das gesamte PES abgeschaltet werden können.

Alle HIMatrix Steuerungen, Remote I/Os und Module verfügen jeweils über eigene LEDs zur Anzeige der entdeckten Fehler. Damit ist im Störungsfall eine schnelle Fehlerdiagnose über einen internen Fehler oder einen Fehler der externen Beschaltung möglich.

Zusätzlich kann das Anwenderprogramm verschiedene Systemvariable auswerten, die den Zustand des Systems anzeigen, z. B. den Temperaturzustand.

Eine umfangreiche diagnostische Aufzeichnung des Systemverhaltens und erkannter Fehler werden im Diagnosespeicher der Steuerungen abgelegt. Die Aufzeichnung kann auch nach einer Systemstörung oder Ausfall der Versorgungsspannung über das PADT ausgelesen werden.

Weitere Informationen über die Auswertung der Diagnosemeldungen finden Sie im HIMatrix Systemhandbuch HI 800 140 D.

Bei einem sehr kleinen Teil der Bauelement-Ausfälle, welche die Sicherheit nicht beeinflussen, erzeugt das HIMatrix 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 Aufbau von Sicherheitssystemen nach dem Arbeitsstromprinzip

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

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.

3.1.4.1 Erkennen ausgefallener Komponenten

Das Sicherheitssystem erkennt durch die automatisch ablaufenden Tests, dass Module defekt sind.

3.1.4.2 Sicherheitsfunktion im Arbeitsstromprinzip

Die Ausführung der Sicherheitsfunktion besteht darin, dass das Sicherheitssystem einen oder mehrere Aktoren einschaltet (energize), so dass der sichere Zustand erreicht wird.

Anwenderseitig ist folgendes zu planen:

- Leitungsschluss- und Leitungsbruch-Überwachung bei Eingängen und Ausgängen. Diese Funktionen sind zu parametrieren.
- Die Funktion von Aktoren kann über eine Stellungsrückmeldung überwacht werden.

3.2 Sicherheitsrelevante Zeiten

Folgende Zeiten sind für die Sicherheitsbetrachtung der Steuerung zu beachten:

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

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

3.2.1 Prozess-Sicherheitszeit

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

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

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

3.2.2 Parameter «Sicherheitszeit [ms]» Ressource

Die Reaktionszeit der Ressource $\mathbf{t}_{RR}$ wird durch den Parameter *Sicherheitszeit [ms]* in den Eigenschaften der Ressource $\mathbf{t}_{SR}$ wie folgt beeinflusst:

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

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

Bei Einsatz der F60 AO 8 01 ist zusätzlich zu beachten:

Für die Reaktionszeit der analogen Ausgänge ist zur zweifachen Watchdog-Zeit ($2 \times \mathbf{t}_{WD\ CPU}$) noch die zweifache Watchdog-Zeit der AO-CPU ($2 \times \mathbf{t}_{WD\ AO\ \mu P}$) zu addieren.

$\mathbf{t}_{RR} \leq \mathbf{t}_{SR} + \mathbf{12\ ms}$

$\mathbf{t}_{SR}$ 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).

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 programmierten Verzögerungen durch das Anwenderprogramm.

3.2.3 Maximale Reaktionszeit

Die maximale Reaktionszeit gilt für ein ungestörtes System. Sie ist die maximale Zeit, die das HIMatrix System benötigen darf, um auf die Änderung eines Eingangssignals durch ein entsprechendes Ausgangssignal zu antworten. Bei den zyklisch arbeitenden HIMatrix Steuerungen ist die maximale Reaktionszeit die doppelte maximale Zykluszeit. Die Voraussetzungen dafür sind:

- Die Logik des Anwenderprogramms ist so ausgeführt, dass Verzögerungen, z. B. durch ungünstige Abarbeitungsreihenfolge, nicht auftreten können.
- Ein kompletter Zyklus des Anwenderprogramms ist in einem Zyklus des Prozessorsystems abgeschlossen.
- Für die Reaktion entscheidende Daten werden nicht zwischen verschiedenen Anwenderprogrammen übertragen.

Die Zykluszeit einer Steuerung besteht aus folgenden wesentlichen Teilen:

- Prozessdaten-Kommunikation: Empfangsverarbeitung.
- Lesen der Eingänge.
- Verarbeiten des Anwenderprogramms oder der Anwenderprogramme.
- Schreiben der Ausgänge.
- Prozessdaten-Kommunikation: Sendeverarbeitung.
- Ausführen der Test-Routinen.

Weitere Informationen zur Berechnung der Reaktionszeit bei Kommunikation (Response Time) finden Sie im Kapitel 9 und im Kommunikationshandbuch HI 801 100 D.

3.2.4 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 4 … 5000 ms einstellbar und wird in den Eigenschaften der Ressource eingegeben. Die Standardeinstellung ist 200 ms für alle Steuerungen und 100 ms für Remote I/Os.Das PADT überprüft die Parameter *Sicherheitszeit [ms]* und *Watchdog-Zeit [ms]* und lehnt beim Generieren die Konfiguration ab, wenn die Watchdog-Zeit größer als ½ mal die Sicherheitszeit der Ressource gewählt wurde.

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

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

HINWEIS

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

Einstellungen vor jeder Online-Änderung genau prüfen!

i Für die zu steuernde Anlage sind Sicherheitszeit und Watchdog-Zeit zu bestimmen.

3.2.5 Abschätzung der Watchdog-Zeit

HIMA empfiehlt für eine ausreichende Verfügbarkeit der Steuerung (PES) folgende Bedingung einzuhalten:

$$\mathbf{3 \times t_{WD}} \quad \leq \quad \mathbf{t_{SR}} \text{ (Parameter } \textit{Sicherheitszeit [ms])}$$

3.2.6 Watchdog-Zeit durch Test ermitteln

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

Voraussetzungen für den Test:

- Die HIMatrix Hardware ist vollständig aufgebaut, z. B. enthält das F60 Rack alle vorgesehenen Module.
- Kommunikationspartner einschließlich Remote I/Os sind vorhanden und verbunden.
- Die Anwenderprogramm-Logik ist vollständig vorhanden.
- Die *Sollzykluszeit [ms]* ist auf 0 eingestellt.
- *Max. CPU-Zyklen Programm* ist auf 1 eingestellt (Programm-Eigenschaften).
- *Max. Dauer pro Zyklus [µs]* ist auf 0 eingestellt (Programm-Eigenschaften).
- Die *Max. Kom.Zeitscheibe [ms]* ist auf einen geeigneten Wert eingestellt.
- Die *Max. Dauer Konfigurationsverbindungen [ms]* ist auf einen geeigneten Wert eingestellt.

Minimalen Wert für die Watchdog-Zeit ermitteln

1. System unter voller Last betreiben. Auch die Kommunikation sollte unter voller Last arbeiten.
2. Eingangsdaten so vorgeben, dass möglichst die längsten Programmpfade durchlaufen werden. Dazu können Sequenzen von Eingangswerten nötig sein.
3. Zykluszeit-Statistik im Control Panel zurücksetzen.
4. Mehrmals Reload durchführen, wenn die Anwendung dies vorsieht.
5. Im Control Panel die Maximalwerte der Zykluszeiten betrachten.
   ☑ $\mathbf{t_{Zyklus}}$ ist ermittelt.
6. Die maximale Abweichung der Gesamt-Ausführungsdauer des Anwenderprogramms zur mittleren Gesamt-Ausführungsdauer ermitteln.
   ☑ $\mathbf{\Delta t_{Spitze}}$ ist ermittelt.
7. Minimale Watchdog-Zeit $\mathbf{t_{WD}}$ berechnen aus:

$$\mathbf{t_{WD}} \quad = \quad \mathbf{t_{Zyklus} + t_{Reserve} + t_{Komm} + t_{Konfig} + \Delta t_{Spitze}}$$

$\mathbf{t_{Zyklus}}$ Beobachtete maximale Zykluszeit (Grundlast, enthält bereits Anteile von $\mathbf{t_{Komm}}$ und $\mathbf{t_{Konfig}}$)

$t_{Reserve}$ Sicherheitsreserve 6 ms.

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

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

t_{Spitze} Maximale Lastspitze der Zykluszeit (t_{Spitze}) abzüglich beobachteter Grundlast, siehe Schritt 6.

► Die eingestellte Watchdog-Zeit sollte sein: Ermittelter Minimalwert $\mathbf{t_{WD}}$ + Zuschlag für zukünftige Änderungen oder Erweiterungen.

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

In folgenden Fällen ist der HIMA Support hinzuzuziehen:

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

Das HIMatrix System lässt Einstellungen zu, die eine noch bessere Performance ermöglichen. Um diese Einstellungen zu ermitteln, sind tiefergehende Kenntnisse in verschiedenen Bereichen erforderlich.

3.3 Sicherheitsauflagen

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

3.3.1 Produktunabhängige Auflagen der Hardware

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

- An das System dürfen nur Geräte angeschlossen werden, die eine sichere Trennung zum Netz aufweisen.
- Die sichere elektrische Trennung der Stromversorgung muss in der 24-V-Versorgung des Systems erfolgen. Es dürfen nur Netzgeräte in Ausführungen eingesetzt werden, die sicherstellen, dass Steuerung und Remote I/Os mit Niederspannung 24 V betrieben werden.
- 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 HIMatrix 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 HIMatrix 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 die zulässige maximale Reaktionszeit nicht überschreitet. Die im Kapitel 9.2 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 seriellen Schnittstellen sind in dieser Ausbaustufe ausschließlich für nicht sicherheitsbezogene Zwecke verwendbar.
- 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 HIMatrix Systems in Bahnanwendungen zu beachten:

- Die Standardvarianten der HIMatrix Systemfamilie können in einem Container oder in einem Gebäude mit geregelter Temperatur und Luftfeuchte eingesetzt werden, siehe Tabelle 4.
- Die Standardvarianten der HIMatrix Systemfamilie sind für den Einsatz auf Bahnfahrzeugen nicht zugelassen.
- Die HIMatrix Varianten für Bahnanwendungen (siehe Tabelle 3) können 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 Leitungsschlussüberwachung. Maßnahmen beim Ansprechen der Überwachung müssen durch das Anwenderprogramm erfolgen.
- Der Temperaturzustand (Betriebstemperatur) der HIMatrix Systeme ist durch das Anwenderprogramm auszuwerten. Sicherheitsbezogene Maßnahmen müssen ebenfalls durch das Anwenderprogramm erfolgen. Weitere Informationen finden Sie im HIMatrix Systemhandbuch HI 800 140 D.
- 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 verwendeten Programmierwerkzeug ausgelesen werden. Weitere Informationen finden Sie im HIMatrix Systemhandbuch HI 800 140 D.
- 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

HIMatrix 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 HIMatrix System für den industriellen Einsatz geprüft und zertifiziert ist, können dem Sicherheitshandbuch HI 800 022 D entnommen werden.

3.6 Zusätzliche Prüfbedingungen für Bahnanwendungen

Nachfolgende Tabellen zeigen die HIMatrix Komponenten, die für den Einsatz in Bahnanwendungen zugelassen sind:

Kompaktsteuerungen
F30 03
F35 03
Remote I/Os
F1 DI 16 01
F2 DO 4 01
F2 DO 8 01
F2 DO 16 01
F2 DO 16 02
F3 AIO 8/4 01
F3 DIO 8/8 01
F3 DIO 16/8 01
F3 DIO 20/8 02
Modulares System F60
AI 8 01
CIO 2/4 01
CPU 03
DI 32 01
DIO 24/16 01
DO 8 01
GEH 01
MI 24 01
PS 01

Tabelle 2: HIMatrix Standardvarianten

Alle in Tabelle 2 aufgeführten HIMatrix Standardvarianten sind nur für den Einsatz als Signal- und Telekommunikationseinrichtung gemäß EN 50125-3 zugelassen.

Kompaktsteuerungen
F30 034
F35 034
Remote I/Os
F1 DI 16 014
F2 DO 8 014
F2 DO 16 014
F3 AIO 8/4 014
F3 DIO 8/8 014
F3 DIO 16/8 014
F3 DIO 20/8 024
Modulares System F60
AI 8 014
CIO 2/4 014
CPU 034
DI 32 014
DIO 24/16 014
GEH 014
MI 24 014
PS 014

Tabelle 3: HIMatrix Varianten für Bahnanwendungen

Alle in Tabelle 3 aufgeführten HIMatrix Komponenten sind für den Einsatz auf Bahnfahrzeugen gemäß EN 61373, Kategorie 1, Klasse B, und als Signal- und Telekommunikationseinrichtung gemäß EN 50125-3 für den Einsatzpunkt außerhalb der Gleise (1 … 3 m Abstand vom Gleis) zugelassen. Diese Varianten der Standardkomponenten erhalten den Zusatz 4 in der Typenbezeichnung.

Alle HIMatrix Komponenten wurden für die zusätzliche Einhaltung der Anforderungen nachfolgender EMV-, Klima- und Umweltanforderungen entwickelt.

3.6.1 Höhenbereich

Für alle HIMatrix Komponenten gelten für den Höhenbereich folgende Klassen:

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

Für die in Tabelle 3 aufgeführten HIMatrix 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

Alle HIMatrix Standardvarianten sind für einen Temperaturbereich von 0 … 60 °C und für eine relative Luftfeuchte von 10 … 95 % (nicht betauend) ausgelegt und getestet. Für die Bahnanwendung gemäß EN 50125-3 ergeben sich daraus die folgenden Temperaturklassen:

HIMatrix	Im Freien	Im Schaltschrank	Im Container		Im Gebäude	
			N.T.C	T.C	N.C.C.	C.C
Standard	-	-	-	T1, T2, TX	-	T1, T2, TX

Tabelle 4: Temperaturklassen der HIMatrix Standardvarianten gemäß EN 50125-3

Die Standardvarianten der HIMatrix Systemfamilie können, wie die Tabelle 4 darstellt, in einem Container oder in einem Gebäude mit geregelter Temperatur und Luftfeuchte eingesetzt werden.

HINWEIS

Die Standardvarianten der HIMatrix Systemfamilie sind für den Einsatz auf Bahnfahrzeugen gemäß EN 50155 nicht zugelassen!

3.6.2.1 Einsatz in der Signaltechnik

Die HIMatrix Varianten für Bahnanwendungen sind für einen Temperaturbereich von -25 … +70 °C ausgelegt. Alle HIMatrix Varianten für Bahnanwendungen wurden gemäß EN 50125-3 getestet und sind in den folgenden Temperaturklassen einsetzbar:

HIMatrix	Im Freien	Im Schaltschrank	Im Container		Im Gebäude	
			N.T.C	T.C	N.C.C.	C.C
F30 034	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F35 034	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F1 DI 16 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F2 DO 8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F2 DO 16 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 AIO 8/4 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 DIO 8/8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 DIO 16/8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 DIO 20/8 024	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
PS 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
CPU 034	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
AI 8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
CIO 2/4 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
DI 32 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
DIO 24/16 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
MI 24 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX

Tabelle 5: Temperaturklassen gemäß EN 50125-3

3.6.2.2 Einsatz auf Bahnfahrzeugen

Alle HIMatrix Varianten für Bahnanwendungen wurden gemäß EN 50155 getestet und sind in den folgenden Temperaturklassen einsetzbar:

HIMatrix	Temperaturklassen
F30 034	OT3
F35 034	OT3
F1 DI 16 014	OT3
F2 DO 8 014	OT3
F2 DO 16 014	OT3
F3 AIO 8/4 014	OT3
F3 DIO 8/8 014	OT3
F3 DIO 16/8 014	OT3
F3 DIO 20/8 024	OT3
PS 014	OT3
CPU 034	OT3
AI 8 014	OT3
CIO 2/4 014	OT3
DI 32 014	OT3
DIO 24/16 014	OT3
MI 24 014	OT3

Tabelle 6: Temperaturklassen gemäß EN 50155

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

Für die schnelle Temperaturänderung gilt für die HIMatrix Systemfamilie die Temperaturänderungsklasse H1, wie im Kapitel 4.3.4 der EN 50155 definiert.

Da die Platinen in den Komponenten der HIMatrix Systemfamilie mit einem Schutzüberzug beschichtet sind, besitzen diese die Schutzlackierungsklasse PC2, wie im Kapitel 10.7 der EN 50155 definiert.

3.6.2.3 Derating der Digitalen Ausgänge

Bei einer Umgebungstemperatur größer 60 °C muss die Belastung der digitalen Ausgänge verringert werden (Derating). Die Ausgänge können in diesem Fall mit jeweils maximal 0,5 A belastet werden, siehe Handbücher der Komponenten.

3.6.3 Mechanische Bedingungen

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

3.6.3.1 Einsatz in der Signaltechnik

Alle HIMatrix Komponenten wurden gemäß der EN 50125-3 mechanisch geprüft. Die wichtigsten Prüfungen und Grenzwerte für mechanische Bedingungen sind in nachstehender Tabelle aufgelistet:

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

Tabelle 7: Mechanische Bedingungen für Einsatz in der Signaltechnik

3.6.3.2 Einsatz auf Bahnfahrzeugen

Die in Tabelle 3 aufgeführten Komponenten wurden gemäß der EN 50155 mechanisch geprüft. Die Prüfung erfolgte gemäß EN 61373, Kategorie 1, Klasse B.

Die HIMatrix Systemfamilie 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 nachfolgenden Kapitel enthalten die Prüfungen und Grenzwerte der EMV-Anforderungen für den Einsatz in der Signaltechnik und auf Bahnfahrzeugen.

3.6.4.1 Einsatz in der Signaltechnik

Alle HIMatrix Komponenten wurden gemäß den EMV-Anforderungen der EN 50121-4 positiv getestet. Die wichtigsten Prüfungen und Grenzwerte 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 … 1000 MHz:	10 V/m
		800 … 1000 MHz:	20 V/m
		1400 … 2000 MHz:	10 V/m
		2000 … 2700 MHz:	5 V/m
		5100 … 6000 MHz:	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
		Geschirmte Leitungen:	2 kV CM
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 8: EMV-Bedingungen für Einsatz in der Signaltechnik gemäß EN 50121-4

Anmerkungen zum Surge mit 2 kV (CM) / 1 kV (DM):

Nachfolgende Anmerkungen gelten für die Standardvarianten und die Varianten für Bahnanwendungen, auch wenn diese nicht explizit genannt werden.

Bei den HIMatrix Kompaktsystemen ist gegen den Surge auf die DC-Versorgungsspannung das externe Filter H 7013 von HIMA zwingend notwendig. Die Versorgungsspannung für die HIMatrix F35 03 darf nicht von außen zugeführt werden, sondern muss im gleichen Schaltschrank erzeugt werden.

i In folgenden Fällen sind ebenfalls externe Surge-Filter für alle ungeschirmten Eingangs- und Ausgangsleitungen erforderlich:

- Anschluss von Einrichtungen innerhalb des 3-m-Bereichs.
- Anschluss von Einrichtungen innerhalb des 10-m-Bereichs mit Verbindung innerhalb des 3-m-Bereichs.
- Anschuss von Einrichtungen innerhalb des 10-m-Bereichs mit Leitungen, die länger als 30 m sind.

Bei den Kompaktsystemen F30 03, F1 DI 16 01, F3 DIO 20/8 02 und den F60 Modulen DIO 24/16 01 und DI 32 01 müssen zum Schutz der digitalen Eingänge gegen Surge-Impulse der Überspannungsableiter DCO RK ME24 (aktuell DCO SD2 ME24) vom Hersteller DEHN eingesetzt werden.

Bei der Steuerung F30 03 und dem F60 Modul DIO 24/16 01 müssen zum Schutz der digitalen Ausgänge gegen Surge-Impulse der Überspannungsableiter DCO RK MD24 (aktuell DCO SD2 MD24) vom Hersteller DEHN eingesetzt werden.

Es können auch Überspannungsableiter anderer Hersteller verwendet werden, wenn die Datenblattangaben gleichwertig oder besser sind.

3.6.4.2 Einsatz auf Bahnfahrzeugen

Die in Tabelle 3 aufgeführten Komponenten wurden gemäß den EMV-Anforderungen der EN 50121-3-2 positiv getestet. Die wichtigsten Prüfungen und Grenzwerte 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 … 1000 MHz: 20 V/m 1400 … 2000 MHz: 10 V/m 2000 … 2700 MHz: 5 V/m 5100 … 6000 MHz: 3 V/m
EN 61000-4-4	Burst-Prüfung	Versorgungsspannung: 2 kV E/A-Leitungen: 2 kV
EN 61000-4-5	Surge	Versorgungsspannung: 2 kV CM 1 kV DM
EN 61000-4-6	Einströmung	Versorgungsspannung: 10 V E/A-Leitungen: 10 V

Tabelle 9: EMV-Bedingungen für Einsatz auf Bahnfahrzeugen gemäß EN 50121-3-2

Anmerkungen zum Surge mit 2 kV (CM) / 1 kV (DM):

Bei den HIMatrix Kompaktsystemen ist gegen den Surge auf die DC-Versorgungsspannung das externe Filter H 7013 von HIMA zwingend notwendig. Die Versorgungsspannung für die HIMatrix F35 034 darf nicht von außen zugeführt werden, sondern muss im gleichen Schaltschrank erzeugt werden.

Es können auch Überspannungsableiter anderer Hersteller verwendet werden, wenn die Datenblattangaben gleichwertig oder besser sind.

3.6.5 Erschwerte Bedingungen

Das HIMatrix 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 HIMatrix Systeme sind in nachstehender Tabelle aufgelistet:

IEC/EN 61131-2	Nachprüfung der Eigenschaften der Gleichstromversorgung
	Prüfung des Spannungsbereiches: 24 VDC, -15 … +20 %, $w_S \leq 5$ %
	Prüfung auf Unempfindlichkeit gegen Kurzzeitunterbrechung der externen Stromversorgung: DC, PS 2: 10 ms
	Polaritätsumkehr der Versorgungsspannung: geprüft für 10 s

Tabelle 10: Prüfung der Unempfindlichkeit gegenüber Fehlern bei der Versorgungsspannung

3.6.6.1 Bedingungen an die Versorgungspannung auf Bahnfahrzeugen

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

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

Damit ergeben sich die folgenden Toleranzen:

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

Die in Tabelle 2 aufgeführten HIMatrix Varianten wurden gemäß EN 50155, Kapitel 5.1 getestet.

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

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

HIMatrix Systeme sind für Spannungsunterbrechungen bis zu 20 ms ausgelegt. Damit erfüllt die HIMatrix die Anforderungen der Klasse S3 gemäß EN 50155, Kapitel 5.1.1.4.

Das HIMatrix 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 zwei Versorgungsspannungen werden nicht erfüllt. Es sind externe Maßnahmen durch den Anwender erforderlich.

4 Zentrale Funktionen

Bei den Steuerungen und Remote I/Os der Typen F1 …, F2 …, F3 … handelt es sich um Kompaktsysteme, die nicht modifiziert werden können.

Bei den Steuerungen des Typs F60 handelt es sich um modulare Systeme. Bei diesen sind innerhalb einer Steuerung neben einem Stromversorgungsmodul und einem Prozessormodul bis zu 6 E/A-Module einsetzbar.

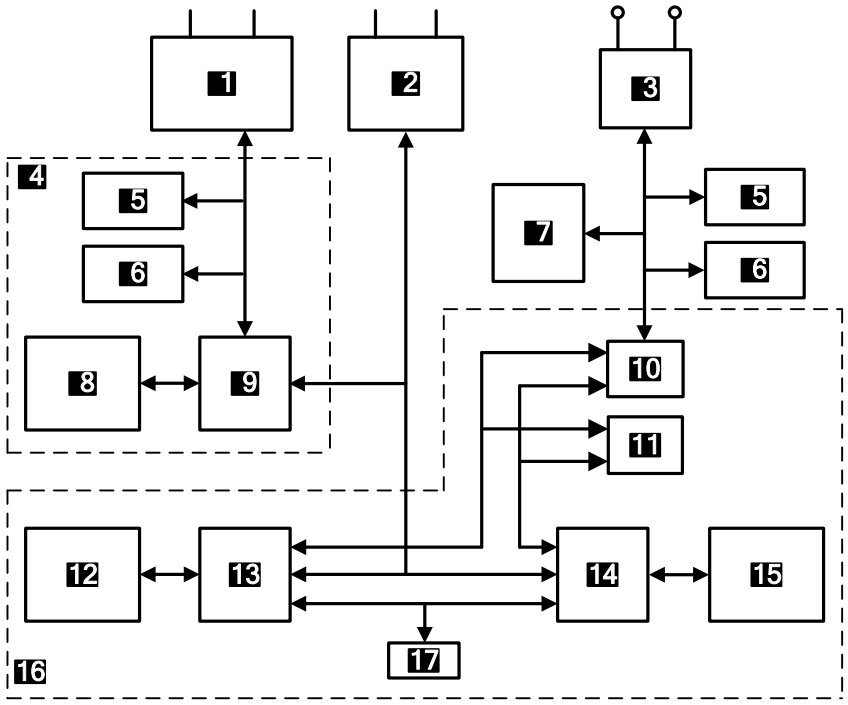
4.1 Netzgeräte

Die Versorgung der HIMatrix Systeme muss aus Netzgeräten erfolgen, welche die Steuerungen und die Remote I/Os mit Niederspannung 24 V versorgen.

Die ordnungsgemäße Funktion der Steuerung wird mit Einhaltung der zulässigen Spannungsgrenzen sichergestellt.

4.2 Funktionsbeschreibung des Prozessorsystems

Das Prozessorsystem ist die zentrale Komponente der Steuerung. Nachfolgende Abbildung zeigt das Blockschaltbild des Prozessorsystems am Beispiel der CPU 03 des modularen Systems F60:



1 Feldbus-Schnittstellen
2 Ethernet-Schnittstellen
3 E/A-Bus-Submodul
4 Kommunikationssystem
5 NVSRAM
6 Flash
7 V_{CC} und Temperaturüberwachung
8 SDRAM des Kommunikationssystems
9 Prozessor des Kommunikationssystems
10 Vergleicher
11 Watchdog
12 SDRAM 1 des Prozessorsystems
13 Prozessor 1 des Prozessorsystems
14 Prozessor 2 des Prozessorsystems
15 SDRAM 2 des Prozessorsystems
16 Sicherheitsbezogenes Prozessorsystem
17 Real Time Clock

Bild 1: Blockschaltbild der CPU 03

Eigenschaften des Prozessorsystems

- Zwei taktsynchrone Mikroprozessoren (Prozessor 1 und Prozessor 2).
- Jeder Mikroprozessor hat einen eigenen SDRAM-Speicher.
- Testbarer Hardware-Vergleicher für alle externen Zugriffe beider Mikroprozessoren.
- Im Fehlerfall wird der Watchdog in den sicheren Zustand gesetzt.
- Flash als Programmspeicher für Betriebssysteme und Anwenderprogramm, geeignet für min. 100 000 Speicherzyklen.
- Datenspeicher in NVSRAM.
- Goldcap zur Pufferung von Datum/Uhrzeit.
- Kommunikationsprozessor für Feldbus- und Ethernet-Anschlüsse.
- Schnittstelle zum Datenaustausch zwischen Geräten, Steuerungen F60 und dem PADT, basierend auf Ethernet.
- Optionale Schnittstelle(n) zum Datenaustausch per Feldbus.
- Signalisierung der Systemzustände durch LEDs.
- E/A-Bus-Logik zur Verbindung mit den E/A-Modulen.
- Sicherer Watchdog (WD).
- Netzgerätüberwachung, testbar (1,8 VDC / 3,3 VDC).
- Temperaturüberwachung.

4.3 Selbst-Tests

Das Betriebssystem des Prozessorsystems 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.

Die für die Erfüllung der Sicherheitsnormen geforderten Diagnosemaßnahmen werden durch das sicherheitsbezogene Prozessorsystem durchgeführt.

Nachfolgend sind die wichtigsten Selbsttestroutinen der sicherheitsbezogenen Prozessorsysteme stichwortartig erläutert.

4.3.1 Mikroprozessor-Test

Geprüft werden:

- Alle verwendeten Befehle und Adressierungsarten.
- Die Beschreibbarkeit der Flags und die durch sie bedingten Befehle.
- Die Beschreibbarkeit und das Übersprechen der Register.

4.3.2 Test der Speicherbereiche

Das Betriebssystem, das Anwenderprogramm, die Konstanten und Parameter sowie die variablen Daten sind in Speicherbereichen beider Prozessoren gespeichert und werden von einem Hardware-Vergleicher geprüft.

4.3.3 Gesicherte Speicherbereiche

Betriebssystem, Anwenderprogramm und Parameterbereich sind in je einem Speicher abgelegt. Sie werden durch einen Schreibschutz und einen CRC-Test gesichert.

4.3.4 RAM-Test

Ein Schreib- und Lesetest prüft die änderbaren RAM-Bereiche insbesondere auf Stuck-at und Übersprechen.

4.3.5 Watchdog-Test

Das Watchdog-Signal schaltet sich ab, wenn es nicht in einem festgelegten Zeitfenster von beiden CPUs getriggert wird; ebenso, wenn der Test des Hardware-Vergleichers fehlschlägt. Durch einen weiteren Test wird die Abschaltbarkeit des Watchdog-Signals geprüft.

4.3.6 Test des E/A-Busses innerhalb der Steuerung

Die Verbindung zwischen der CPU und den zugehörigen Eingängen und Ausgängen (E/A-Modulen) wird geprüft.

4.4 Reaktionen auf Fehler im Prozessorsystem

Ein Hardware-Vergleicher innerhalb des Prozessorsystems vergleicht ständig, ob die Daten des Mikroprozessors 1 identisch sind mit den Daten des Mikroprozessors 2. Ist das nicht der Fall oder finden die Testroutinen einen Fehler, schaltet das Watchdog-Signal ab. Das bedeutet, dass die Steuerung keine Eingangssignale mehr verarbeitet und die Ausgänge in den energielosen, abgeschalteten Zustand übergehen.

Beim ersten derartigen Fehler startet die Steuerung erneut (Reboot). Tritt innerhalb einer Minute nach dem Neustart ein weiterer Fehler auf, dann geht die Steuerung in den Zustand STOP/FEHLERHAFTE KONFIGURATION und bleibt in diesem Zustand.

4.5 Fehlerdiagnose

Alle Module der F60 verfügen jeweils über eine eigene LED zur Fehleranzeige bei Störungen des Modules oder der externen Beschaltung. Damit ist im Störungsfall eine schnelle Fehlerdiagnose über ein als fehlerhaft gemeldete Modul möglich.

Bei den Kompaktsystemen F1 …, F2 …, F3 … sind diese Fehleranzeigen zu einer Sammel-Fehlermeldung zusammengefasst.

Zusätzlich kann im Anwenderprogramm eine Auswertung von verschiedenen Systemvariablen der Eingänge und Ausgänge oder der Steuerung erfolgen.

Eine Fehlersignalisierung findet nur statt, wenn der Fehler die Kommunikation mit dem Prozessorsystem nicht behindert, d. h. eine Auswertung über das Prozessorsystem noch ermöglicht.

Die Logik im Anwenderprogramm kann die Fehlercodes aller Eingangssignale und Ausgangssignale und der Systemvariablen auswerten.

Eine umfangreiche diagnostische Aufzeichnung des Systemverhaltens und erkannter Fehler werden im Diagnosespeicher des Prozessor- und des Kommunikationssystems abgelegt. Die Aufzeichnung kann auch nach einer Störung oder Abschaltung des Systems über das PADT ausgelesen werden.

Weitere Informationen über die Auswertung der Diagnosemeldungen finden Sie im Systemhandbuch, HI 800 140 D.

5 Eingänge

Die Aussagen in diesem Kapitel gelten für die Standardvarianten und die Varianten für Bahnanwendungen, auch wenn diese nicht explizit genannt werden.

Nachfolgende Tabelle gibt eine Übersicht über die Eingänge des HIMatrix Systems:

Komponente	Typ	Anzahl	sicherheits-bezogen	rückwirkungsfrei	galvanisch getrennt
Kompaktsysteme					
F30 03	Digital	20	•	•	– [1]
F35 03	Digital	24	•	•	– [1]
	Zähler 24 Bit	2	•	•	– [1]
	Analog	8	•	•	– [1]
F1 DI 16 01	Digital	16	•	•	– [1]
F3 DIO 8/8 01	Digital	8	•	•	– [1]
F3 DIO 16/8 01	Digital	16	•	•	– [1]
F3 AIO 8/4 01	Analog	8	•	•	– [1]
F3 DIO 20/8 02	Digital	20	•	•	– [1]
Modulares System F60					
DIO 24/16 01	Digital	24	•	•	•
DI 32 01 (konfigurierbar für Line Control)	Digital	32	•	•	•
CIO 2/4 01	Zähler 24 Bit	2	•	•	•
AI 8 01	Analog	8	•	•	•
MI 24 01	Analog oder Digital	24	•	•	•
[1] Bezugspotential L-					

Tabelle 11: Übersicht über die Eingänge des HIMatrix Systems

5.1 Allgemein

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

Die Steuerungen liefern Status- und Fehlerinformation auf folgende Weisen:

- Durch Diagnose-LEDs.
- Durch Systemvariablen, die das Anwenderprogramm auswerten kann.
- Durch Einträge im Diagnosespeicher, die das PADT auslesen kann.

Sicherheitsbezogene Eingangsmodule werden während des Betriebes durch einen hochwertigen, zyklischen Selbst-Test überprüft. Diese Test-Routinen sind TÜV-geprüft und überwachen die sichere Funktion des jeweiligen Moduls.

Bei einem kleinen Teil der Bauelement-Ausfälle, welche die Sicherheit nicht beeinflussen, wird keine Diagnoseinformation erzeugt.

5.2 Reaktion im Fehlerfall

Wenn die Test-Routinen einen Fehler feststellen, lösen sie folgende Reaktionen aus:

- Das Anwenderprogramm verarbeitet den Initialwert der globalen Variablen, die dem Eingang zugewiesen ist.
- Der Fehlercode und weitere Systemvariablen können zur Programmierung von anwenderspezifischen Fehlerreaktionen verwendet werden. Einzelheiten sind dem Handbuch der jeweiligen Komponente zu entnehmen.

Im Fehlerfall aktiviert ein Kompaktsystem die LED *ERROR,* ein F60 Modul die LED *ERR*.

5.3 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.

5.4 Sicherheitsbezogene digitale Eingänge

Die beschriebenen Eigenschaften gelten sowohl für die digitalen Eingangskanäle der F60 Module als auch für die digitalen Eingangskanäle aller Kompaktsysteme, sofern keine spezifischen Benennungen erfolgen.

5.4.1 Allgemein

Die digitalen Eingänge werden einmal in jedem Zyklus gelesen und intern gespeichert; sie werden zyklisch auf sichere Funktion getestet.

Eingangssignale, die kürzer als die Zeit zwischen zwei Abtastungen anstehen, werden unter Umständen nicht erfasst.

5.4.2 Test-Routinen

Die Test-Routinen prüfen, ob die Eingangskanäle in der Lage sind, unabhängig von den anstehenden Eingangssignalen beide Signalpegel (LOW und HIGH) durchzuschalten. Dieser Funktionstest wird vor jedem Lesen der Eingangssignale durchgeführt.

5.4.3 Surge auf digitalen Eingängen

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

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. Dadurch verlängert sich die maximale Reaktionszeit.

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 HIMatrix Systemhandbuch HI 800 140 D und der relevanten Normen.

5.4.4 Parametrierbare digitale Eingänge

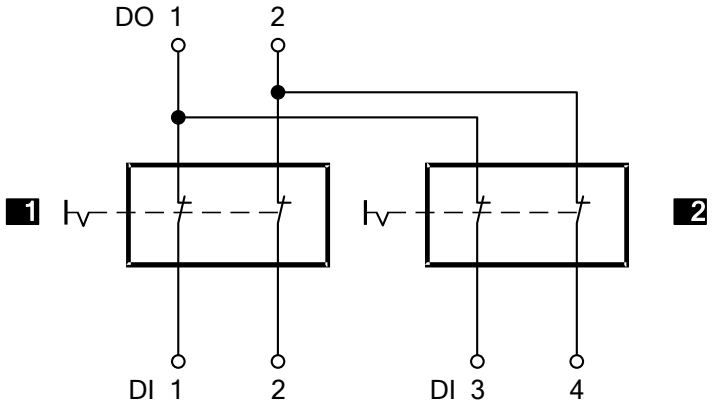
Die digitalen Eingänge der Steuerung F35 03 und des Moduls MI 24 01 arbeiten nach dem Prinzip analoger Eingänge, die durch Parametrierung von Schaltschwellen einen digitalen Wert liefern.

Für parametrierbare digitale Eingänge gelten die dieselben Test-Routinen und Sicherheitsfunktionen wie für analoge Eingänge, siehe Kapitel 5.5.

5.4.5 Line Control

Line Control ist eine Leitungsschluss- und Leitungsbruch-Erkennung zum Beispiel von NOT-AUS-Geräten, die bei HIMatrix Systemen mit digitalen Eingängen (nicht bei Steuerung F35 03 und Modul MI 24 01) konfiguriert werden kann.

Dazu werden die digitalen Ausgänge des Systems mit den digitalen Eingängen desselben Systems wie folgt verbunden (Beispiel):

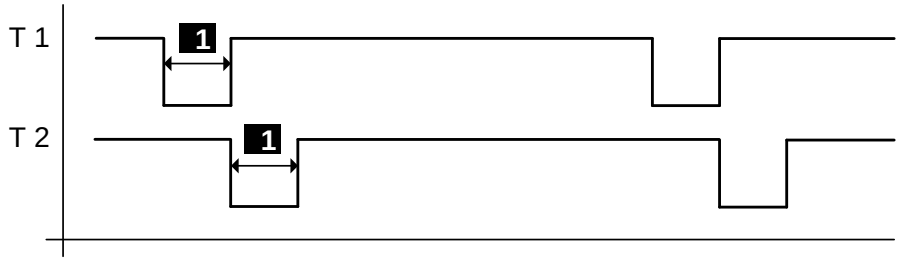


1 NOT-AUS 1
2 NOT-AUS 2

NOT-AUS-Schalter nach den Normen EN 60947-5-1 und EN 60947-5-5

Bild 2: Line Control

Die Steuerung taktet die digitalen Ausgänge, um Leitungsschluss und Leitungsbruch der Leitungen zu den digitalen Eingängen zu erkennen. Hierzu in SILworX die Systemvariable *Wert [BOOL] ->* parametrieren. Die Taktausgänge können beliebigen digitalen Eingängen zugeordnet werden.



1 Konfigurierbar 5 … 2000 µs

Bild 3: Taktsignale T1, T2

Ein (auswertbarer) Fehlercode wird erzeugt, wenn folgende Fehler auftreten:

- Querschluss zwischen zwei parallelen Leitungen.
- Vertauschung von zwei Leitungen (z. B. DO 2 an DI 3).
- Erdschluss einer der Leitungen (nur bei geerdetem Bezugspol).
- Leitungsbruch oder Öffnen der Kontakte.

Weitere Informationen und eine Beschreibung der Konfiguration von Line Control finden Sie im HIMatrix Systemhandbuch HI 800 140 D.

5.5 Sicherheitsbezogene analoge Eingänge (F35 03, F3 AIO 8/4 01 und F60)

Die analogen Eingangskanäle wandeln die gemessenen Eingangsströme in einen INTEGER-Wert um. Die Werte stehen dem Anwenderprogramm in Variablen zur Verfügung, die der Systemvariablen *-> Wert [INT]* zugewiesen sind.

Die Wertebereiche der Eingänge sind abhängig von der Komponente.

Steuerung F35 03

Eingangskanäle	Messverfahren	Strom, Spannung	Wertebereich in der Anwendung	
			FS1000 [1]	FS2000 [1]
8	unipolar	0 … +10 V	0 … 1000	0 … 2000
8	unipolar	0 … 20 mA	0 … 500 [2] 0 … 1000 [3]	0 … 1000 [2] 0 … 2000 [3]

[1] Einstellbar über Typauswahl im PADT.
[2] Mit externem Shunt-Adapter 250 Ω.
[3] Mit externem Shunt-Adapter 500 Ω.

Tabelle 12: Analoge Eingänge der Steuerung F35 03

Remote I/O F3 AIO 8/4 01

Eingangskanäle	Messverfahren	Strom, Spannung	Wertebereich in der Anwendung
8	Unipolar	0 … +10 V	0 … 2000
8	Unipolar	0/4 … 20 mA	0 … 1000 [1] 0 … 2000 [2]

[1] Mit externem Shunt-Adapter 250 Ω.
[2] Mit externem Shunt-Adapter 500 Ω.

Tabelle 13: Analoge Eingänge der Remote I/O F3 AIO 8/4 01

F60 Module

Eingangskanäle	Messverfahren	Strom, Spannung	Wertebereich in der Anwendung	
			FS1000 [1]	FS2000 [1]
AI 8 01				
8	unipolar	-10 … +10 V	-1000 … 1000	-2000 … 2000
8	unipolar	0 … 20 mA	0 … 1000 [3]	0 … 2000 [3]
8	unipolar	0 … 20 mA	0 … 500 [2]	0 … 1000 [2]
4	bipolar	-10 … +10 V	-1000 … 1000	-2000 … 2000
MI 24 01				
24	unipolar	0 … 20 mA	0 … 2000 [4]	

[1] Einstellbar über Typauswahl im PADT (F60).
[2] Mit externem Mess-Shunt 250 Ω.
[3] Mit externem Mess-Shunt 500 Ω (Genauigkeit 0,05 %, 1 W). Bei HIMA nicht mehr verfügbar.
[4] Interne Mess-Shunts.

Tabelle 14: Analoge Eingänge der Steuerung F60

Das F60 Modul AI 8 01 kann im Anwenderprogramm auf acht unipolare oder vier bipolare Funktionen konfiguriert werden. Das Mischen der Funktionen auf einem Modul ist jedoch nicht zulässig.

Die analogen Eingänge der Steuerung F35 03, der Remote I/O F3 AIO 8/4 01 und des Moduls AI 8 01 arbeiten mit Spannungsmessung. Mit den analogen Eingängen der F35 03 und der F3 AIO 8/4 01 können digitale Ausgänge des eigenen Systems (F35 03) oder anderer HIMatrix Steuerungen auf Leitungsbruch überwacht werden. Weitere Informationen finden Sie in den Handbüchern der entsprechenden HIMatrix Steuerungen.

Erfolgt keine Leitungsüberwachung durch das System, werden bei Leitungsbruch an den hochohmigen Eingängen beliebige Eingangssignale verarbeitet. Der aus dieser schwebenden Eingangsspannung resultierende Wert ist nicht sicher; bei Spannungseingängen müssen die Kanäle mit einem Widerstand von 10 kΩ abgeschlossen werden. Der Innenwiderstand der Quelle ist dabei zu beachten.

Für eine Strommessung wird dem Eingang der Shunt parallel geschaltet; der Widerstand von 10 kΩ ist dann nicht erforderlich.

Die Eingänge des Moduls MI 24 01 sind aufgrund der internen Mess-Shunts Stromeingänge und können nicht als Spannungseingänge genutzt werden.

Bei unbenutzten Eingangskanälen muss der Messeingang mit dem Bezugspotenzial verbunden werden. Negative Einflüsse auf andere Kanäle im Falle eines Leitungsbruches (schwebende Spannungswerte) werden damit vermieden. Es genügt, unbenutzten Eingängen keine globale Variable zuzuweisen.

5.5.1 Test-Routinen

Die Analogwerte werden parallel über zwei Multiplexer und zwei Analog/Digital-Wandler mit 12 Bit Auflösung verarbeitet und die Ergebnisse werden miteinander verglichen. Zusätzlich werden über vorhandene Digital/Analog-Wandler Testwerte aufgeschaltet, wieder in Digitalwerte rückgewandelt und mit dem Vorgabewert verglichen.

5.6 Sicherheitsbezogene Zähler (F35 03 und F60)

Die aufgeführten Punkte gelten sowohl für das Zählermodul CIO 2/4 01 der F60 als auch für die Zähler der F35 03, sofern nicht anders beschrieben.

5.6.1 Allgemein

Ein Zählerkanal ist für den Betrieb als schneller Vorwärts-/Rückwärtszähler mit 24-Bit Auflösung oder als Decoder im Gray-Code parametrierbar.

Bei der Verwendung als schneller Vorwärts-/Rückwärtszähler sind die Signale des Impulseingangs und des Zählrichtungseingangs in der Anwendung zu verwenden. Ein Reset erfolgt nur im Anwenderprogramm.

Die Encoder der Zähler haben folgende Auflösungen:

- Die Zähler des F60 Moduls CIO 2/4 01 haben 4 oder 8 Bit Auflösung.
- Die Zähler der F35 03 haben 3 oder 6 Bit Auflösung.

Ein Reset ist möglich.

Die Verknüpfung von zwei unabhängigen 4-Bit-Eingängen zu einem 8-Bit-Eingang (Beispiel für F60) erfolgt ausschließlich per Anwenderprogramm. Eine Schaltmöglichkeit für diesen Zweck ist nicht vorgesehen.

Die Encoder-Funktion überwacht die Änderung der Bitmuster an den Eingangskanälen. Die Bitmuster an den Eingängen werden direkt an das Anwenderprogramm übergeben. Die Darstellung im PADT erfolgt in Form einer dem Bitmuster entsprechenden Dezimalzahl (*Zähler[0x].Wert*).

Je nach Applikation kann diese Zahl, die dem Gray-Code-Bitmuster entspricht, z. B. in den zugehörigen Dezimalwert gewandelt werden.

5.7 Checklisten Eingänge

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

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

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

6 Ausgänge

Die Aussagen in diesem Kapitel gelten für die Standardvarianten und die Varianten für Bahnanwendungen, auch wenn diese nicht explizit genannt werden.

Nachfolgende Tabelle gibt eine Übersicht über die Ausgänge des HIMatrix Systems:

Komponente	Typ	Anzahl	sicherheits-bezogen	galvanisch getrennt
Kompaktsysteme				
F30 03 (konfigurierbar für Line Control)	Digital	8	•	–[1)]
F35 03	Digital	8	•	–[1)]
F1 DI 16 01	Takt	4	-	–[1)]
F2 DO 4 01 [2)]	Digital	4	•	–[1)]
F2 DO 8 01	Relais	8	•	•
F2 DO 16 01	Digital	16	•	–[1)]
F2 DO 16 02 [2)]	Relais	16	•	•
F3 DIO 8/8 01	Digital 1-polig	8	•	–[1)]
	Digital 2-polig	2		
F3 DIO 16/8 01	Digital 1-polig	16	•	–[1)]
	Digital 2-polig	8		
F3 AIO 8/4 01	Analog	4	-	–[1)]
F3 DIO 20/8 02 (konfigurierbar für Line Control)	Digital	8	•	–[1)]
Modulares System F60				
DIO 24/16 01 (konfigurierbar für Line Control)	Digital	16	•	
DO 8 01 (250 V) [2)]	Relais	8	•	•
CIO 2/4 01	Digital	4	•	

[1)] Bezugspotential L-.

[2)] Nur als Standardvariante verfügbar.

Tabelle 15: Übersicht über die Ausgänge des HIMatrix Systems

6.1 Allgemein

Die Steuerung beschreibt die sicherheitsbezogenen Ausgänge einmal in jedem Zyklus, liest die Ausgangssignale zurück und vergleicht sie mit den vorgegebenen Ausgangsdaten.

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

In den sicherheitsbezogenen Ausgangskanälen sind drei testbare Schalter in Serie integriert. Somit ist der sicherheitstechnisch erforderliche, unabhängige zweite Abschaltweg auf dem Ausgangsmodul integriert. Diese integrierte Sicherheitsabschaltung schaltet im Fehlerfall alle Kanäle des defekten Ausgangsmoduls sicher ab (energieloser Zustand).

Außerdem ist auch das Watchdog-Signal der CPU die zweite Möglichkeit der Sicherheitsabschaltung: Ein Wegfall des Watchdog-Signals bewirkt das sofortige Einnehmen des sicheren Zustandes aller Ausgangskanäle.

Diese Funktion ist nur wirksam für alle digitalen Ausgänge und Relaisausgänge der Steuerungen.

Die Verwendung des jeweiligen Fehlercodes bietet zusätzliche Möglichkeiten, Fehlerreaktionen im Anwenderprogramm zu konfigurieren.

6.2 Reaktion im Fehlerfall

Wenn die Testroutinen bei den Ausgängen einen Fehler feststellen, schaltet die Steuerung im Fehlerfall den jeweiligen Ausgang ab, also in den sicheren Zustand.

Der Fehlercode und weitere Systemvariablen können zur Programmierung von anwenderspezifischen Fehlerreaktionen verwendet werden. Einzelheiten sind dem Handbuch des jeweiligen Moduls zu entnehmen.

Im Fehlerfall aktiviert ein Kompaktsystem die LED *ERROR,* ein F60 Modul die LED *ERR*.

6.3 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.

6.4 Sicherheitsbezogene digitale Ausgänge

Die aufgeführten Punkte gelten sowohl für die digitalen Ausgangskanäle der F60 Module als auch für die digitalen Ausgangskanäle der Kompaktsysteme. Ausgenommen sind in beiden Fällen die Relaismodule, außer diese werden spezifisch benannt.

6.4.1 Test-Routinen für digitale Ausgänge

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

- Rücklesen des Ausgangssignals des Schaltverstärkers. Die Schaltschwelle für einen rückgelesenen Low-Pegel ist 2 V. Die eingesetzten Dioden verhindern ein Rückspeisen von Signalen.
- Prüfen der integrierten zweifachen Sicherheitsabschaltung.
- Ein Abschalttest der Ausgänge erfolgt als Hintergrundtest für jeweils max. 200 µs. Der Mindestabstand zwischen zwei Tests beträgt ≥ 20 s.

Das System überwacht seine Betriebsspannung und steuert alle Ausgänge bei einer Unterspannung < 13 V ab.

6.4.2 Verhalten bei externem Kurzschluss oder Überlast

Bei einem Schluss des Ausgangs nach L- oder Überlast bleibt die Testbarkeit des Moduls erhalten. Eine Abschaltung über die Sicherheitsabschaltung ist nicht notwendig.

Die Steuerung überwacht die Gesamtstromaufnahme des Moduls und setzt bei Überschreiten der Schwelle alle Ausgangskanäle in den sicheren Zustand.

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.

6.4.3 Line Control

Die Steuerung kann sicherheitsbezogene digitale Ausgänge oder spezielle Taktausgänge takten und zusammen mit sicherheitsbezogenen digitalen Eingängen des gleichen Systems (nicht mit digitalen Eingängen von F35 03 oder F60 MI 24 01) für eine Leitungsschluss- und Leitungsbruch-Erkennung verwenden, siehe Kapitel 5.4.5.

HINWEIS

Fehlfunktionen der angeschlossenen Aktoren möglich!

Taktausgänge dürfen nicht als sicherheitsbezogene Ausgänge verwendet werden, z. B. zur Ansteuerung von sicherheitsbezogenen Aktoren!

Relaisausgänge können nicht als Taktausgänge verwendet werden.

6.5 Sicherheitsbezogene 2-polige digitale Ausgänge

Die hier beschriebenen Eigenschaften beziehen sich auf 2-polige digitale Ausgänge der Remote I/Os F3 DIO 8/8 01 und F3 DIO 16/8 01.

Die Remote I/Os testen sich automatisch während des Betriebes. Die wesentlichen Testfunktionen sind:

- Rücklesen des Ausgangssignals des Schaltverstärkers. Die eingesetzten Dioden verhindern ein Rückspeisen von Signalen.
- Prüfen der integrierten (zweifachen) Sicherheitsabschaltung
- Ein Abschalttest der Ausgänge erfolgt als Hintergrundtest für jeweils max. 200 µs. Der Mindestabstand zwischen zwei Tests beträgt ≥ 20 s.
- Leitungsdiagnose bei 2-poligem Anschluss
  F3 DIO 16/8 01:
  - Kurzschluss gegen L+, L-
  - Kurzschluss zwischen 2-poligen Anschlüssen
  - Leitungsbruch in einem der beiden 2-poligen Anschlüsse

  F3 DIO 8/8 01:
  - Kurzschluss gegen L+, L-

Das System überwacht seine Betriebsspannung und steuert alle Ausgänge bei einer Unterspannung < 13 V ab.

Bei einem 2-poligen Anschluss sind die folgenden Hinweise zu beachten:

i Unbeabsichtigtes Einschalten eines am Ausgang angeschlossenen Relais oder Aktors möglich!

Bei Anwendungen in der Maschinensicherheit sind bei Erkennen des Leitungsschlusses die Ausgänge DO+, DO- abzuschalten.

i Wenn die obigen Anforderungen nicht erfüllt werden können, ist folgender Fall zu beachten:

Bei einem Leitungsschluss von DO- nach L- kann ein Relais anziehen oder ein sonstiger Aktor in einen anderen Schaltzustand versetzt werden.

Grund: Während der für die Leitungsdiagnose laufenden Überwachungszeit liegt ein 24-V-Spannungspegel (DO+ Ausgang) am Verbraucher (Relais, schaltender Aktor) an, so dass dieser genügend elektrische Energie aufnehmen könnte, um in einen anderen Zustand zu schalten.

Die Überwachungszeit ist so zu parametrieren, dass ein Aktor vom Testimpuls für die Leitungsdiagnose nicht aktiviert werden kann.

i Störung der Leitungsbruch-Erkennung möglich!

Bei 2-poligem Anschluss darf kein DI Eingang mit einem DO Ausgang verbunden sein. Dies würde die Erkennung des Leitungsbruches verhindern.

6.5.1 Verhalten bei externem Kurzschluss oder Überlast

Bei einem Schluss des Ausgangs nach L-, L+ oder Überlast bleibt die Testbarkeit der Remote I/O erhalten. Eine Abschaltung über die Sicherheitsabschaltung ist nicht notwendig.

Die Gesamtstromaufnahme der Remote I/O wird überwacht. Bei Überschreiten der Schwelle setzt die Remote I/O alle Kanäle in den sicheren Zustand.

Die Remote I/O prüft in diesem Zustand zyklisch im Abstand weniger Sekunden, ob die Überlast der Ausgänge noch vorhanden ist. Bei Normalzustand schaltet die Remote I/O die Ausgänge wieder zu.

6.6 Relaisausgänge

Die Relaisausgänge entsprechen funktional digitalen Ausgängen, bieten aber galvanische Trennung und höhere Spannungsfestigkeit.

6.6.1 Test-Routinen für Relaisausgänge

Das Relaismodul testet seine Ausgänge automatisch während des Betriebs. 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.

Das System überwacht seine Betriebsspannung und steuert alle Ausgänge bei einer Unterspannung < 13 V ab.

Beim Modul DO 8 01 und den Remote I/Os F2 DO 8 01 und F2 DO 16 02 sind die Ausgänge mit drei Sicherheitsrelais ausgestattet:

- 2 Relais mit zwangsgeführten Kontakten.
- 1 Standardrelais.

Damit sind die Ausgänge für Sicherheitsabschaltungen verwendbar.

6.7 Analoge Ausgänge mit sicherheitsbezogener Abschaltung (F3 AIO 8/4 01)

Die Remote I/O beschreibt die analogen Ausgänge einmal je Zyklus und speichert die Werte intern.

Die Ausgänge sind nicht sicherheitsbezogen, sie können aber gemeinsam sicher abgeschaltet werden.

Zum Erreichen von SIL 4 sind die Ausgangswerte über sicherheitsbezogene analoge Eingänge zurückzulesen und im Anwenderprogramm auszuwerten. Im Anwenderprogramm sind auch Reaktionen auf fehlerhafte Ausgangswerte festzulegen.

6.7.1 Test-Routinen

Die Remote I/O testet die beiden Sicherheitsschalter für das Abschalten aller vier Ausgänge automatisch während des Betriebs.

6.8 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.

7 Software

Die Software für das sicherheitsbezogene Automatisierungssystem HIMatrix 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.

7.1 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 HIMatrix 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.

7.2 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.

7.3 Sicherheitstechnische Aspekte für die Programmierung

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

7.3.1 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!

7.3.2 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.

7.3.3 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.

7.3.4 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.

i Bei der ersten Inbetriebnahme oder einer Änderung des Anwenderprogramms einer sicherheitsbezogenen Steuerung ist ein vollständiger Funktionstest durchzuführen.

Ein Projekt-Archiv ist zu erstellen.

7.4 Parameter der Ressource

Einige Parameter werden in SILworX für die zulässigen 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 HIMatrix Systemhandbuch HI 800 140 D.**
- **Die in der Tabelle 16 als Sicherheitsparameter gekennzeichneten Parameter.**

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

7.4.1 Systemparameter der Ressource

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

Parameter	S [1)]	Beschreibung	Einstellung für sicheren Betrieb
Name	N	Name der Ressource	Beliebig
System-ID [SRS]	J	System-ID der Ressource Wertebereich: 1 … 65 535 Standardwert: 60 000 Es ist notwendig, der System-ID einen anderen Wert als den Standardwert zuweisen, sonst ist das Projekt nicht ablauffähig!	Eindeutiger Wert innerhalb des Netzwerks der Steuerungen. Das sind alle Steuerungen, die potentiell miteinander verbunden sind.
Sicherheitszeit [ms]	J	Sicherheitszeit der Ressource in Millisekunden, siehe Kapitel Sicherheitsrelevante *Zeiten im* Sicherheitshandbuch. Wertebereich: 20 … 22 500 ms. Standardwert: 600 ms bei Steuerungen, 400 ms bei Remote I/Os (online änderbar)	Applikationsspezifisch
Watchdog-Zeit [ms]	J	Watchdog-Zeit in Millisekunden, siehe Kapitel Sicherheitsrelevante *Zeiten im* Sicherheitshandbuch. Wertebereich: 4 … 5000 ms. Standardwert: 200 ms bei Steuerungen, 100 ms bei Remote I/Os (online änderbar)	Applikationsspezifisch
Sollzykluszeit [ms]	N	Gewünschte oder maximale Zykluszeit, siehe *Sollzykluszeit-Modus.* *Wertebereich*: 0 … 5000 ms. Standardwert: 0 ms (online änderbar) Die Sollzykluszeit darf höchstens so groß sein wie die eingestellte *Watchdog-Zeit [ms]* abzüglich des kleinsten einstellbarer Werts der *Watchdog-Zeit [ms]* (4 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.	Applikationsspezifisch

Parameter	S [1)]	Beschreibung	Einstellung für sicheren Betrieb
Optimierte Nutzung Kom.-Zeitscheibe	N	Der Systemparameter verkürzt die Antwortzeiten für die Kommunikation über das oder die Prozessormodule. i Es kann sich die zeitliche Ausnutzung der *Max. Kom.-Zeitscheibe [ms]* und somit der Systemparameter *Max. Dauer Konfigurationsverbindungen [ms]* ändern, so dass diese stärker beansprucht werden können, z. B. beim Reload.	---
Max. Dauer 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	Für HIMatrix Steuerungen nicht anwendbar! Standardwert: *System-Standardwerte*	---
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.	

Parameter	S [1)]	Beschreibung		Einstellung für sicheren Betrieb
Autostart	J	TRUE:	Wenn die Steuerung an die Versorgungsspannung angeschlossen wird, starten die Anwenderprogramme automatisch. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Kein automatischer Start nach Zuschalten der Versorgungsspannung.	
		Einstellungen in den Programm-Eigenschaften der Ressource beachten!		
Start erlaubt	J	TRUE:	Kaltstart oder Warmstart durch PADT im Zustand RUN oder STOPP erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Kein Start erlaubt.	
Laden erlaubt	J	TRUE:	Download der Konfiguration erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Kein Start erlaubt.	
Reload erlaubt	J	TRUE:	Reload der Konfiguration erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Reload der Konfiguration nicht erlaubt. Ein laufender Reload-Prozess wird beim Umschalten auf FALSE nicht abgebrochen.	
Globales Forcen erlaubt	J	TRUE:	Globales Forcen für diese Ressource erlaubt. Standardwert: TRUE.	Applikations-spezifisch
		FALSE:	Globales Forcen für diese Ressource nicht erlaubt.	
Globale Force-Timeout-Reaktion	N	Legt fest, wie sich die Ressource beim Ablauf des globalen Force-Timeout verhält: ▪ Nur Forcen beenden. ▪ Forcen beenden und Ressource stoppen. Standardwert: Nur Forcen beenden.		Applikations-spezifisch
Globales MultiForcen erlaubt	J	TRUE:	Anwender mit MultiForcen-Zugriff können in einer Ressource Force-Daten (Force-Werte und Force-Einzelschalter) für globale Variablen schreiben, wenn die dafür erforderlichen, übergeordneten Bedingungen gegeben und Force-Freigaben erfolgt sind.	Applikations-spezifisch
		FALSE:	Anwender mit MultiForcen-Zugriff können keine globale Variablen forcen. Standardwert: FALSE (online änderbar).	

Parameter	S [1]	Beschreibung		Einstellung für sicheren Betrieb
Minimale Konfigurationsversion	N	Mit dieser Einstellung ist es möglich, Code zu generieren, der entsprechend den Projektanforderungen zu alten oder zu neuen Versionen des HIMatrix Betriebssystems kompatibel ist. Standardwert: SILworX V11 bei neuen Projekten.		Applikationsspezifisch
		SILworX V2	Für HIMatrix Steuerungen nicht anwendbar!	
		SILworX V3		
		SILworX V4	Codegenerierung erfolgt wie bei SILworX V4, V5, oder V6.48. Der generierte Code ist kompatibel zum CPU-Betriebssystem V8.	
		SILworX V5		
		SILworX V6		
		SILworX V6b	Codegenerierung erfolgt wie bei SILworX V6.114. Der generierte Code ist kompatibel zum CPU-Betriebssystem V10.	
		SILworX V7	Codegenerierung erfolgt wie bei SILworX V7. Der generierte Code ist kompatibel zum CPU-Betriebssystem V11.	
		SILworX V8	Codegenerierung erfolgt wie bei SILworX V8. Der generierte Code ist kompatibel zum CPU-Betriebssystem V12.	
		SILworX V9	Codegenerierung erfolgt wie bei SILworX V9. Der generierte Code ist kompatibel zum CPU-Betriebssystem V13.	
		SILworX V10	Codegenerierung erfolgt wie bei SILworX V10. Der generierte Code ist kompatibel zum CPU-Betriebssystem V13.	
		SILworX V11	Codegenerierung erfolgt wie bei SILworX V11. Der generierte Code ist kompatibel zum CPU-Betriebssystem V15.	
Schneller Hochlauf	J	Die Ressource fährt bei Zuschalten der Versorgungsspannung schneller hoch, < 10 s. Siehe Kapitel Parameter «Schneller Hochlauf». Standardwert: FALSE.		Applikationsspezifisch

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

Tabelle 16: Die Systemparameter der Ressource

7.4.1.1 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.

HIMatrix 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 17: Einstellungen Sollzykluszeit-Modus

7.4.1.2 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 HIMatrix CPU wird $\mathbf{t}_{Konfig}$ wie folgt berechnet:

HIMatrix CPU $\mathbf{t}_{Konfig} = (\mathbf{n}_{Com} + \mathbf{n}_{PADT} + \mathbf{n}_{RIO}) * 0{,}25\ ms + 4\ ms$

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

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*.

7.4.1.3 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.

7.4.1.4 Parameter «Schneller Hochlauf»

Der Parameter *Schneller Hochlauf* existiert ab SILworX V7 und erfordert eine Ressource mit einem CPU-Betriebssystem ab V11 und einem COM-Betriebssystem ab V16. Außerdem muss die Ressource mit einem CPU-Boot-Loader ab V11.2 und einem COM-Boot-Loader ab V16.8 ausgestattet sein. Der Boot-Loader unterscheidet sich vom OS-Loader (Notfall-Lader) und ist nicht durch den Anwender austauschbar.

Der Parameter ist nur beim Zuschalten der Versorgungsspannung der PES wirksam. Ein Betrieb mit SIL 4 bleibt gewährleistet.

Der schnelle Hochlauf wird erreicht durch:

- Verkürzten Selbst-Test.
- Keine Prüfung auf doppelte IP-Adressen.

  Durch das Auslassen der Erkennung doppelter IP-Adressen können bei fehlerhafter Netzwerk-Konfiguration doppelte IP-Adressen im Netzwerk wirksam sein!

  Die Parametrierung muss sicherstellen, dass keine doppelten IP-Adressen im Netzwerk existieren!

Wird ein LED-Test beim Booten gewünscht, ist der Parameter *Schneller Hochlauf* auf FALSE zu setzen!

7.4.1.5 Systemvariablen der Hardware

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 Hardware.

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 2 … Leer 21	N	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
Relaiskontakt 1 … Relaiskontakt 4	N	Nur anwendbar für F60! ODER-verknüpfte Systemvariablen, die das Relais des FAULT-Kontakts auf der F60 PS 01 ansteuern. Das Relais ist ein Wechsler mit dem gemeinsamen Kontakt 2, dem Ruhekontakt 3 und dem Arbeitskontakt 1. ▪ Ist die F60 im Zustand RUN und sind die Systemvariablen *Relaiskontakt 1 … 4* FALSE, ist der Kontakt 1-2 geschlossen (Kontakt 2-3 offen). ▪ Ist die F60 im Zustand RUN und sind den Systemvariablen *Relaiskontakt 1 … 4* keine globalen Variablen zugeordnet, ist der Kontakt 1-2 geschlossen (Kontakt 2-3 offen). ▪ Ist die F60 im Zustand RUN und ist mindestens eine der Systemvariablen *Relaiskontakt 1 … 4* TRUE, ist der Kontakt 1-2 offen (Kontakt 2-3 geschlossen). ▪ Ist die F60 nicht im Zustand RUN, ist der Kontakt 1-2 offen (Kontakt 2-3 geschlossen). ▪ Ist die F60 im spannungslosen Zustand, ist der Kontakt 1-2 offen (Kontakt 2-3 geschlossen).	Applikations-spezifisch
Reload-Deaktivierung	J	Sperrt die Durchführung von Reload. Die Standardeinstellung ist FALSE.	Applikations-spezifisch
User LED 1, User LED 2	N	Nur anwendbar für spezielle Steuerungen! Steuert die entsprechende LED an, sofern vorhanden. Die Standardeinstellung ist 0.	---

Tabelle 18: Die Systemvariablen der Hardware

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

7.4.2 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.

7.5 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.

7.5.1 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 7.5.3.

⚠ 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.

7.5.2 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.

7.5.3 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 HIMatrix 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!

7.5.4 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.

7.5.5 MultiForcen

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

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

⚠ WARNUNG

Nicht steuerbares Verhalten durch den Anwender möglich!

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

⚠ WARNUNG

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

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

Näheres zum Forcen im Systemhandbuch HI 800 140 D und in der SILworX Online-Hilfe.

7.5.5.1 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.

7.5.5.2 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.

7.6 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.

8 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.

8.1 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 HIMatrix).
- 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!

8.1.1 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.

8.1.1.1 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.

8.1.2 Schritte der Programmierung

Die Programmierung von HIMatrix 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.

8.1.3 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.

8.1.4 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 19: Systemparameter des Anwenderprogramms

8.1.5 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.

8.1.6 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.

8.1.7 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.

8.1.8 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.

Die Anwendung von Reload erfordert eine Lizenz. Weitere Informationen zum Reload finden Sie im HIMatrix Systemhandbuch HI 800 140 D.

8.1.9 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.

8.1.10 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 20: 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!

8.1.11 Online-Änderung von Systemparametern

Es ist möglich, die Systemparameter der Tabelle 21 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 21: Online änderbare Parameter

8.1.12 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.
- Code-Generator-Informationen.

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

8.1.13 Multitasking

Multitasking bezeichnet die Fähigkeit der HIMatrix Systeme, bis zu 32 Anwenderprogramme innerhalb des Prozessorsystems abzuarbeiten.

Die einzelnen Anwenderprogramme lassen sich unabhängig voneinander starten und stoppen.

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

$\text{Watchdog-Zeit}_{\text{Anwenderprogramm}} = \textit{Watchdog-Zeit}_{\text{Prozessormodul}} * \textit{Maximale Zyklenanzahl}$

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 parametrierte Limitierung durch *Max Dauer pro Zyklus* erfolgt.
- Die Verteilung der Anwenderprogramm-Zyklen auf Prozessormodul-Zyklen beeinflusst die Reaktionszeit des Anwenderprogramms und der von ihm beschriebenen Variablen stark!

- Ein Anwenderprogramm wertet globale Variable, die ein anderes Anwenderprogramm beschrieben hat, um bis zu so viele Zyklen des Prozessorsystems später aus, wie der Systemparameter *Maximale CPU-Zyklen Programm* für das Programm eingestellt ist. Im ungünstigen Fall ist folgender Ablauf denkbar:
  - Programm A schreibt globale Variable, die Programm B benötigt.
  - Programm A beendet seinen Zyklus in demjenigen Zyklus des Prozessorsystems, in dem Programm B seinen Zyklus beginnt.
  - Dann kann Programm B erst beim Beginn seines nächsten Zyklus die von A geschriebenen Werte lesen.
  - Der gerade begonnene Zyklus von B kann *Maximale CPU-Zyklen Programm**Zykluszeit dauern. B erhält die von A geschriebenen Werte erst zu diesem Zeitpunkt.
  - Bis eine Reaktion von B auf diese Werte erfolgt, können weitere *Maximale CPU-Zyklen Programm* Zyklen des Prozessorsystems vergehen!

⚠ VORSICHT

Gegenseitige Beeinflussung von Anwenderprogrammen möglich!

Verwendung derselben globalen Variablen in mehreren Anwenderprogrammen kann zu gegenseitiger Beeinflussung von Anwenderprogrammen mit unterschiedlichen Auswirkungen führen.

- **Verwendung von globalen Variablen in mehreren Anwenderprogrammen genau planen.**
- **Querverweise in SILworX nutzen, um die Verwendung globaler Daten zu prüfen. Globale Daten dürfen nur an einer Stelle mit Werten beschrieben werden, entweder in einem Anwenderprogramm, von sicherheitsbezogenen Eingängen oder durch sicherheitsbezogene Kommunikationsprotokolle!**

Es liegt in der Verantwortung des Anwenders, Störungen des Betriebs durch gegenseitige Beeinflussung von Anwenderprogrammen auszuschließen!

Weitere Informationen zum Multitasking finden Sie im HIMatrix Systemhandbuch HI 800 140 D.

8.1.14 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 HIMatrix, die bereits baumustergeprüft sind.

8.2 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.

9 Konfiguration der Kommunikation

Neben den physikalischen Eingangs- und Ausgangsvariablen können Variable 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.

Dieser Datenaustausch kann sowohl lesend als auch schreibend sein.

9.1 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 je nach Ausführung der Steuerung zur Verfügung:

- SNTP
- Send/Receive TCP
- Modbus (Master/Slave)
- PROFIBUS-DP (Master/Slave)
- PROFINET und PROFIsafe (ab CPU BS V7)

Alle Standardprotokolle sind rückwirkungsfrei auf das sichere Prozessorsystem.

9.2 Sicherheitsbezogenes Protokoll safe**ethernet**

Für den sicherheitsbezogenen Datenaustausch zwischen sicherheitsbezogenen Komponenten ist safe**ethernet** einzusetzen.

Als Systemkomponente der HIMatrix ist safe**ethernet** bis SIL 4 zertifiziert.

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

Für die Berechnung der safe**ethernet** Parameter *Receive Timeout* und *Response Time* gilt folgende Bedingung:
Die Kommunikations-Zeitscheibe muss ausreichend groß sein, um in einem CPU-Zyklus alle safe**ethernet** Verbindungen abzuarbeiten.

Für sicherheitsbezogene Funktionen, die über safe**ethernet** realisiert werden, muss die Einstellung **Initialwert verwenden** benutzt werden.

HINWEIS

Unbeabsichtigter Übergang in den sicheren Zustand möglich!

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

Der Wert eines Signals muss länger als *ReceiveTMO* anstehen oder über Loop-Back überwacht werden, falls jeder Wert übertragen werden soll.

9.2.1 ReceiveTMO

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

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

Da die *ReceiveTMO* sicherheitsrelevant und Bestandteil der Worst Case Reaction Time T_R (maximale Reaktionszeit, siehe Kapitel 3.2.3ff) ist, muss die *ReceiveTMO* wie folgt berechnet und im safe**ethernet** Editor eingetragen werden.

ReceiveTMO ≥ 4*Delay + 5*max. Zykluszeit

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

Delay:	Verzögerung auf der Übertragungsstrecke, z. B. durch Switch, Satellit
max. Zykluszeit:	maximale Zykluszeit der beiden Steuerungen

i Eine erwünschte Fehlertoleranz der Kommunikation kann über eine Erhöhung der *ReceiveTMO* erreicht werden, sofern dies für den Anwendungsprozess zeitlich zulässig ist.

HINWEIS

Der maximal zulässige Wert für *ReceiveTMO* hängt vom Anwendungsprozess ab und wird im safe**ethernet Editor zusammen mit der maximal zu erwartenden Response Time und dem Profil eingestellt.**

9.2.2 Response-Time

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

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

Die vorgegebene *ResponseTime* hat Einfluss auf die Konfiguration aller Parameter der safe**ethernet** Verbindung, die wie folgt zu berechnen sind:

ResponseTime ≤ ReceiveTMO / n

n = 2, 3, 4, 5, 6, 7, 8.....

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

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

min. ResponseTime ≤ ReceiveTMO / 2 ≥ 2*Delay + 2,5*max. Zykluszeit

Ist diese Bedingung erfüllt, kann der Verlust wenigstens eines Datenpaketes abgefangen werden, ohne dass die safe**ethernet** Verbindung / Peer-to-Peer-Verbindung unterbrochen wird.

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

i Es ist sicherzustellen, dass das Kommunikationssystem die parametrierte Response-Time einhält!

Für Fälle, in denen dies nicht immer garantieren werden kann, steht zur Überwachung der Response-Time eine entsprechende Systemvariable der Verbindung zur Verfügung. Kommt es nicht nur in seltenen Einzelfällen zu einer Überschreitung der gemessenen Response-Time über die halbe ReceiveTMO, muss die parametrierte Response-Time erhöht werden.

Die Receive Timeout ist der neu parametrierten Response Time anzupassen.

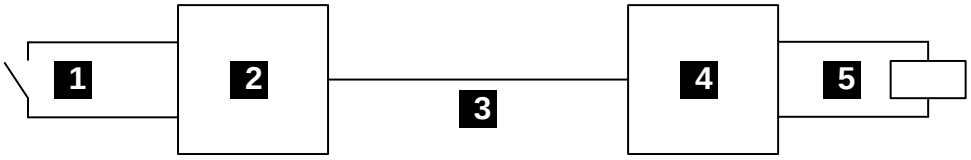
HINWEIS

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 die Sicherheitszeit wie folgt eingestellt ist:

Sicherheitszeit = 2 * Watchdog-Zeit

9.2.3 Berechnung der maximalen Reaktionszeit

Die maximale Reaktionszeit T_R (*Worst Case*) vom Wechsel einer Feldkomponente der Steuerung 1 (In) bis zur Reaktion des Ausgangs (Out) der Steuerung 2 kann wie folgt berechnet werden:



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

Bild 4: Reaktionszeit bei Verbindung zweier HIMatrix Steuerungen

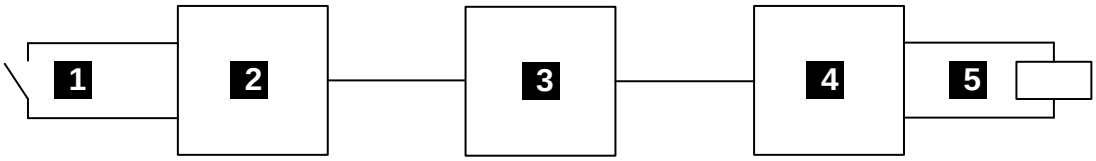
$$\mathbf{T_R = t_1 + t_2 + t_3}$$

T_R	Worst Case Reaction Time
t_1	2 ∗ Watchdog-Zeit der Steuerung 1
t_2	ReceiveTMO
t_3	2 ∗ Watchdog-Zeit der Steuerung 2

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

9.2.4 Berechnung der max. Reaktionszeit mit zwei Remote I/Os

Die maximale Reaktionszeit T_R vom Wechsel einer Feldkomponente (In) der ersten Remote I/O bis zur Reaktion des Ausgangs (Out) der zweiten Remote I/O kann wie folgt berechnet werden:



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

Bild 5: Reaktionszeit mit Remote I/Os

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

T_R	Worst Case Reaction Time
t_1	2 ∗ Watchdog-Zeit der Remote I/O 1
t_2	$ReceiveTMO_1$
t_3	2 ∗ Watchdog-Zeit der Steuerung
t_4	$ReceiveTMO_2$
t_5	2 ∗ Watchdog-Zeit der Remote I/O 2

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

9.2.5 Begriffe

ReceiveTMO	Überwachungszeit in Steuerung 1, in der eine gültige Antwort von Steuerung 2 empfangen werden muss. Nach Ablauf der Zeit wird die sicherheitsbezogene Kommunikation geschlossen.
$ReceiveTMO_1$	Remote I/O 1 → Steuerung
$ReceiveTMO_2$	Steuerung → Remote I/O 2
Watchdog-Zeit	Maximal zulässige Dauer des RUN-Zyklus eines PES
Worst Case	Maximale Reaktionszeit für die Übertragung der Änderung des Signals eines physikalischen Einganges (In) einer Steuerung 1 bis zur Änderung des physikalischen Ausgangs (Out) einer Steuerung 2.

Die Datenübertragung erfolgt mit einem sicherheitsbezogenen Protokoll.

9.2.6 Vergabe der safe**ethernet**-Adressen

Bei der Vergabe der Netzwerkadressen (IP-Adressen) für safe**ethernet** auf folgende Punkte achten:

- Die Adressen müssen eindeutig im verwendeten Netz sein.
- Beim Verbinden des safe**ethernet** mit einem anderen Netz (betriebsinternes LAN, usw.), darauf achten, dass keine Störungen auftreten können. Mögliche Störquellen sind z. B.:
  - Der dort anfallende Datenverkehr.
  - Die Kopplung mit weiteren Netzen (z. B. Internet).

In solchen Fällen geeignete Maßnahmen treffen, z. B. Einsatz von Ethernet-Switches, Firewall, um den Störungen entgegenzuwirken.

---

i Der Betreiber hat dafür zu sorgen, dass das für die safe**ethernet** Kommunikation / Peer-to-Peer-Kommunikation verwendete Ethernet ausreichend vor Manipulationen (z. B. durch Hacker) geschützt wird.

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

Anhang

Glossar

Begriff	Beschreibung
AI	Analog Input: Analoger Eingang
AO	Analog Output: Analoger Ausgang
ARP	Address Resolution Protocol: Netzwerkprotokoll zur Zuordnung von Netzwerkadressen zu Hardware-Adressen
COM	Kommunikation (-modul)
CRC	Cyclic Redundancy Check: Prüfsumme
DI	Digital Input: Digitaler Eingang
DO	Digital Output: Digitaler Ausgang
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Normen
ESD	Electrostatic Discharge: Elektrostatische Entladung
FB	Feldbus
FBS	Funktionsbausteinsprache
HW	Hardware
ICMP	Internet Control Message Protocol: Netzwerkprotokoll für Status- und Fehlermeldungen
IEC	Internationale Normen für die Elektrotechnik
LS/LB	Leitungsschluss/Leitungsbruch
MAC	Media Access Control: Hardware-Adresse eines Netzwerkanschlusses
PADT	Programming and Debugging Tool (nach IEC 61131-3), PC mit SILworX
PE	Protective Earth: Schutzerde
PELV	Protective Extra Low Voltage: Funktionskleinspannung mit sicherer Trennung
PES	Programmierbares Elektronisches System
R	Read, Auslesen einer Variablen
rückwirkungsfrei	Eingänge sind für rückwirkungsfreien Betrieb ausgelegt und können in Schaltungen mit Sicherheitsfunktionen eingesetzt werden.
R/W	Read/Write (Spaltenüberschrift für Art von Systemvariable)
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

Tabellenverzeichnis

Index

HANDBUCH
HIMatrix Sicherheitshandbuch Bahn

HI 800 436 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