

HIMatrix[®] M45

Sicherheitshandbuch

SAFETY
NONSTOP



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.

HIMax[®], HIMatrix[®], SILworX[®], XMR[®] 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.

Weitere Informationen sind in der Dokumentation auf der HIMA DVD und auf unserer Webseite unter <http://www.hima.de> und <http://www.hima.com> zu finden.

© Copyright 2015, HIMA Paul Hildebrandt GmbH

Alle Rechte vorbehalten.

Kontakt

HIMA Adresse:

HIMA Paul Hildebrandt GmbH

Postfach 1261

68777 Brühl

Tel: +49 6202 709-0

Fax: +49 6202 709-107

E-Mail: info@hima.com

Revisions- index	Änderungen	Art der Änderung	
		technisch	redaktionell
1.00	Erste Ausgabe	X	X
1.01	Überarbeitet, gelöscht: Fehlertoleranzzeit, Arbeitsstromprinzip, die Unterkapitel „Reaktion im Fehlerfall“	X	X
1.02	Geändert: Kap. Sicherheitshandbuch, Proof Test		X
2.00	Anpassen an SILworX V7, Betriebssystem V11/16, eingefügt: Reaktionen im Fehlerfall, geändert: Reaktionszeit	X	X

Inhaltsverzeichnis

1	Sicherheitshandbuch	7
1.1	Aufbau und Gebrauch der Dokumentation	7
1.2	Zielgruppe	8
1.3	Darstellungskonventionen	8
1.3.1	Sicherheitshinweise	8
1.3.2	Gebrauchshinweise	9
2	Hinweise zum Einsatz	10
2.1	Bestimmungsgemäßer Einsatz	10
2.1.1	Anwendungsbereich	10
2.1.1.1	Anwendung im Ruhestromprinzip	10
2.1.1.2	Einsatz in Brandmelderzentralen	10
2.2	Umgebungsbedingungen	10
2.3	Aufgaben der Maschinen- und Anlagenhersteller sowie des Betreibers	10
2.3.1	Anschluss von Kommunikationspartnern	11
2.3.2	Verwendung der sicherheitsgerichteten Kommunikation	11
2.4	ESD-Schutzmaßnahmen	11
2.5	Restrisiken	11
2.6	Sicherheitsvorkehrungen	11
2.7	Notfallinformationen	11
2.8	Weitere Systemdokumentationen	12
3	Sicherheitskonzept für den Einsatz der PES	13
3.1	Sicherheit und Verfügbarkeit	13
3.1.1	Berechnungen von PFD, PFH und SFF	13
3.1.2	Selbsttest und Fehlerdiagnose	13
3.1.3	PADT	14
3.2	Für die Sicherheit wichtige Zeiten	14
3.2.1	Sicherheitszeit des PES	14
3.2.2	Sicherheitszeit des Anwenderprogramms	14
3.2.3	Maximale Reaktionszeit	14
3.2.4	Watchdog-Zeit des Prozessorsystems	15
3.2.5	Watchdog-Zeit des Anwenderprogramms	15
3.3	Wiederholungsprüfung (Proof Test nach IEC 61508-4, Absatz 3.8.5)	15
3.3.1	Durchführung der Wiederholungsprüfung	16
3.3.2	Häufigkeit der Wiederholungsprüfungen	16
3.4	Sicherheitsauflagen	16
3.4.1	Hardware-Projektierung	16
3.4.1.1	Produktunabhängige Auflagen	16
3.4.1.2	Produktabhängige Auflagen	16
3.4.2	Programmierung	17
3.4.2.1	Produktunabhängige Auflagen	17
3.4.2.2	Produktabhängige Auflagen	17
3.4.3	Kommunikation	17
3.4.4	Wartungseingriffe	17
3.4.5	Cyber Security bei HIMatrix M45 Systemen	17

3.5	Zertifizierung	19
3.5.1	TÜV-Zertifikat/EG-Baumusterprüfung	19
3.5.2	Normenspiegel	19
3.5.3	Prüfbedingungen	20
3.5.3.1	Klimatische Bedingungen	20
3.5.3.2	Mechanische Bedingungen	21
3.5.3.3	EMV-Bedingungen	21
3.5.3.4	Versorgungsspannung	23
4	Zentrale Funktionen	24
4.1	Stromversorgung	24
4.2	Funktionsbeschreibung des Prozessorsystems	24
4.3	Selbst-Tests	25
4.3.1	Mikroprozessor-Test	25
4.3.2	Test der Speicherbereiche	25
4.3.3	Gesicherte Speicherbereiche	25
4.3.4	RAM-Test	25
4.3.5	Watchdog-Test	25
4.3.6	Reaktionen auf Fehler im Prozessorsystem	25
4.4	Fehlerdiagnose	25
5	Eingänge	27
5.1	Allgemeines	27
5.2	Sicherheit von Sensoren, Encodern und Transmittern	27
5.3	Reaktion im Fehlerfall	27
5.4	Sicherheitsgerichtete digitale Eingänge	27
5.4.1	Allgemeines	27
5.4.2	Test-Routinen	27
5.4.3	Surge auf digitalen Eingängen	27
5.4.4	Line Control	28
5.5	Sicherheitsgerichtetes Zählermodul	29
5.6	Checkliste für sicherheitsgerichtete Eingänge	29
6	Ausgänge	30
6.1	Allgemeines	30
6.2	Sicherheit von Aktoren	30
6.3	Reaktion im Fehlerfall	30
6.4	Sicherheitsgerichtete digitale Ausgänge	30
6.4.1	Testroutinen für digitale Ausgänge	30
6.4.2	Verhalten bei externem Kurzschluss oder Überlast	31
6.5	Relaisausgänge	31
6.5.1	Testroutinen für Relaisausgänge	31
6.6	Checkliste für sicherheitsgerichtete Ausgänge	31
7	Software für HIMatrix M45 Systeme	32
7.1	Sicherheitstechnische Aspekte für das Betriebssystem	32
7.2	Arbeitsweise und Funktionen des Betriebssystems	32
7.3	Sicherheitstechnische Aspekte für die Programmierung	33
7.3.1	Sicherheitskonzept des Programmierwerkzeugs	33

7.3.2	Überprüfung der Konfiguration und des Anwenderprogramms	33
7.3.3	Archivierung eines Projekts	33
7.3.4	Möglichkeit zur Programm- und Konfigurations-Identifizierung	34
7.4	Parameter der Ressource	34
7.4.1	Systemparameter	34
7.4.1.1	Systemparameter der Ressource	34
7.4.1.2	Verwendung der Parameter <i>Sollzykluszeit</i> und <i>Sollzykluszeit-Modus</i>	36
7.4.1.3	Berechnung der <i>Maximalen Dauer der Konfigurationsverbindungen [μs]</i>	37
7.4.1.4	Hinweise zum Parameter <i>Minimale Konfigurationsversion</i>	37
7.4.1.5	Hinweis zum Parameter <i>Schnelles Hochfahren</i>	38
7.4.1.6	Systemvariable der Hardware	38
7.5	Checkliste zur Erstellung eines Anwenderprogramms	39
8	Sicherheitstechnische Aspekte für das Anwenderprogramm	40
8.1	Rahmen für den sicherheitsgerichteten Einsatz	40
8.1.1	Basis der Programmierung	40
8.1.2	Funktionen des Anwenderprogramms	41
8.1.3	Variablendeklaration	41
8.1.4	Dokumentation der anwenderspezifischen LEDs	41
8.2	Vorgehensweisen	42
8.2.1	Zuordnung von Variablen zu Ein-/Ausgängen	42
8.2.2	Ab- und Aufschließen der Steuerung	42
8.2.3	Code-Erzeugung	43
8.2.4	Laden und Starten des Anwenderprogramms	43
8.2.5	Reload	43
8.2.6	Forcen	44
8.2.6.1	Forcen von Datenquellen	44
8.2.7	Online-Änderung von Systemparametern	45
8.2.8	Projekt-Dokumentation für sicherheitsgerichtete Anwendungen	45
8.2.9	Multitasking	46
8.2.10	Abnahme durch Genehmigungsbehörden	46
9	Kommunikation	47
9.1	Standardprotokolle	47
9.2	Sicherheitsgerichtetes Protokoll safeethernet	47
9.2.1	Receive Timeout	47
9.2.2	Response Time	48
9.2.3	Berechnung der max. Reaktionszeit mit zwei Remote I/Os	49
9.2.4	Berechnung der max. Reaktionszeit, zwei HIMatrix M45, eine HIMax Steuerung	49
9.2.5	Begriffe	50
9.2.6	Vergabe der safeethernet-Adressen	50
	Anhang	51
	Glossar	51
	Abbildungsverzeichnis	52
	Tabellenverzeichnis	53
	Index	54

1 Sicherheitshandbuch

Dieses Handbuch enthält Informationen für den bestimmungsgemäßen Gebrauch der sicherheitsgerichteten HIMatrix Automatisierungsgeräte.

Voraussetzung für die risikolose Installation, Inbetriebnahme und für die Sicherheit bei Betrieb und Instandhaltung der HIMatrix M45 Automatisierungssysteme sind:

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

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

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

HIMA entwickelt, fertigt und prüft HIMatrix M45 Automatisierungssysteme unter Beachtung der einschlägigen Sicherheitsnormen. Die Verwendung der Geräte ist nur zulässig, wenn alle folgenden Voraussetzungen erfüllt sind:

- Nur die in den Beschreibungen vorgesehenen Einsatzfälle.
- Nur die spezifizierten Umgebungsbedingungen.
- Nur in Verbindung mit zugelassenen Fremdgeräten.

Aus Gründen der Übersichtlichkeit enthält dieses Handbuch nicht sämtliche Details aller Ausführungen der HIMatrix M45 Automatisierungsgeräte. Weitere Details sind den jeweiligen Handbüchern zu entnehmen.

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 Aufbau und Gebrauch der Dokumentation

Dieses Sicherheitshandbuch enthält folgende Themen:

- Bestimmungsgemäßer Einsatz
- Sicherheitskonzept
- Zentrale Funktionen
- Eingänge
- Ausgänge
- Software
- Sicherheitstechnische Aspekte für das Anwenderprogramm
- Konfiguration der Kommunikation
- Einsatz in Brandmelderzentralen
- Anhang:
 - Erhöhung des SIL von Sensoren und Aktoren
 - Glossar
 - Verzeichnisse/Index

1.2 Zielgruppe

Dieses Dokument wendet sich an Planer, Projektoren und Programmierer von Automatisierungsanlagen sowie Personen, die zu Inbetriebnahme, Betrieb und Wartung der Geräte, Module und Systeme berechtigt sind. Vorausgesetzt werden spezielle Kenntnisse auf dem Gebiet der sicherheitsgerichteten Automatisierungssysteme.

1.3 Darstellungskonventionen

Zur besseren Lesbarkeit und zur Verdeutlichung gelten in diesem Dokument folgende Schreibweisen:

Fett	Hervorhebung wichtiger Textteile Bezeichnungen von Schaltflächen, Menüpunkten und Registern im Programmierwerkzeug, die angeklickt werden können
<i>Kursiv</i>	Parameter und Systemvariablen
<code>Courier</code>	Wörtliche Benutzereingaben
RUN	Bezeichnungen von Betriebszuständen in Großbuchstaben
Kap. 1.2.3	Querverweise sind Hyperlinks, auch wenn sie nicht besonders gekennzeichnet sind. Wird der Mauszeiger darauf positioniert, verändert er seine Gestalt. Bei einem Klick springt das Dokument zur betreffenden Stelle.

Sicherheits- und Gebrauchshinweise sind besonders gekennzeichnet.

1.3.1 Sicherheitshinweise

Die Sicherheitshinweise im Dokument sind wie folgend beschrieben dargestellt. Um ein möglichst geringes Risiko zu gewährleisten, sind sie unbedingt zu befolgen. Der inhaltliche Aufbau ist:

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

SIGNALWORT



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

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.

2 Hinweise zum Einsatz

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

2.1 Bestimmungsgemäßer Einsatz

Dieses Kapitel beschreibt die Bedingungen für den Einsatz von HIMatrix M45 Systemen.

2.1.1 Anwendungsbereich

Die sicherheitsgerichteten Steuerungen HIMatrix sind einsetzbar bis zum Sicherheits-Integritätslevel SIL 3 gemäß IEC 61508.

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

2.1.1.1 Anwendung im Ruhestromprinzip

Die Automatisierungsgeräte sind für das Ruhestromprinzip konzipiert.

Ein System, das nach dem Ruhestromprinzip funktioniert, um seine Sicherheitsfunktion auszuführen, nimmt im Fehlerfall den spannungs- oder stromlosen Zustand ("de-energize to trip") ein.

2.1.1.2 Einsatz in Brandmelderzentralen

HIMatrix Systeme sind für Brandmelderzentralen nach DIN EN 54-2 und NFPA 72 geeignet. In diesen Systemen ist folgendes gefordert:

- Auf Anforderung wird der aktive Zustand zur Beherrschung des Risikos angenommen.
- Leitungsbruch- und Leitungsschlusserkennung

Die Umgebungsbedingungen sind zu beachten!

Zu Einzelheiten siehe das Sicherheitshandbuch der HIMatrix F-Systeme, HI 800 022 D.

2.2 Umgebungsbedingungen

Art der Bedingung	
Schutzklasse	Schutzklasse III nach IEC/EN 61131-2
Umgebungstemperatur	0...+60 °C
Lagertemperatur	-40...+85 °C
Verschmutzung	Verschmutzungsgrad II nach IEC/EN 61131-2
Aufstellhöhe	< 2000 m
Gehäuse	Standard: IP20
Anforderungen der Applikation	Falls es die zutreffenden Applikationsnormen (z. B. EN 60204, EN 13849) fordern, muss das HIMatrix System in ein Gehäuse der geforderten Schutzart (z. B. IP54) eingebaut werden.
Versorgungsspannung	24 VDC

Tabelle 1: Umgebungsbedingungen

Die in diesem Handbuch genannten Umgebungsbedingungen sind beim Betrieb des HIMatrix Systems einzuhalten.

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 sicherheitsgerichteten Kommunikation

Bei der Verwendung der sicherheitsgerichteten Kommunikation zwischen verschiedenen Geräten muss beachtet werden, dass die Gesamtreaktionszeit des Systems nicht die Fehlertoleranzzeit überschreitet. Die in Kapitel aufgeführten Berechnungsgrundlagen sind anzuwenden.

2.4 ESD-Schutzmaßnahmen

Nur Personal, das Kenntnisse über ESD-Schutzmaßnahmen besitzt, darf Änderungen oder Erweiterungen des Systems oder den Austausch eines Moduls durchführen.

HINWEIS



Elektrostatische Entladungen können die in den HIMatrix Systemen eingebauten elektronischen Bauteile beschädigen!

- 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 Restrisiken

Von einem HIMatrix M45 System selbst geht kein Risiko aus.

Restrisiken können ausgehen von:

- Fehlern in der Projektierung
- Fehlern im Anwenderprogramm
- Fehlern in der Verdrahtung

2.6 Sicherheitsvorkehrungen

Am Einsatzort geltende Sicherheitsbestimmungen beachten und vorgeschriebene Schutzausrüstung tragen.

2.7 Notfallinformationen

Ein HIMatrix M45 System ist Teil der Sicherheitstechnik einer Anlage. Der Ausfall eines Geräts oder eines Moduls bringt die Anlage in den sicheren Zustand.

Im Notfall ist jeder Eingriff, der die Sicherheitsfunktion der HIMatrix M45 Systeme verhindert, verboten.

2.8 Weitere Systemdokumentationen

Für die Projektierung der HIMatrix M45 Systeme stehen außerdem noch folgende Dokumentationen zur Verfügung:

Name	Inhalt	Dokument-Nr.	Format
HIMatrix M45 Systemhandbuch	Beschreibungen des M45 Systems mit technischen Daten	HI 800 650 D	PDF-Datei
Zertifikat	Prüfergebnis		PDF-Datei
Versionsliste	Vom TÜV geprüfte Versionen		PDF-Datei
HIMatrix M45 Modulhandbücher			PDF-Dateien
Kommunikationshandbuch	Beschreibung der Kommunikationsprotokolle, ComUserTask und ihrer Projektierung in SILworX	HI 801 100 D	PDF-Datei
SILworX Online-Hilfe	SILworX-Bedienung	-	chm-Datei
SILworX Handbuch Erste Schritte	Einführung in SILworX	HI 801 102 D	PDF-Datei

Tabelle 2: Systemdokumentation HIMatrix M45

Einzelheiten zu den Modulen in den jeweiligen Handbüchern.

3 Sicherheitskonzept für den Einsatz der PES

Dieses Kapitel behandelt wichtige allgemeine Fragen der funktionellen Sicherheit von HIMatrix M45 Systemen:

- Sicherheit und Verfügbarkeit
- Für Sicherheit wichtige Zeiten
- Wiederholungsprüfung
- Sicherheitsauflagen
- Zertifizierung

3.1 Sicherheit und Verfügbarkeit

Die HIMatrix M45 Systeme sind für Prozess-Steuerungen, Schutzsysteme, Brenner- und Maschinensteuerungen zertifiziert.

Von den HIMatrix M45 Systemen gehen keine unmittelbaren Risiken aus.

WARNUNG



Personenschaden durch falsch angeschlossene oder falsch programmierte sicherheitsgerichtete Automatisierungssysteme möglich!
Anschlüsse vor Inbetriebnahme prüfen und Gesamtanlage auf Einhaltung der spezifizierten Sicherheitsanforderungen testen!

3.1.1 Berechnungen von PFD, PFH und SFF

Für die HIMatrix M45 Systeme wurden gemäß IEC 61508 die Berechnungen von PFD, PFH und SFF durchgeführt.

Die Werte für PFD, PFH und SFF werden auf Anfrage von HIMA mitgeteilt.

3.1.2 Selbsttest und Fehlerdiagnose

Das Betriebssystem der Steuerungen führt beim Start und im laufenden Betrieb umfangreiche Selbsttests durch. Getestet werden dabei vor allem:

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

Stellen diese Tests Fehler fest, dann schaltet das Betriebssystem das defekte Modul 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 M45 Module verfügen jeweils über eigene LEDs zur Anzeige der entdeckten Fehler. Damit ist im Störfall eine schnelle Fehlerdiagnose über ein als fehlerhaft gemeldetes Gerät oder der externen Beschaltung möglich.

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

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

Details über die Auswertung der Diagnosemeldungen siehe auch Systemhandbuch, HI 800 650 D.

Bei einem sehr kleinen Teil der Bauelement-Ausfälle, welche die Sicherheit nicht beeinflussen, erzeugt das HIMatrix M45 System keine Diagnoseinformation.

3.1.3 PADT

Mit dem PADT erstellt der Anwender das Programm und konfiguriert die Steuerung. 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 Planungswerkzeug SILworX installiert ist.

3.2 Für die Sicherheit wichtige Zeiten

Diese sind:

- Sicherheitszeit
- Watchdog-Zeit
- Maximale Reaktionszeit

3.2.1 Sicherheitszeit des PES

Die Sicherheitszeit ist die Zeit, in der das PES im RUN-Zustand nach Auftreten eines internen Fehlers reagieren muss.

Von der Prozessseite her gesehen, ist die Sicherheitszeit die maximale Zeit, in der das Sicherheitssystem bei einer Änderung von Eingangssignalen an den Ausgängen reagieren muss (Reaktionszeit).

Die Einstellung der Sicherheitszeit hat keinen Einfluss auf das HIMatrix M45 PES.

3.2.2 Sicherheitszeit des Anwenderprogramms

Die Sicherheitszeit des Anwenderprogramms lässt sich nicht unmittelbar einstellen. HIMatrix M45 errechnet die Sicherheitszeit eines Anwenderprogramms aus den Parametern *Sicherheitszeit* der Ressource und *Maximale Zyklusanzahl*. Zu Einzelheiten siehe Kapitel 8.2.9.

3.2.3 Maximale Reaktionszeit

Die maximale Reaktionszeit gilt für ein ungestörtes System. Sie ist die maximale Zeit, die das HIMatrix M45 System benötigen darf, um auf die Änderung eines Eingangssignals durch ein entsprechendes Ausgangssignal zu antworten. Bei den zyklisch arbeitenden HIMatrix M45-Steuerungen ist die maximale Reaktionszeit die doppelte maximale Zykluszeit, also die doppelte Watchdog-Zeit. Die Voraussetzungen dafür sind:

- Die Logik des Anwenderprogramms enthält keine Verzögerungen.
- Ein Zyklus des Anwenderprogramms dauert einen Zyklus des Prozessorsystems.

Die Zykluszeit einer Steuerung besteht aus folgenden wesentlichen Teilen:

- Lesen der Eingänge
- Verarbeiten des Anwenderprogramms bzw. der Anwenderprogramme
- Schreiben der Ausgänge
- Prozessdatenkommunikation
- Ausführen der Testroutinen

Zusätzlich sind bei der Worst Case-Betrachtung des gesamten Systems die Schaltzeiten der Eingänge und Ausgänge zu berücksichtigen.

Die Reaktionszeit setzt sich im Allgemeinen zusammen aus:

- Schaltzeit des Eingangs
- Doppelte Watchdog-Zeit des Anwenderprogramms

- Schaltzeit des Ausgangs

Zur Berechnung der Reaktionszeit bei Kommunikation siehe Kapitel 9 oder das Kommunikationshandbuch HI 801 100 D.

3.2.4 Watchdog-Zeit des Prozessorsystems

Die Watchdog-Zeit wird im Menü für die Einstellung der Eigenschaften des PES vorgegeben. Sie ist die maximal zulässige Dauer eines RUN-Zyklus (Zykluszeit). Überschreitet die Zykluszeit die vorgegebene Watchdog-Zeit, so schaltet das System ab. Anschließend startet das System neu, falls Autostart parametrisiert wurde. Falls Autostart nicht parametrisiert wurde, geht das System in den Zustand STOPP/GÜLTIGE KONFIGURATION.

Die Watchdog-Zeit des Prozessorsystems ist $\leq \frac{1}{2} \cdot \text{Sicherheitszeit des PES}$ einzustellen.

Wertebereich Watchdog-Zeit	Standardwert
4...5 000 ms	200 ms

Tabelle 3: Wertebereich der Watchdog-Zeit

Die Watchdog-Zeit des Prozessorsystems muss so groß eingestellt sein, dass im fehlerfreien Betrieb auftretende Lastspitzen nicht zu einem Fehlerstopp durch Überschreiten der Watchdog-Zeit führen.

Zur Abschätzung einer geeigneten Einstellung empfiehlt HIMA einen Test am weitestgehend vollständigen System:

- Die HIMatrix M45 Hardware ist vollständig aufgebaut.
- Kommunikationspartner sind vorhanden, evtl. als Simulationen.
- Sensoren und Aktoren sind evtl. als Simulationen vorhanden.
- Das Projekt ist möglichst vollständig vorhanden.

Minimalen Wert für die Watchdog-Zeit ermitteln

1. System unter voller Last betreiben. Auch die Kommunikation sollte mit voller Last arbeiten.
 2. Eingangsdaten so vorgeben, dass möglichst die längsten Programmpfade durchlaufen werden. Dazu können Sequenzen von Eingangswerten nötig sein.
 3. Reload durchführen.
 4. Im Control Panel die Maximalwerte der Zykluszeiten betrachten. Die größten Zykluszeit-Werte notieren.
- Der Minimalwert für die Watchdog-Zeit ist die höchste abgelesene Zykluszeit.

Der eingestellte Wert der Watchdog-Zeit sollte der ermittelte Minimalwert, erhöht um einen Sicherheitszuschlag, sein.

3.2.5 Watchdog-Zeit des Anwenderprogramms

Jedes Anwenderprogramm hat eine eigene Watchdog-Zeit.

Die Watchdog-Zeit des Anwenderprogramms lässt sich nicht unmittelbar einstellen. HIMatrix M45 Systeme errechnen die Watchdog-Zeit eines Anwenderprogramms aus den Parametern *Watchdog-Zeit* der Ressource und *Maximale Zyklenanzahl*.

Es ist darauf zu achten, dass die errechnete Watchdog-Zeit höchstens halb so groß ist wie die Reaktionszeit, die für den vom Anwenderprogramm bearbeiteten Teil des Prozesses gefordert ist.

3.3 Wiederholungsprüfung (Proof Test nach IEC 61508)

Eine Wiederholungsprüfung ist eine Prüfung zur Aufdeckung verdeckter Fehler in einem sicherheitstechnischen System, so dass das System, wenn nötig, wieder in einen Zustand gebracht werden kann, in dem es seine geplante Funktion erfüllt.

HIMA Sicherheitssysteme müssen **in Intervallen von 10 Jahren** einer Wiederholungsprüfung unterzogen werden.

Durch eine Analyse der realisierten Sicherheitskreise mittels Berechnung kann das Intervall häufig verlängert werden.

Bei Modulen mit Relaisausgängen muss die Wiederholungsprüfung für die Relais in für die Anlage festgelegten Intervallen erfolgen.

3.3.1 Durchführung der Wiederholungsprüfung

Die Durchführung der Wiederholungsprüfung hängt davon ab, wie die Anlage (EUC = equipment under control) beschaffen ist und welches Gefährdungspotential sie hat, und welche der Normen daher für den Betrieb der Anlage zur Anwendung kommen und von der zuständigen Prüfstelle als Grundlage für die Genehmigung benutzt wurden.

Nach den Normen IEC 61508 1-7, IEC 61511 1-3, IEC 62061 und VDI/VDE 2180 Blatt 1 bis 4 hat bei sicherheitsgerichteten Systemen der Betreiber für eine Wiederholungsprüfung zu sorgen.

3.3.2 Häufigkeit der Wiederholungsprüfungen

Die HIMatrix M45 Steuerung kann einer Wiederholungsprüfung unterzogen werden, indem der gesamte Sicherheitskreis überprüft wird.

In der Praxis wird für die Eingangs- und Ausgangs-Feldgeräte ein kürzeres Intervall für die Wiederholungsprüfung (z. B. alle 6 oder 12 Monate) gefordert als für die HIMatrix M45 Steuerung. Wenn der Anwender den kompletten Sicherheitskreis wegen des Feldgeräts prüft, dann ist die HIMatrix M45 Steuerung in diesen Test automatisch eingeschlossen. Es sind dann keine zusätzlichen Wiederholungsprüfungen für die HIMatrix M45 Steuerung erforderlich.

Falls die Wiederholungsprüfung der Feldgeräte die HIMatrix M45 Steuerung nicht mit einbezieht, dann muss diese für SIL 3 mindestens einmal in 10 Jahren überprüft werden. Dies kann erreicht werden, indem die HIMatrix M45 Steuerung neu gestartet wird.

Gibt es für spezielle Module zusätzliche Anforderungen für die Wiederholungsprüfung, dann ist das Handbuch des jeweiligen Moduls zu beachten.

3.4 Sicherheitsauflagen

Für den Einsatz der sicherheitsgerichteten PES des Systems HIMatrix M45 gelten folgende Sicherheitsauflagen:

3.4.1 Hardware-Projektierung

Personen, die die HIMatrix M45 Hardware projektieren, müssen die folgenden Sicherheitsauflagen beachten.

3.4.1.1 Produktunabhängige Auflagen

- Für sicherheitsgerichteten Betrieb darf nur hierfür zugelassene sicherheitsgerichtete Hardware und Software verwendet werden. Die zugelassene Hardware und Software ist in der *Versionsliste der Module und der Firmware der HIMatrix M45 Systeme der Firma HIMA Paul Hildebrandt GmbH, Zertifikatsnummer 01/205/5355/00/13* aufgeführt. Die jeweils aktuellen Versionsstände sind der gemeinsam mit der Prüfstelle geführten Versionsliste zu entnehmen. Die aktuelle Versionsliste befindet sich auf der HIMA Webseite www.hima.de.
- Die spezifizierten Umgebungsbedingungen (siehe Kapitel 2.2) bezüglich EMV, mechanischen, chemischen, klimatischen Einflüssen müssen eingehalten werden.

3.4.1.2 Produktabhängige Auflagen

- 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 den Ausführungen PELV oder SELV eingesetzt werden.

Die Netzgeräte müssen auch im Fehlerfall eine Versorgungsspannung ≤ 35 V abgeben!

3.4.2 Programmierung

Personen, die Anwenderprogramme erstellen, müssen die folgenden Sicherheitsauflagen beachten.

3.4.2.1 Produktunabhängige Auflagen

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

3.4.2.2 Produktabhängige Auflagen

Auflagen für die Verwendung des Programmierwerkzeugs

- Zur Programmierung ist das Werkzeug **SILworX** zu verwenden.
- **Die korrekte Umsetzung der Spezifikation der Applikation ist zu validieren und zu verifizieren. Es muss eine vollständige Prüfung der Logik durch Erprobung erfolgen.**
- Die Fehlerreaktion des Systems bei Fehlern in den fehlersicheren Eingangsmodulen und Ausgangsmodulen muss gemäß den anlagenspezifischen sicherheitstechnischen Gegebenheiten durch das Anwenderprogramm festgelegt werden.

3.4.3 Kommunikation

- Bei Verwendung der sicherheitsgerichteten Kommunikation zwischen verschiedenen Geräten ist zu beachten, dass die Gesamtreaktionszeit des Systems nicht die zulässige Reaktionszeit überschreitet. Die im Kapitel 9.2 aufgeführten Berechnungsgrundlagen sind anzuwenden.
- Bei der Übertragung von (sicherheitsrelevanten) Daten sind Regeln der Cyber Security (IT-Sicherheit) zu beachten.
Eine Übertragung der sicherheitsrelevanten Daten über öffentliche Netze (z. B. Internet) ist nur zulässig mit zusätzlichen Sicherheitsmaßnahmen, z. B. VPN-Tunnel und Firewall.
- Falls die Übertragung der Daten über firmen-/fabrikinterne Netze erfolgt, muss durch administrative oder technische Maßnahmen dafür Sorge getragen werden, dass ausreichender Schutz vor Manipulation gegeben ist, z. B. durch Abschottung des sicherheitsrelevanten Teiles des Netzes von anderen Netzen mit einer Firewall.
- Die Standard-Protokolle dürfen nicht für die Übertragung von sicherheitsrelevanten Daten eingesetzt werden.
- An alle Kommunikationsschnittstellen dürfen nur Geräte angeschlossen werden, die eine sichere elektrische Trennung gewährleisten.

3.4.4 Wartungseingriffe

Wartungseingriffe liegen in der Verantwortung des Betreibers. Der Betreiber hat geeignete Maßnahmen zu treffen, um den sicheren Betrieb während der Wartungseingriffe zu gewährleisten.

Erforderlichenfalls muss der Betreiber in Absprache mit der für die Applikation zuständigen Abnahmestelle administrative Maßnahmen für den Zugangsschutz zu den Systemen festlegen.

3.4.5 Cyber Security bei HIMatrix M45 Systemen

Industrielle Steuerungen müssen gegen IT-typische Problemquellen geschützt werden. Diese Problemquellen sind:

- Angreifer innerhalb und außerhalb der Kundenanlage
- Bedienungsfehler

- Software-Fehler

Eine HIMatrix M45 Installation besteht aus folgenden Teilen, die zu schützen sind:

- HIMatrix M45 PES
- PADT
- OPC-Server: X-OPC DA, X-OPC AE (optional)
- Kommunikationsverbindungen zu externen Systemen (optional)

HIMatrix M45 ist in den Grundeinstellungen bereits ein System, das Anforderungen an die Cyber Security (IT-Sicherheit) erfüllt.

Im PES und im Programmierwerkzeug sind Schutzmechanismen integriert, die versehentliche oder nicht genehmigte Veränderungen am Sicherheitssystem verhindern:

- Eine Änderung des Anwenderprogramms oder der Konfiguration führt zu einem neuen Konfigurations-CRC.
- Die Bedienmöglichkeiten sind abhängig von den Rechten des Anwenders, der am PES angemeldet ist.
- Das Programmierwerkzeug benötigt für die Verbindung zum PES beim Anmelden des Anwenders ein Passwort.
- Der Zugang zu Daten des PES ist nur möglich, wenn das PADT über das Anwenderprojekt in der aktuell laufenden Version (Archiv-Pflege!) verfügt.
- Eine Verbindung zwischen PADT und PES ist während des RUN-Betriebs nicht notwendig und kann unterbrochen werden.

Für Wartungsarbeiten oder für die Diagnose kann das PADT für kurze Zeit verbunden werden.

Die Anforderungen der Sicherheits- und Anwendungsnormen bezüglich des Schutzes vor Manipulationen sind zu beachten. Die Autorisierung von Personal und die notwendigen Schutzmaßnahmen unterliegen der Verantwortung des Betreibers.

WARNUNG



**Personenschaden durch unbefugte Manipulation an der Steuerung möglich!
Die Steuerung ist gegen unbefugte Zugriffe zu schützen!**

Z. B.:

- **die Standardeinstellungen für Login und Passwort ändern**
- **physischen Zugang zur Steuerung und zum PADT kontrollieren!**

Sorgfältige Planung sollte die zu ergreifenden Maßnahmen nennen. Nach erfolgter Risikoanalyse sind die benötigten Maßnahmen zu ergreifen. Solche Maßnahmen sind beispielsweise:

- Sinnvolle Einteilung von Benutzergruppen
- Gepflegte Netzwerkpläne helfen sicherzustellen, dass secure Netzwerke dauerhaft von öffentlichen Netzwerken getrennt sind und, falls nötig, nur ein definierter Übergang (z. B. über eine Firewall oder eine DMZ) besteht.
- Verwendung geeigneter Passwörter, die nicht leicht zu erraten sind

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

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

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

3.5 Zertifizierung

Die sicherheitsgerichteten HIMA Automatisierungsgeräte (Programmierbare Elektronische Systeme, PES) des Systems HIMatrix M45 sind nach den im folgenden aufgelisteten Normen für die funktionale Sicherheit geprüft und vom TÜV zertifiziert sowie konform zu **CE**:

Zusätzlich zu den hier aufgeführten Normen können einzelne Geräte für weitere Einsatzbereiche zertifiziert sein. Näheres in den Handbüchern der Geräte.

3.5.1 TÜV-Zertifikat/EG-Baumusterprüfung



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

Zertifikat/EG-Baumusterprüfbescheinigung Nr. 01/205/5355.00/13
Sicherheits-SPS (PES) Systemfamilie
HIMatrix M45

3.5.2 Normenspiegel

Internationale Normen:

EN / IEC 61508, Teile 1-7: 2010

SIL 3

EN / IEC 61511, Teile 1-3: 2004

SIL 3

EN ISO 13849-1: 2008 + AC: 2009

Performance level e

EN 62061: 2005 + AC:2010 + A1:2013

SIL CL 3

EN 50156-1: 2004

SIL 3

EN 12067-2: 2004

EN 298: 2012

NFPA 85: 2011

NFPA 86: 2011

EN 61131-2: 2007

EN 61326-3-1:2008

EN 54-2: 1997 + AC:1999 + A1:2006

EN 50130-4: 2011

Prüfnorm für EN 54-2

NFPA 72: 2013

EG-Richtlinien

siehe die zugehörigen Konformitätserklärungen

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

Alle Geräte tragen das **CE** - Prüfzeichen.

3.5.3 Prüfbedingungen

Die HIMatrix Systeme wurden auf Einhaltung der Anforderungen der folgenden Normen für EMV, Klima- und Umweltsanforderungen geprüft:

Norm	Inhalt
IEC/EN 61131-2: 2007	Speicherprogrammierbare Steuerungen, Teil 2 Betriebsmittelanforderungen und Prüfungen
IEC/EN 61131-6: 2012	Speicherprogrammierbare Steuerungen, Teil 6 Funktionelle Sicherheit
IEC/EN 61000-6-2: 2005	Elektromagnetische Verträglichkeit (EMV) Teil 6-2: Fachgrundnormen Störfestigkeit für Industriebereiche
IEC/EN 61000-6-4: 2007 + A1:2011	Elektromagnetische Verträglichkeit (EMV) Teil 6-4: Fachgrundnormen Störaussendung für Industriebereiche

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

3.5.3.1 Klimatische Bedingungen

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

Norm	Klimaprüfungen
IEC/EN 61131-2	Umgebungstemperatur: 0...+60 °C (Prüfgrenzen: -10...+70 °C)
	Lagertemperatur: -40...+85 °C
	Trockene Wärme und Kälte; Beständigkeitsprüfungen: +70 °C / -40 °C, 16 h, +85 °C, 1 h Stromversorgung nicht angeschlossen
	Temperaturwechsel; Beständigkeitsprüfung: Schneller Temperaturwechsel: -40 °C / +70 °C, Stromversorgung nicht angeschlossen
	Unempfindlichkeitsprüfung Langsamer Temperaturwechsel: - 10 °C / +70 °C, Stromversorgung angeschlossen
	Zyklen mit feuchter Wärme; Beständigkeitsprüfungen: +25 °C / +55 °C, 95 % relative Feuchte, Stromversorgung nicht angeschlossen
EN 54-2	Feuchte Wärme 93 % relative Feuchte, 40 °C, 4 Tage in Betrieb 93 % relative Feuchte, 40 °C, 21 Tage, Stromversorgung nicht angeschlossen

Tabelle 5: Klimatische Bedingungen

Hiervon abweichende Einsatzbedingungen sind in den Handbüchern der Kompaktsteuerungen, Remote I/Os oder Module genannt.

3.5.3.2 Mechanische Bedingungen

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

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

Tabelle 6: Mechanische Prüfungen

3.5.3.3 EMV-Bedingungen

Für speicherprogrammierbare Steuerungen in Zone C werden gemäß IEC 61131-2 die in Tabelle 7 genannten Pegel bei der Störbeeinflussung gefordert. HIMatrix Systeme erfüllen diese Anforderungen.

Prüfnormen	Prüfungen der Störfestigkeit	Kriterium
IEC/EN 61000-4-2	ESD-Prüfung: 4 kV Kontakt-, 8 kV Luftentladung	B
IEC/EN 61000-4-3	RFI-Prüfung (10 V/m): 80 MHz...1 GHz, 80 % AM RFI-Prüfung (3 V/m): 1,4 GHz...2 GHz, 80 % AM RFI-Prüfung (1 V/m): 2,0 GHz...2,7 GHz, 80 % AM	A
IEC/EN 61000-4-4	Burst-Prüfung: Versorgungsspannung: 2 kV Signalleitungen: 2 kV Geschirmte Kommunikationsleitungen: 1 kV	B
IEC/EN 61000-4-5	Stoßspannung: Versorgungsspannung: 2 kV CM, 1 kV DM Signalleitungen (AC): 2 kV CM, 1 kV DM Geschirmte Leitungen: 2 kV CM Sonstige: 1 kV CM	B
IEC/EN 61000-4-6	Hochfrequenz, asymmetrisch: 10 V, 150 kHz...80 MHz, 80 % AM 20 V, ISM-Frequenzen, 80 % AM (gemäß EN 298)	A
IEC/EN 61000-4-18	Prüfung mit gedämpften Schwingungen: 2,5 kV L-, L+ / PE 1 kV L+ / L- Signalleitungen (AC): 2,5 kV CM, 1 kV DM Geschirmte Leitungen: 0,5 kV CM Sonstige: 1 kV CM, 0,5 kV DM	B

Tabelle 7: Prüfungen der Störfestigkeit gemäß IEC 61131-2, Zone C

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

Prüfnormen	Prüfungen der Störfestigkeit	Kriterium
IEC/EN 61000-4-2	ESD-Prüfung: 6 kV Kontakt-, 8 kV Luftentladung	FS
IEC/EN 61000-4-3	RFI-Prüfung (20 V/m): 80 MHz...1 GHz, 80 % AM	FS
	RFI-Prüfung (10 V/m): 1,4 GHz...2 GHz, 80 % AM	FS
	RFI-Prüfung (3 V/m): 2,0 GHz...2,7 GHz, 80 % AM	FS
IEC/EN 61000-4-4	Burst-Prüfung:	
	Versorgungsspannung: 3 kV Signalleitungen: 2 kV	FS FS
IEC/EN 61000-4-5	Stoßspannung:	
	DC-Versorgungsspannung: 2 kV CM, 1 kV DM Signalleitungen: 2 kV CM	FS FS
IEC/EN 61000-4-6	Hochfrequenz, asymmetrisch: 10 V, 150 kHz...80 MHz, 80 % AM	FS
IEC/EN 61000-4-16	Versorgungsleitungen und Signalleitungen:	
	1...10 V, 20 dB/Dekade (1,5...15 kHz)	FS
	10 V (15...150 kHz)	FS
	10 V konstant (mit DC, 16 ² / ₃ Hz, 50/60 Hz, 150/180 Hz)	FS
	100 V kurzzeitig (1 s, mit DC, 16 ² / ₃ Hz, 50/60 Hz)	FS

Tabelle 8: Prüfungen der Störfestigkeit gemäß IEC 61326-3-1

Für sicherheitsbezogene Systeme werden erhöhte Pegel bei der Störbeeinflussung gefordert. HIMatrix Systeme erfüllen diese Anforderungen nach IEC 61326-3-2.

Prüfnormen	Prüfungen der Störfestigkeit	Kriterium
IEC/EN 61000-4-2	ESD-Prüfung: 6 kV Kontakt-, 8 kV Luftentladung	A
IEC/EN 61000-4-3	RFI-Prüfung (10 V/m): 80 MHz...1 GHz, 80 % AM	A
	RFI-Prüfung (10 V/m): 1,4 GHz...2 GHz, 80 % AM	
	RFI-Prüfung (3 V/m): 2,0 GHz...2,7 GHz, 80 % AM	
IEC/EN 61000-4-4	Burst-Prüfung:	A
	Versorgungsspannung: 2 kV Signalleitungen: 1 kV	
IEC/EN 61000-4-5	Stoßspannung:	A FS
	Versorgungsspannung: 1 kV CM, 0,5 kV DM Signalleitungen: 1 kV CM	
IEC/EN 61000-4-6	Hochfrequenz, asymmetrisch:	A
	10 V, 10 kHz...80 MHz, 80 % AM	
	20 V, ISM-Frequenzen, 80 % AM	

Tabelle 9: Prüfungen der Störfestigkeit gemäß IEC 61326-3-2

IEC/EN 61000-6-4	Prüfungen der Störaussendung
EN 55011 Klasse A, Gruppe1	Störaussendung: gestrahlt, leitungsgebunden

Tabelle 10: Prüfungen der Störaussendung

3.5.3.4 Versorgungsspannung

Die wichtigsten Prüfungen und Grenzwerte für die Versorgungsspannung der HIMatrix Systeme sind in nachstehender Tabelle aufgelistet:

IEC/EN 61131-2	Prüfung der Unempfindlichkeit gegenüber Fehlern bei der Versorgungsspannung
	Prüfung des Spannungsbereiches: 24 VDC, -20...+25 % (19,2...30,0 V)
	Prüfung auf Unempfindlichkeit gegen Kurzzeitunterbrechung der externen Stromversorgung: DC, PS 2: 2 ms
	Polaritätsumkehr der Versorgungsspannung: geprüft für 10 s

Tabelle 11: Prüfung der Unempfindlichkeit gegenüber Fehlern bei der Versorgungsspannung

4 Zentrale Funktionen

Bei einer Steuerung der Familie M45 handelt es sich um ein modulares System. Innerhalb einer Steuerung sind außer Stromversorgungsmodulen und dem Prozessormodul bis zu 62 E/A-Module einsetzbar. Darin enthalten sind bis zu drei Kommunikationsmodule.

4.1 Stromversorgung

Ein Stromversorgungsmodul M-PWR 01 ist in den Sockel des Prozessormoduls M-CPU 01 einzufügen. Bei einer Stromaufnahme von mehr als 10 A müssen weitere Stromversorgungsmodule zwischen die E/A-Module eingefügt werden. Näheres im Handbuch des Stromversorgungsmoduls HI 800 658 D.

4.2 Funktionsbeschreibung des Prozessorsystems

Das Prozessorsystem ist beim modularen System M45 in einem eigenen Modul enthalten.

Das Prozessorsystem besteht aus folgenden Funktionsblöcken:

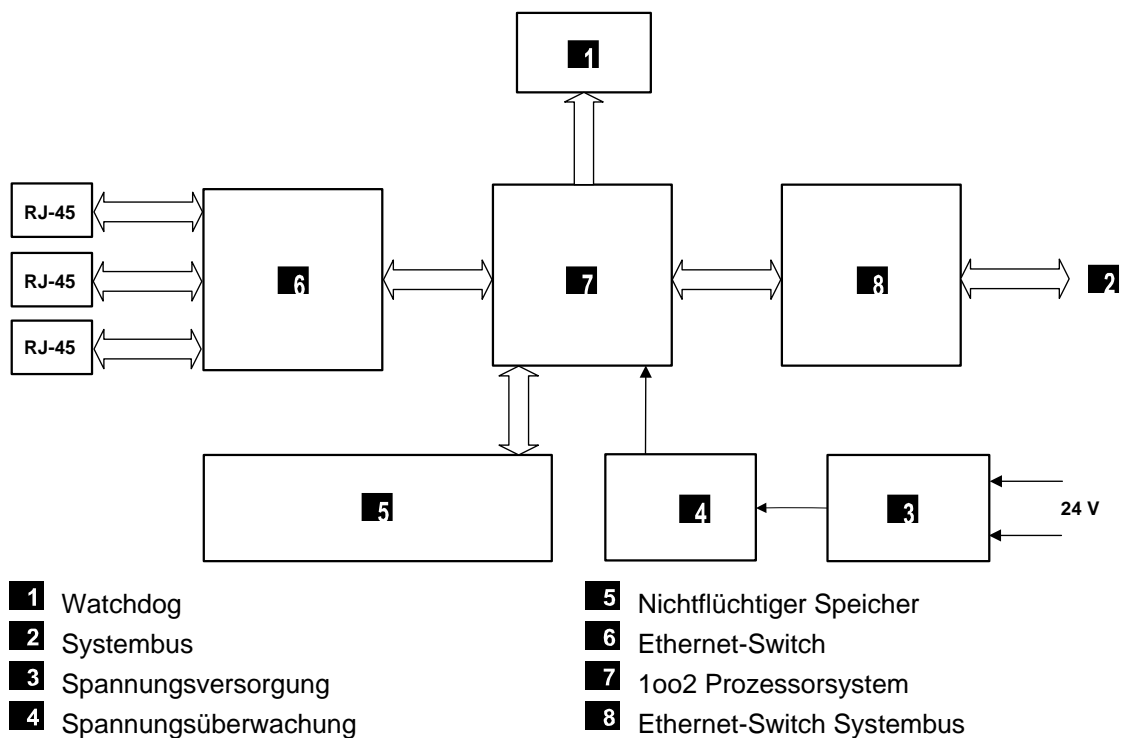


Bild 1: Darstellung der Funktionsblöcke des M-CPU 01

Eigenschaften des Prozessormoduls M-CPU 01 der M45:

- Zwei taktsynchrone Mikroprozessoren.
- Jeder Mikroprozessor hat einen eigenen RAM-Speicher.
- Testbarer Hardware-Vergleicher für alle externen Zugriffe beider Mikroprozessoren.
- Im Fehlerfall wird der Watchdog nicht mehr getriggert und geht in den sicheren Zustand.
- Flash-EPROM für Betriebssystem und Anwenderprogramm, geeignet für min. 100.000 Speicherzyklen.
- Datenspeicher für Retain-Variable in NVRAM.
- Mit Goldcap gepufferte Hardware-Uhr.
- Kommunikationsprozessor für Feldbus- und Ethernet-Interface.
- safeethernet-Schnittstellen zum Datenaustausch zwischen HIMatrix M45 Steuerungen, Remote I/Os und dem PADT.
- Signalisierung der Systemzustände durch LEDs.

- E/A-Bus-Logik zur Verbindung mit den E/A-Modulen.
- Sicherer Watchdog (WD).
- Überwachung aller Systemspannungen.

4.3 Selbst-Tests

Die Selbsttesteinrichtungen erkennen Einzelfehler, die zu einem gefährlichen Betriebszustand führen können, und lösen innerhalb der Sicherheitszeit der Steuerung definierte Fehlerreaktionen aus, welche die fehlerhaften Teile in den sicheren Zustand überführen.

Nachfolgend sind die wichtigsten Selbsttestroutinen der sicherheitsgerichteten Prozessormodule der Steuerungen stichwortartig erläutert:

4.3.1 Mikroprozessor-Test

Dieser prüft folgendes:

- 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 der Hardware-Vergleicher fehlschlägt. Der Watchdog wird geprüft.

4.3.6 Reaktionen auf Fehler im Prozessorsystem

Finden die Selbsttestroutinen einen Fehler, schaltet automatisch das Watchdog-Signal ab, und die Steuerung geht in den Fehlerstopp. Die Steuerung verarbeitet keine Eingangssignale mehr und die Ausgänge gehen in den energielosen, abgeschalteten Zustand über.

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

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

4.4 Fehlerdiagnose

Alle M45 Module verfügen jeweils über eine eigene LED zur Fehleranzeige bei Störungen des Moduls oder der externen Beschaltung. Damit ist im Störfall eine schnelle Fehlerdiagnose über ein als defekt gemeldetes Modul möglich.

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 möglich ist.

Die Logik im Anwenderprogramm kann die Fehlercodes aller Eingangs- und Ausgangssignale und der Systemvariable auswerten.

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

Details über die Auswertung der Diagnosemeldung siehe auch Systemhandbuch M45, HI 800 650 D, Kapitel *Diagnose*.

5 Eingänge

Übersicht über die Eingänge des HIMatrix M45 Systems:

Modul	Typ	Anzahl Eingänge	sicherheits-gerichtet	rückwirkungs-frei	Galvanisch getrennt
M-DI 8 01 (Line Control konfigurierbar)	Digital	8	•	•	-
M-CI 8 01	Zähler	8	•	•	-

Tabelle 12: Übersicht über die Eingänge des HIMatrix M45 Systems

5.1 Allgemeines

Es ist möglich, sicherheitsgerichtete Eingänge sowohl für sicherheitsgerichtete als auch für nicht sicherheitsgerichtete Signale zu benutzen.

Die Steuerungen liefern Status- und Fehlerinformation auf folgende Weisen:

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

Sicherheitsgerichtete Eingangsmodule führen während des Betriebes automatisch einen hochwertigen, zyklischen Selbsttest durch.

5.2 Sicherheit von Sensoren, Encodern und Transmittern

In einer sicherheitsgerichteten Anwendung müssen sowohl die Steuerung 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 zum Beispiel in IEC 61511-1, Abschnitt 11.4.

5.3 Reaktion im Fehlerfall

Wenn die Testroutinen einen Fehler feststellen, aktiviert ein M45 Modul die LED *Err*.

Bei Eingängen verarbeitet das Anwenderprogramm den Initialwert der globalen Variablen.

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

5.4 Sicherheitsgerichtete digitale Eingänge

Die beschriebenen Eigenschaften gelten für die digitalen Eingangskanäle der M45-Module.

5.4.1 Allgemeines

Die digitalen Eingänge werden einmal in jedem Zyklus gelesen und der Wert intern gespeichert. Sie werden zyklisch auf sichere Funktion getestet.

Eingangssignale, die kürzer als die Zeit zwischen zwei Abtastungen (also kürzer als für eine Zykluszeit) anstehen, werden unter Umständen nicht erfasst.

5.4.2 Test-Routinen

Die Online-Testroutinen prüfen, ob die Eingangskanäle in der Lage sind, unabhängig von den anstehenden Eingangssignalen beide Signalpegel (LOW und HIGH) durchzuschalten. Dieser Funktionstest wird bei 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:

1. Installation abgeschirmter Eingangsleitungen
2. Störaustastung im Anwenderprogramm programmieren. Ein Signal muss mindestens zwei Zyklen anstehen, bevor es ausgewertet wird. Die Fehlerreaktion erfolgt entsprechend verzögert.

i

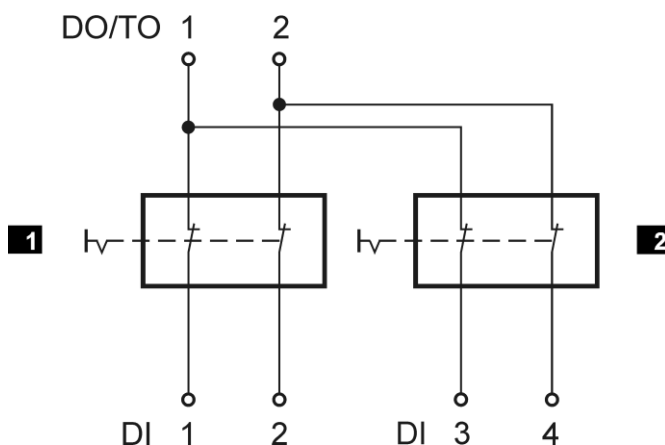
Auf obige Maßnahmen kann verzichtet werden, wenn durch die Auslegung der Anlage Surges im System ausgeschlossen werden können.

Zur Auslegung gehören insbesondere Schutzmaßnahmen betreffend Überspannung, Blitzschlag, Erdung und Anlagenverdrahtung auf Basis der Angaben im Systemhandbuch HI 800 650 D und der relevanten Normen.

5.4.4 Line Control

Line Control ist eine Erkennung von Leitungsschluss, Leitungsbruch und Querschluss zum Beispiel von NOT-AUS-Geräten, die bei HIMatrix M45 Systemen mit digitalen Eingängen konfiguriert werden kann.

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

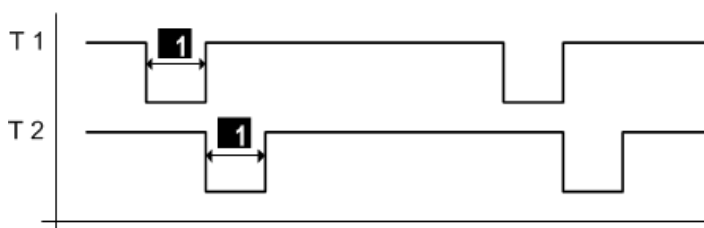


- 1** NOT-AUS 1
2 NOT-AUS 2

NOT-AUS-Geräte 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 Variablen für die Taktausgaben müssen bei Kanal 1 beginnen und direkt nacheinander liegen, siehe Systemvariable in den Handbüchern.



- 1** Konfigurierbar 5...2 000 µs

Bild 3: Taktsignale T1, T2

Line Control kann folgende Fehler feststellen:

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

Tritt ein solcher Fehler auf, erfolgen folgende Reaktionen:

- Die Leuchtdiode *Err* auf der Frontplatte des Moduls blinkt. Bei Leitungsbruch oder Öffnen der Kontakte blinkt die LED nicht.
- Die Eingänge werden auf Low-Pegel gesetzt.
- Ein auswertbarer Fehlercode wird erzeugt.

Das Modul kann die Taktausgänge takten und zusammen mit sicherheitsgerichteten digitalen Eingängen desselben Moduls für eine Leitungsschluss- und Leitungsbruchererkennung verwenden.

i

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

5.5 Sicherheitsgerichtetes Zählermodul

Das Zählermodul entspricht SIL 1.

Für SIL 3-Anwendungen sind redundante Sensoren zu verwenden und entsprechend dem Handbuch für M-CI 8 01 (HI 800 666 D) zu verschalten.

Ein Zählerkanal ist für den Betrieb als Vorwärtszähler mit 24-Bit Auflösung parametrierbar.

Ein Kanalpaar ist notwendig für den Betrieb als Quadraturzähler.

5.6 Checkliste für sicherheitsgerichtete Eingänge

Diese Checkliste ist eine Empfehlung zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsgerichteten Eingängen. Sie ist als Planungsunterlage einsetzbar, dient aber gleichzeitig auch als Nachweis für eine sorgfältig durchgeführte Planung.

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

Die Checkliste *HIMatrix_M45_Checkliste_Eingänge.docx* steht als Dokument im Format von Microsoft® Word® zur Verfügung. Die ZIP-Datei *HIMatrix_M45_Checklisten.zip* enthält alle Checklisten und kann von der HIMA Webseite www.hima.de heruntergeladen werden.

6 Ausgänge

Übersicht über die Ausgänge des HIMatrix M45 Systems

Modul	Typ	Anzahl Ausgänge	sicherheitsgerichtet	Galvanisch getrennt
M-DO 2 01	Relais	2	•	•
M-DO 8 01	Digital	8	•	-
M-DI 8 01	Digital	2	-	-

Tabelle 13: Übersicht über die Ausgänge des HIMatrix M45 Systems

6.1 Allgemeines

Die Steuerung beschreibt die sicherheitsgerichteten 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 sicherheitsgerichteten Ausgangskanälen sind zwei testbare Schalter in Serie integriert. Somit ist der sicherheitstechnisch erforderliche, unabhängige zweite Abschaltweg auf dem Ausgangskanal 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.

Im Anwenderprogramm kann der Status der Systemvariablen des jeweiligen Moduls ausgewertet werden.

6.2 Sicherheit von Aktoren

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

6.3 Reaktion im Fehlerfall

Wenn die Testroutinen einen Fehler feststellen, aktiviert ein M45 Modul die LED *Err*.

Bei Ausgängen 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.

6.4 Sicherheitsgerichtete digitale Ausgänge

Die aufgeführten Punkte gelten für die digitalen Ausgangskanäle der Module der M45 mit Ausnahme der Relaisausgänge.

6.4.1 Testroutinen für digitale Ausgänge

Die Module testen sich automatisch während des Betriebes. Die wesentlichen Testfunktionen sind:

- Rücklesen des Ausgangssignals
- Prüfen der integrierten zweifachen Sicherheitsabschaltung.
- Abschalttest der Ausgänge

- Überwachung der Versorgungsspannung

6.4.2 Verhalten bei externem Kurzschluss oder Überlast

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

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.

6.5 Relaisausgänge

Die Relaisausgänge verwenden Relais mit zwangsgeführten Kontakten.

6.5.1 Testroutinen für Relaisausgänge

Das Modul testet seine Ausgänge automatisch während des Betriebs. Die wesentlichen Testfunktionen sind:

- Rücklesen der Ausgangssignale der Schaltverstärker vor den Relais.
- Prüfen der integrierten zweifachen Sicherheitsabschaltung.
- Überwachung der Versorgungsspannung

6.6 Checkliste für sicherheitsgerichtete Ausgänge

Diese Checkliste ist eine Empfehlung zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsgerichteten Ausgängen. Sie ist als Planungsunterlage einsetzbar, dient aber gleichzeitig auch als Nachweis für eine sorgfältig durchgeführte Planung.

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

Die Checkliste *HIMatrix_M45_Checkliste_Ausgänge.docx* steht als Dokument im Format von Microsoft® Word® zur Verfügung. Die ZIP-Datei *HIMatrix_Checklisten.zip* enthält alle Checklisten und kann von der HIMA Webseite www.hima.de heruntergeladen werden.

7 Software für HIMatrix M45 Systeme

Die Software für die sicherheitsgerichteten Automatisierungsgeräte der HIMatrix M45 Systeme gliedert sich in die folgenden Teile:

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

Das Betriebssystem wird in den Zentralteil (CPU) der Steuerung geladen und ist in der jeweils gültigen, vom TÜV zertifizierten Form für sicherheitsgerichtete Anwendungen einzusetzen.

Das Programmierwerkzeug dient zur Erstellung des Anwenderprogramms, das die anlagenspezifischen Funktionen enthält, die das Automatisierungsgerät ausführen soll. Die Parametrierung und Bedienung für Betriebssystemfunktionen erfolgt ebenfalls über das Programmierwerkzeug.

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

7.1 Sicherheitstechnische Aspekte für das Betriebssystem

Jedes zugelassene Betriebssystem ist durch seine Bezeichnung gekennzeichnet. Zur besseren Unterscheidung sind die Revision und die CRC-Signatur angegeben. Die jeweils gültigen, vom TÜV für sicherheitsgerichtete Automatisierungsgeräte zugelassenen Versionen des Betriebssystems und die dazugehörigen Signaturen (CRCs) unterliegen der Revisionskontrolle und werden auf einer Liste dokumentiert, die HIMA gemeinsam mit dem TÜV erstellt.

Ein Auslesen der laufenden Betriebssystemversion ist nur mit dem Programmierwerkzeug möglich. Eine Kontrolle der Betriebssystemversion durch den Anwender ist erforderlich, damit der sicherheitsgerichtete Betrieb mit der für die Anlage zugelassenen Version erfolgt. (vgl. 7.5, Checkliste zur Erstellung eines Anwenderprogramms).

7.2 Arbeitsweise und Funktionen des Betriebssystems

Das Betriebssystem arbeitet das Anwenderprogramm zyklisch ab. Dabei führt es folgende Funktionen aus:

- Lesen der Eingangsdaten von physikalischen Eingängen und Kommunikationspartnern
- Verarbeiten der Logikfunktionen, die gemäß IEC 61131-3 programmiert worden sind
- Schreiben der Ausgangsdaten auf physikalische Ausgänge und Kommunikationspartner

Hinzu kommen folgende wesentlichen Funktionen:

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

7.3 Sicherheitstechnische Aspekte für die Programmierung

7.3.1 Sicherheitskonzept des Programmierwerkzeugs

Das Sicherheitskonzept des Programmierwerkzeugs SILworX:

- Bei der Installation des Programmierwerkzeugs sichert eine CRC-Prüfsumme die Integrität des Programmpakets auf dem Weg vom Hersteller zum Anwender.
- Das Programmierwerkzeug führt Plausibilitätsprüfungen durch, um Fehler bei der Eingabe zu verringern.
- Das Programmierwerkzeug und die Anwendung der in diesem Sicherheitshandbuch definierten Maßnahmen machen es hinreichend unwahrscheinlich, dass ein semantisch und syntaktisch korrekter Code erzeugt wird, der noch unerkannte systematische Fehler aus dem Prozess der Code-Erzeugung enthält.

i

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

Bei der ersten Inbetriebnahme einer sicherheitsgerichteten Steuerung ist die Sicherheit der gesamten Anlage durch einen vollständigen Funktionstest zu prüfen:

- Überprüfung der korrekten Umsetzung der Steuerungsaufgabe anhand der Daten und Signalflüsse.
- Vollständige Funktionsprüfung der Logik durch Erprobung (siehe Kapitel 7.3.2).

Der sichere Revisionsvergleich von SILworX kann die Änderungen gegenüber der Vorversion ermitteln und anzeigen.

Nach einer Änderung des Anwenderprogramms sind nur diejenigen Programmteile zu testen, die von der Änderung betroffen sind.

7.3.2 Überprüfung der Konfiguration und des Anwenderprogramms

Um das erstellte Anwenderprogramm auf Einhaltung der spezifischen Sicherheitsfunktion zu überprüfen, sind geeignete Testfälle zu erzeugen, welche die Spezifikation abdecken.

In der Regel ist der unabhängige Test jedes Loops (bestehend aus Eingang, den aus Anwendungssicht wichtigen Verknüpfungen, und Ausgang) ausreichend.

Auch für die numerische Auswertung von Formeln sind geeignete Testfälle zu generieren. Sinnvoll sind Äquivalenzklassentests, das sind Tests innerhalb definierter Wertebereiche, an den Grenzen oder in unzulässigen Wertebereichen. Die Testfälle sind so zu wählen, dass die Korrektheit der Programmlogik nachgewiesen wird. Die notwendige Anzahl der Testfälle hängt von der verwendeten Programmlogik ab und muss kritische Wertepaare umfassen.

Nur eine aktive Simulation mit Quellen kann eine korrekte Verdrahtung der Sensoren und Aktoren des Systems (auch über Kommunikation mit Remote I/Os angeschlossene) nachweisen. Außerdem ist auch nur so die Systemkonfiguration überprüfbar.

SILworX ist als Prüfhilfsmittel verwendbar:

- 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 Laden des Programms in die Steuerung das Projekt zu archivieren. Dies gilt für Download wie für Reload.

SILworX legt ein Projekt in einer Projektdatei an. Diese ist geeignet, z. B. auf einem externen Speichermedium, zu sichern.

7.3.4 Möglichkeit zur Programm- und Konfigurations-Identifizierung

Die Anwenderprogramme werden eindeutig an den Konfigurations-CRCs des Projekts identifiziert. Dieser lässt sich mit dem Konfigurations-CRC des geladenen Projekts vergleichen.

Um sicherzustellen, dass die gesicherte Projektdatei unverändert ist, die enthaltene Ressource kompilieren und den Konfigurations-CRC mit dem CRC der geladenen Konfiguration vergleichen. Dieser kann mit SILworX angezeigt werden.

7.4 Parameter der Ressource

WARNUNG



Personenschaden durch fehlerhafte Konfiguration möglich!

Weder das Programmiersystem noch die Steuerung können projektspezifisch festgelegte Parameter überprüfen. Deshalb unbedingt diese Parameter korrekt ins Programmiersystem eintragen und den erfolgten Eintrag überprüfen.

Diese Parameter sind die Rack-ID, siehe Systemhandbuch HI 800 650 D und die in der Tabelle 14 hervorgehobenen Parameter.

Die nachfolgend angeführten Parameter werden im Programmierwerkzeug für die zulässigen Aktionen im sicherheitsgerichteten Betrieb des Automatisierungsgeräts festgelegt und als sicherheitsgerichtete Parameter bezeichnet.

Die während des sicherheitsgerichteten 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

Es gibt eine Aufteilung in Systemparameter der Ressource und Systemparameter der Hardware.

7.4.1.1 Systemparameter der Ressource

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

Systemparameter	S ¹⁾	Beschreibung	Einstellung für sicheren Betrieb
Name		Name der Ressource	Beliebig
System ID [SRS]	X	System-ID der Ressource 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]		Sicherheitszeit in Millisekunden (20...22 500 ms, Standardwert: 600 ms) Für HiMatrix M45 Steuerungen nicht anwendbar!	-
Watchdog-Zeit [ms]	X	Watchdog-Zeit in Millisekunden: 4...5000 ms, Standardwert: 200 ms (online änderbar)	applikations-spezifisch

Sollzykluszeit [ms]		Gewünschte oder maximale Zykluszeit, siehe <i>Sollzykluszeit-Modus</i> , 0...7500 ms, Standardwert: 0 ms. Die Sollzykluszeit darf höchstens so groß sein wie die <i>Watchdog-Zeit [ms]</i> abzüglich des kleinsten einstellbaren Werts der <i>Watchdog-Zeit [ms]</i> (4 ms, s. o.), andernfalls lehnt das PES sie ab. Ist der Standardwert 0 ms eingestellt, so wird die Sollzykluszeit nicht beachtet. Siehe Kapitel 7.4.1.2. (online änderbar)	applikations-spezifisch
Sollzykluszeit-Modus		Verwendung der <i>Sollzykluszeit [ms]</i> (online änderbar) siehe Kapitel 7.4.1.2. Standardwert: fest-tolerant	applikations-spezifisch
Multitasking Modus		Mode 1 Die Länge eines Zyklus der CPU richtet sich nach der benötigten Ausführungsdauer aller Anwenderprogramme.	applikations-spezifisch
		Mode 2 Prozessor stellt von Anwenderprogrammen niedriger Priorität nicht benötigte Ausführungszeit den Anwenderprogrammen hoher Priorität zur Verfügung. Betriebsart für hohe Verfügbarkeit.	
		Mode 3 Prozessor wartet nicht benötigte Ausführungszeit von Anwenderprogrammen ab und verlängert so den Zyklus.	
		Standardwert: Mode 1	
Max. Kom. Zeitscheibe ASYNC [ms]		Höchstwert in ms der Zeitscheibe, die innerhalb des Zyklus der Resource für Kommunikation verwendet wird, siehe Kommunikationshandbuch HI 801 100 D, 2...5000 ms, Standardwert: 60 ms. Siehe Kapitel 7.4.1.3.	applikations-spezifisch
Max. Dauer Konfigurationsverbindungen [ms]		Definiert, wie viel Zeit innerhalb eines CPU-Zyklus für die Konfigurationsverbindungen zur Verfügung steht, 2...3500 ms, Standardwert: 12 ms	applikations-spezifisch
Maximale Systembus-Latenzzeit [µs]		Für HiMatrix M45 Steuerungen nicht anwendbar! (Standardwert: 0 µs)	-
Online-Einstellungen erlauben	X	ON: Alle unter OFF genannten Schalter/Parameter sind online mit dem PADT änderbar. Dies gilt nur, wenn die Systemvariable <i>Read-only in RUN</i> den Wert OFF hat.	OFF empfohlen
		OFF: Diese Parameter sind nicht online änderbar: <ul style="list-style-type: none"> ▪ <i>System-ID</i> ▪ <i>Autostart</i> ▪ <i>Globales Forcen erlaubt</i> ▪ <i>Globale Force-Timeout-Reaktion</i> ▪ <i>Laden erlaubt</i> ▪ <i>Reload erlaubt</i> ▪ <i>Start erlaubt</i> 	
		Diese Parameter sind online änderbar, wenn <i>Reload erlaubt</i> ON ist: <ul style="list-style-type: none"> ▪ <i>Watchdog-Zeit</i> (der Resource) ▪ <i>Sicherheitszeit</i> ▪ <i>Sollzykluszeit</i> ▪ <i>Sollzykluszeit-Modus</i> Sie sind nicht online änderbar, wenn <i>Reload erlaubt</i> OFF ist.	
		 Bei gestopptem PES und durch Reload ist es möglich, <i>Online-Einstellungen erlauben</i> auf ON zu setzen. Standardwert: ON	
Autostart	X	ON: Wird das Prozessormodul an die Versorgungsspannung angeschlossen, startet das Anwenderprogramm/die Anwenderprogramme automatisch	applikations-spezifisch
		OFF: kein automatischer Start nach Zuschalten der Versorgungsspannung.	
		Standardwert: OFF	
Start erlaubt	X	ON: Kaltstart oder Warmstart durch PADT im Zustand RUN oder STOPP erlaubt.	applikations-spezifisch
		OFF: Kein Start erlaubt	
		Standardwert: ON	

Systemparameter	S ¹⁾	Beschreibung	Einstellung für sicheren Betrieb
Laden erlaubt	X	ON: Download der Konfiguration erlaubt.	applikations-spezifisch
		OFF: Download der Konfiguration nicht erlaubt	
		Standardwert: ON	
Reload erlaubt	X	ON: Reload der Konfiguration erlaubt.	applikations-spezifisch
		OFF: Reload der Konfiguration nicht erlaubt. Ein laufender Reload-Prozess wird beim Umschalten auf OFF nicht abgebrochen	
		Standardwert: ON	
Globales Forcen erlaubt	X	ON: Globales Forcen für diese Ressource erlaubt.	applikations-spezifisch
		OFF: Globales Forcen für diese Ressource nicht erlaubt	
		Standardwert: ON	
Globale Force-Timeout-Reaktion		Legt fest, wie sich die Ressource beim Ablauf des globalen Force-Timeout verhält: <ul style="list-style-type: none"> Forcen beenden Ressource stoppen Standardwert: Forcen beenden	applikations-spezifisch
Minimale Konfigurationsversion		Mit dieser Einstellung ist es möglich, Code zu generieren, der entsprechend den Projektanforderungen zu alten oder zu neuen Versionen des CPU-Betriebssystems kompatibel ist. Siehe Kapitel 7.4.1.4. Standardwert: SiLworX V7	SiLworX-V7
		SiLworX V2 Für HiMatrix M45 Steuerungen nicht anwendbar!	
		SiLworX V3	
		SiLworX V4	
		SiLworX V5	
		SiLworX V6 Einstellung für HiMatrix M45. Generiert Code passend zum CPU-Betriebssystem V10.	
		SiLworX V6b Einstellung für HiMatrix M45. Generiert Code passend zum CPU-Betriebssystem V10.	
		SiLworX V7 Einstellung für HiMatrix M45. Generiert Code passend zum CPU-Betriebssystem V11.	
Schnelles Hochfahren		Die Ressource fährt bei Zuschalten der Versorgungsspannung schneller hoch. Siehe Kapitel 7.4.1.5. Standardwert: OFF	applikations-spezifisch

Tabelle 14: Die Systemparameter der Ressource

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

Diese Parameter sind dazu verwendbar, die Zykluszeit möglichst konstant auf dem Wert von *Sollzykluszeit [ms]* zu halten. Dazu muss dieser Parameter auf einen Wert > 0 eingestellt sein. In diesem Fall begrenzt HiMatrix M45 die Aktivität Reload soweit, dass die Sollzykluszeit eingehalten wird.

Die folgende Tabelle beschreibt die Wirkung des *Sollzykluszeit-Modus*.

Sollzykluszeit-Modus	Wirkung auf Anwenderprogramme	Wirkung auf Reload von Prozessormodulen
fest	Das PES hält die Sollzykluszeit ein und verlängert den Zyklus, falls nötig. Falls die Abarbeitungszeit der Anwenderprogramme die Sollzykluszeit überschreitet, wird der Zyklus verlängert.	Reload wird nur durchgeführt, falls die Sollzykluszeit ausreicht.
fest-tolerant		Höchstens jeder fünfte Zyklus wird verlängert, um Reload durchzuführen.
dynamisch-tolerant	HIMatrix führt den Zyklus in möglichst kurzer Zeit aus.	Höchstens jeder fünfte Zyklus wird verlängert, um Reload durchzuführen.
dynamisch		Reload wird nur durchgeführt, falls die Sollzykluszeit ausreicht.

Tabelle 15: Wirkung des Sollzykluszeit-Modus

7.4.1.3 Berechnung der *Maximalen Dauer der Konfigurationsverbindungen* [μ s]

Wird die Kommunikationsverarbeitung in einem CPU-Zyklus nicht fertig, wird sie im nächsten, unmittelbar folgenden CPU-Zyklus an der Unterbrechungsstelle fortgesetzt.

Die Kommunikation wird dadurch zwar verzögert, jedoch werden alle Verbindungen mit externen Partnern gleichberechtigt und vollständig verarbeitet.

Passende Einstellung: den Wert so wählen, dass in der verbleibenden Zeit *Watchdog-Zeit - Max. Dauer Konfigurationsverbindungen* die zyklischen Aufgaben des Prozessors noch ausführbar sind.

Die Menge der zu kommunizierenden Konfigurationsdaten ist abhängig von der Anzahl der konfigurierten Remote-IOs, der bestehenden Verbindungen zu PADTs und der Module im System, die eine Ethernet-Schnittstelle besitzen.

Eine erste Einstellung lässt sich wie folgt berechnen:

$$T_{\text{Konfig}} = (n_{\text{Kom}} + n_{\text{RIO}} + n_{\text{PADT}}) \cdot 0,25 \text{ ms} + 2 \text{ ms}, \text{ wobei}$$

T_{Konfig}	Systemparameter <i>Max. Dauer Konfigurationsverbindungen</i> [ms]
n_{Kom}	Anzahl Module mit Ethernet-Schnittstellen {CPU, COM}
n_{RIO}	Anzahl konfigurierter Remote IOs
n_{PADT}	max. Anzahl PADT-Verbindungen = 5

Es ist möglich, die berechnete Zeit später anhand der Online-Statistik nachträglich entweder in den Eigenschaften der Ressource zu korrigieren, oder direkt online zu verändern.

Bei der Codegenerierung und bei der Projektkonvertierung wird auf dem PADT ein Hinweis ausgegeben, wenn die eingestellte *Max. Dauer Konfigurationsverbindungen* kleiner ist, als nach obiger Formel errechnet.

i

Wurde die *Max. Dauer Konfigurationsverbindungen* zu klein eingestellt, arbeitet die Kommunikation zwischen PADT und PES sehr langsam bis hin zum völligen Ausfall!

7.4.1.4 Hinweise zum Parameter *Minimale Konfigurationsversion*

- Bei einem neu angelegten Projekt wird jeweils die neueste *Minimale Konfigurationsversion* ausgewählt. Ob diese Einstellung zur verwendeten Hardware passt, ist zu prüfen. HIMatrix M45 Geräte benötigen den Wert *SILworX V6* oder höher für die *Minimale Konfigurationsversion*.
- Bei einem Projekt, das von einer früheren SILworX Version konvertiert wurde, bleibt der in der Vorversion eingestellte Wert für die *Minimale Konfigurationsversion* erhalten. Dadurch ist gewährleistet, dass die Codegenerierung denselben Konfigurations-CRC erzeugt wie in der Vorversion, und die generierte Konfiguration kompatibel zum Betriebssystem in der Hardware bleibt.

Bei konvertierten Projekten sollte deshalb die *Minimale Konfigurationsversion* nur im Zusammenhang mit anderen Änderungen an der betroffenen Ressource verändert werden.

- SILworX erzeugt automatisch eine höhere Konfigurationsversion als die eingestellte *Minimale Konfigurationsversion*, wenn im Projekt Fähigkeiten benutzt werden, die nur eine höhere Konfigurationsversion zur Verfügung stellt. Dies zeigt SILworX im Ergebnis der Codegenerierung an. Die Hardware lehnt das Laden einer höheren Konfigurationsversion als zu ihrem Betriebssystem passend ab.

Für die Beseitigung von solchen Inkompatibilitäten kann es nützlich sein, den vom Versionsvergleich gelieferten Informationen die Moduldaten-Übersicht gegenüber zu stellen.

7.4.1.5 Hinweis zum Parameter *Schnelles Hochfahren*

Dieser Parameter existiert ab SILworX V7 und erfordert eine M45 Ressource mit einem CPU-Betriebssystem ab V11. Außerdem muss die Ressource mit einem Boot-Loader ab V11.2/V16.8 ausgestattet sein. Der Boot-Loader unterscheidet sich vom OS-Loader (Notfall-Lader) und ist nicht durch den Anwender austauschbar.

Das schnelle Hochfahren ist nur beim Zuschalten der Versorgungsspannung des PES wirksam. Ein Betrieb mit SIL 3 bleibt gewährleistet.

Schnelles Hochfahren wird erreicht durch:

- verkürzten Selbsttest
- 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 Hochfahren gewünscht, ist der Parameter *Schnelles Hochfahren* auf OFF zu setzen!

7.4.1.6 Systemvariable der Hardware

Diese Variablen 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.

Parameter	Funktion	Standard-Einstellung	Einstellung für sicheren Betrieb
Force-Deaktivierung	Verhindert den Start des Forcens und beendet laufendes Forcen unmittelbar	FALSE	applikationsspezifisch
Leer 0 ... Leer 16	Keine Funktion	-	-
Notaus 1...Notaus 4	Notausschalter zum Abschalten der Steuerung in vom Anwenderprogramm erkannten Störfällen	FALSE	applikationsspezifisch
Relaiskontakt 1... Relaiskontakt 4	Nicht anwendbar bei M45!	FALSE	applikationsspezifisch
Read-only in Run	Nach dem Starten der Steuerung ist keine Bedienaktion (Stopp, Online-Ändern) über SILworX mehr möglich, Ausnahmen: Forcen und Reload	FALSE	applikationsspezifisch
Reload-Deaktivierung	Verhindert ein Laden der Steuerung mittels Reload.	FALSE	applikationsspezifisch
Stromsparmodus	Schaltet die Ausgänge in den Stromsparmodus, d. h. auf OFF	FALSE	applikationsspezifisch
User LED 1...User LED 2	Steuert die entsprechende LED auf der Frontplatte des Prozessormoduls an.	FALSE	-

Tabelle 16: Systemvariable der Hardware

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

Beispiel: An einen digitalen Eingang ist ein Schlüsselschalter angeschlossen. Der digitale Eingang ist einer globalen Variablen zugewiesen, die der Systemvariablen *Read only in Run* zugewiesen ist. Dann kann der Besitzer eines Schlüssels mit dem Schlüsselschalter die Bedienaktionen Stopp, Start, und Download zulassen oder sperren.

7.5 **Checkliste zur Erstellung eines Anwenderprogramms**

Diese Checkliste ist eine Empfehlung für den Anwender zur Einhaltung sicherheitstechnischer Aspekte bei der Programmierung, vor und nach dem Laden des neuen oder geänderten Programms.

Die Checkliste *HIMatrix_M45_Checkliste_Programm.docx* steht als Dokument im Format von Microsoft Word© zur Verfügung. Die ZIP-Datei *HIMatrix_M45_Checklisten.zip* enthält alle Checklisten und kann von der HIMA Webseite www.hima.de heruntergeladen werden.

8 Sicherheitstechnische Aspekte für das Anwenderprogramm

Allgemeiner Ablauf der Programmierung des HIMatrix M45 Automatisierungssystems für sicherheitstechnische Anwendungen:

- Spezifikation der Steuerungsfunktion.
- Schreiben des Anwenderprogramms.
- Kompilieren des Anwenderprogramms mit dem C-Code-Generator.
- Das Programm ist fehlerfrei erzeugt und lauffähig.
- Verifikation und Validation.

Anschließend kann das PES den sicherheitsgerichteten Betrieb aufnehmen.

8.1 Rahmen für den sicherheitsgerichteten Einsatz

(Vorgaben und Regeln, Erläuterungen zu den Sicherheitsauflagen Kapitel 3.4)

Das Anwenderprogramm mit dem zulässigen Programmierwerkzeug SILworX eingeben.

Die freigegebenen Betriebssysteme für Personalcomputer sind den Freigabemitteilungen des Programmierwerkzeugs zu entnehmen.

Das Programmierwerkzeug enthält im Wesentlichen:

- Eingabe (Funktionsbaustein-Editor, Structured-Text-Editor), Überwachung und Dokumentation.
- Variablen mit symbolischen Namen und Datentyp (BOOL, UINT usw.).
- Zuordnung der Steuerungen des Systems HIMatrix M45.
- Codegenerator (Übersetzen des Anwenderprogramms in den Maschinencode).
- Hardware-Konfiguration.
- Konfiguration der Kommunikation.

8.1.1 Basis der Programmierung

Die Steuerungsaufgabe soll in Form einer Spezifikation oder eines Pflichtenheftes vorliegen. Diese Dokumentation ist die Basis der Überprüfung der korrekten Umsetzung in das Anwenderprogramm. Die Art der Darstellung der Spezifikation richtet sich nach der Aufgabenstellung. Dies kann sein:

- 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 Fortschaltbedingungen und der zu steuernden Aktoren.
 - Ablaufpläne.
 - Matrix- oder Tabellenform der Fortschaltbedingungen und der zu steuernden Aktoren.
 - Definition der Randbedingungen, z. B. Betriebsarten, NOT-AUS usw.

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

- Sensoren (digital oder analog).
 - Signal im Normalbetrieb (Ruhestromprinzip bei digitalen Sensoren, life-zero bei analogen Sensoren).
 - Signal im Fehlerfall.
 - Festlegung von sicherheitstechnisch erforderlichen Redundanzen (1oo2, 2oo3).

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

Ziele bei der Programmierung des Anwenderprogramms:

- leicht zu verstehen.
- leicht nachzuvollziehen.
- leicht zu ändern.
- leicht zu testen.

8.1.2 Funktionen des Anwenderprogramms

Die Programmierung unterliegt keiner Einschränkung durch die Hardware. Die Funktionen des Anwenderprogramms 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. Dies ist bei der Programmierung zu berücksichtigen.
- Das Anwenderprogramm kann aus logischen und/oder arithmetischen Funktionen ohne Rücksicht auf das Ruhestromprinzip der physikalischen Eingänge und Ausgänge erstellt sein.
- Die Logik soll übersichtlich konzipiert sein und verständlich dokumentiert für leichte Fehlersuche. Das schließt die Verwendung von Funktionsdiagrammen ein.
- Beliebige Negierungen sind zulässig.
- Fehlersignale von Eingängen und Ausgängen oder aus Logik-Bausteinen sind auszuwerten.

Wichtig ist die Kapselung von Funktionen in selbst erstellten Funktionsbausteinen und Funktionen aus Standardfunktionen. Dadurch kann ein Programm in Module (Funktionen, Funktionsbausteine) klar strukturiert werden. Jedes Modul kann für sich einzeln betrachtet werden, und durch das Zusammenschalten der Module zu einem größeren Modul oder zu einem Programm ergibt sich eine fertige, komplexe Funktion.

8.1.3 Variablendeklaration

Eine Variable ist ein Platzhalter für einen Wert innerhalb der Programmlogik. Über den Variablennamen wird der Speicherplatz mit dem gespeicherten Wert symbolisch adressiert. Eine Variable wird in einer Variablendeklaration im Projekt erstellt. Der Name einer Variablen kann bis zu 120 Zeichen umfassen.

Variable ohne benutzerdefinierten Initialwert haben nach einem Kaltstart den Standard-Initialwert 0 bzw. FALSE.

Variable, deren Quelle ungültig ist, z. B. durch Hardware-Fehler bei physikalischem Eingang, nehmen den konfigurierten Initialwert an.

8.1.4 Dokumentation der anwenderspezifischen LEDs

Das Prozessormodul M-CPU 01 enthält die anwenderspezifisch einsetzbaren Leuchtdioden *User 1* und *User 2*. Für diese LEDs ist unbedingt eine Bedienerbeschreibung zu erstellen, die die HIMA-Dokumentation projektspezifisch ergänzt.

8.2 Vorgehensweisen

Dieses Kapitel beschreibt typische Vorgehensweisen bei der Entwicklung von Anwenderprogrammen für sicherheitsgerichtete HIMatrix M45 Steuerungen.

8.2.1 Zuordnung von Variablen zu Ein-/Ausgängen

Die erforderlichen Testroutinen für sicherheitsgerichtete E/A-Module oder E/A-Kanäle werden vom Betriebssystem automatisch ausgeführt.

Variable einem E/A-Kanal zuweisen

1. Eine globale Variable mit geeignetem Typ definieren.
 2. Bei der Definition einen geeigneten Initialwert angeben.
 3. Die globale Variable dem Kanalwert des E/A-Kanals zuweisen.
 4. Im Anwenderprogramm den Fehlercode -> *Fehlercode [Byte]* auswerten und eine sicherheitsgerichtete Reaktion programmieren.
- Die globale Variable ist einem Ein-/Ausgangskanal zugewiesen.

8.2.2 Ab- und Aufschließen der Steuerung

Abschließen der Steuerung bedeutet das Verriegeln von Funktionen und Eingriffsmöglichkeiten des Anwenders während des Betriebs. Eine Manipulation des Anwenderprogramms wird damit verhindert. Der Umfang der Verriegelungen ist in Abhängigkeit zur Sicherheitsanforderung an den Einsatz des PES zu sehen, kann aber auch in Absprache mit der für die Anlagenabnahme zuständigen Prüfstelle erfolgen.

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

Zum Verriegeln dienen drei Systemvariable:

Variable	Funktion
Read only in run	ON: Start, Stopp und Download der Steuerung sind gesperrt. OFF: Start, Stopp und Download der Steuerung sind möglich.
Reload-Deaktivierung	ON: Reload ist gesperrt. OFF: Reload ist möglich.
Force-Deaktivierung	ON: Forcen wird abgeschaltet. OFF: Forcen ist möglich.

Tabelle 17: Systemvariable zum Ab- und Aufschließen des PES

Sind alle drei Systemvariablen ON, dann ist kein Zugriff auf die Steuerung mehr möglich.

Einfaches Beispiel für die Nutzung dieser Systemvariablen:

Steuerung abschließbar machen

1. Globale Variable vom Typ BOOL definieren, Initialwert auf OFF setzen.
 2. Globale Variable den drei Systemvariablen *Read only in Run*, *Reload-Deaktivierung* und *Force-Deaktivierung* 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 Schlüssels kann die Steuerung ab- und aufschließen. Bei einem Fehler im entsprechenden digitalen Eingangsmodul oder Eingangskanal ist die Steuerung aufgeschlossen.

Das Beispiel beschreibt den einfachen Fall, dass mit einem Schlüssel alle Eingriffe ins PES gesperrt oder zugelassen werden.

Das einfache Beispiel lässt sich durch die Verwendung von mehreren globalen Variablen, digitalen Eingängen und Schlüsselschaltern so abwandeln, dass die Berechtigungen für Forcen, Reload und die Funktionen Stopp + Start + Download auf unterschiedliche Schlüssel/Personen verteilt sind.

8.2.3 Code-Erzeugung

Nach der vollständigen Eingabe des Anwenderprogramms und der E/A-Belegung der Steuerung den Code erzeugen. Dabei bildet der Codegenerator den Konfigurations-CRC. Dieser ist eine Signatur über die gesamte Konfiguration von CPU, Eingängen, Ausgängen und Kommunikation und wird als Hex-Code im 32-Bit-Format ausgegeben. Die Signatur umfasst alle konfigurierbaren oder veränderbaren Elemente wie Logik, Variable und Schaltereinstellungen.

Um Einflüsse des nicht sicheren PC auszuschließen, erzeugt SILworX in der Standardeinstellung den Code zweimal und vergleicht die erzeugten Konfigurations-CRCs. Sie müssen bei beiden Durchläufen gleich sein.

- Sind die Konfigurations-CRCs gleich, ist der erzeugte Code für den sicherheitsgerichteten Betrieb und zur Zertifizierung durch Prüfstellen benutzbar.

8.2.4 Laden und Starten des Anwenderprogramms

Der Ladevorgang mittels Download eines HIMatrix M45 PES kann nur erfolgen, wenn es zuvor in STOPP gesetzt worden ist.

Das vollständige Laden eines Anwenderprogramms wird überwacht. Danach kann das Anwenderprogramm gestartet werden, d. h. die zyklische Abarbeitung der Routine beginnt.

i

Das PADT kann die Ressource nur dann bedienen, z. B. Reload und Force durchführen, wenn in SILworX das in der Ressource geladene Projekt geöffnet ist. Ohne das Projekt in SILworX ist nur ein STOPP der Ressource möglich!

HIMA empfiehlt, nach jedem Laden eines Anwenderprogramms in die Steuerung die Projektdaten zu sichern, z. B. auf einem Wechselspeichermedium.

Damit soll gewährleistet werden, dass die zur Konfiguration auf der Steuerung passenden Projektdaten weiterhin verfügbar sind, auch wenn das PADT ausfällt.

HIMA empfiehlt eine regelmäßige Datensicherung auch unabhängig vom Laden des Programms.

8.2.5 Reload

Wurden Änderungen an Anwenderprogrammen vorgenommen, dann können diese im laufenden Betrieb auf das PES übertragen werden. Das Betriebssystem prüft und aktiviert das geänderte Anwenderprogramm, das dann die Steuerungsaufgabe übernimmt.

Die Benutzung von Reload ist mit der zuständigen Prüfstelle im Einzelfall abzustimmen!

i

Beim Reload von Schrittketten zu beachten:

Die Reload-Information für Schrittketten berücksichtigt nicht den aktuellen Status der Kette. Daher ist es möglich, durch Reload einer entsprechenden Änderung der Schrittkette diese in einen undefinierten Zustand zu versetzen. Die Verantwortung hierfür liegt beim Anwender.

Beispiele:

- Löschen des aktiven Schritts. Danach hat kein Schritt der Schrittkette den Zustand *aktiv*.
 - Umbenennen des Initialschritts, während ein anderer Schritt aktiv ist.
Dies führt zu einer Schrittkette mit zwei aktiven Schritten!
-

i

Beim Reload von Actions 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 gehen.
- Entfernen des 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.

8.2.6 Forcen

Forcen bedeutet das Ersetzen des aktuellen Wertes einer Variablen durch einen Force-Wert. Eine Variable kann ihren aktuellen Wert durch einen physikalischen Eingang, durch die Kommunikation oder durch eine logische Verknüpfung erhalten. Wird die Variable geforct, so hängt ihr Wert nicht mehr vom Prozess ab, sondern wird vom Anwender vorgegeben.

⚠ WARNUNG**Störung des sicherheitsgerichteten Betriebs durch geforcte Werte möglich!**

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

Forcen ist nur nach Rücksprache mit der für die Anlagenabnahme zuständigen Prüfstelle zulässig.

Während des Forcens muss der Verantwortliche die sicherheitstechnisch ausreichende Überwachung des Prozesses durch andere technische und organisatorische Maßnahmen gewährleisten. HIMA empfiehlt, das Forcen zeitlich zu begrenzen.

Näheres zum Forcen im Systemhandbuch M45 HI 800 650 D.

8.2.6.1 Forcen von Datenquellen

Das Ändern der Zuweisung von geforcten globalen Variablen zu folgenden Datenquellen kann zu unerwarteten Ergebnissen führen:

- Physikalische Eingänge
- Kommunikationsprotokolle
- Systemvariable

Folgender Ablauf führt dazu, dass unbeabsichtigt eine Variable geforct wird:

1. Eine globale Variable A ist einer geforcten Datenquelle zugewiesen und damit geforct.
2. Die Zuweisung wird aufgehoben.
3. Der Datenquelle wird eine andere globale Variable B zugewiesen.
4. Die Änderung am Projekt wird mittels Reload auf das PES geladen.

Als Ergebnis ist die **neu zugewiesene** Variable B geforct, ohne dass dies beabsichtigt war!

Abhilfe: Zuerst das Forcen für die betreffende Variable - hier A - beenden.

In der Kanalansicht des Force-Editors ist erkennbar, welche Kanäle geforct sind.

Globale Variable, deren Datenquelle das Anwenderprogramm ist, behalten die Eigenschaft *geforct* bei einer Änderung der Zuweisung.

8.2.7 Online-Änderung von Systemparametern

Es ist möglich, die Systemparameter der Tabelle 18 online in der Steuerung zu ändern. Ein typischer Anwendungsfall ist die vorübergehende Erhöhung der Watchdog-Zeit, um ein Reload durchführen zu können.

Vor dem Setzen der Parameter durch ein Online-Kommando ist zu bedenken, ob diese Parameteränderung zu einem gefährlichen 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 bzw. gegen die tatsächliche Zykluszeit zu prüfen. Diese Werte können vom PES nicht verifiziert werden!

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

Parameter	Änderbar im Zustand des PES
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	ON->OFF: Alle OFF->ON: STOPP
Autostart	Alle
Start erlaubt	Alle
Laden erlaubt	Alle
Reload erlaubt	Alle
Globales Forcen erlaubt	Alle
Globale Force Timeout-Reaktion	Alle

Tabelle 18: Online-änderbare Parameter

Änderungen an Systemparametern während des Betriebs sind auch durch Reload möglich.

8.2.8 Projekt-Dokumentation für sicherheitsgerichtete Anwendungen

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

- Schnittstellendeklaration
- Variablenliste
- Logik
- Beschreibung der Datentypen
- Konfigurationen für System, Module und Systemparameter
- Konfiguration des Netzwerks
- Variablen-Querverweisliste
- Code-Generator-Informationen

Die Dokumentation ist Bestandteil der Funktionsabnahme einer genehmigungspflichtigen Anlage durch eine Prüfstelle (z. B. TÜV). Die Funktionsabnahme bezieht sich nur auf die Anwenderfunktion, nicht aber auf die sicherheitsgerichteten Module und Automatisierungsgeräte des Systems HIMatrix M45, die bereits baumustergeprüft sind.

8.2.9 Multitasking

Multitasking bezeichnet die Fähigkeit der HIMatrix M45 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 Prozessors dauern. Dies ist durch Parameter der Ressource und des Anwenderprogramms steuerbar. Aus diesen Parametern errechnet SILworX die Watchdog-Zeit des Anwenderprogramms zu:

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

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 parametrisierte 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, mindestens einen Zyklus des Prozessormoduls später aus. Abhängig von der Einstellung *Maximale CPU-Zyklen Programm* bei den Programmen kann das Auslesen um viele Zyklen des Prozessormoduls verzögert geschehen. Die Reaktion auf Änderungen solcher globalen Variablen ist somit entsprechend verzögert!

Einzelheiten zum Multitasking siehe M45 Systemhandbuch, HI 800 650 D.

8.2.10 Abnahme durch Genehmigungsbehörden

Es wird empfohlen, 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 sicherheitsgerichteten Module und Automatisierungsgeräte des Systems HIMatrix M45, die bereits baumustergeprüft sind.

9 Kommunikation

HiMatrix M45 unterstützt sichere Protokolle und Standardprotokolle.

9.1 Standardprotokolle

Eine Reihe von Kommunikationsprotokollen erlaubt nur eine nicht sicherheitsgerichtete Übertragung von Daten. Diese können für nicht sicherheitsgerichtete 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:

Protokoll	Schnittstelle	Ausführung des Kommunikationsmoduls
SNTP	RJ-45	Alle
Send/Receive TCP	RJ-45	Alle
Modbus (Master/Slave)	RJ-45, D-Sub	M-COM 010 2
PROFIBUS-DP Master	D-Sub	M-COM 010 2
PROFIBUS-DP Slave	D-Sub	M-COM 010 3
SSI	D-Sub	M-COM 010 7
CAN	D-Sub	M-COM 010 8
RS422/RS485	D-Sub	Alle

Tabelle 19: Standardprotokolle

9.2 Sicherheitsgerichtetes Protokoll safeethernet

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

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

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

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

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

HINWEIS



Unbeabsichtigter Übergang in den sicheren Zustand möglich!

***ReceiveTMO* ist ein sicherheitsgerichteter 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 Receive Timeout

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

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

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

Da die *ReceiveTMO* sicherheitsrelevant und Bestandteil der Worst Case Reaction Time T_R (maximale Reaktionszeit, siehe Kapitel 9.2.3ff) ist, muss die *ReceiveTMO* wie folgt berechnet und im **safeethernet** Editor eingetragen werden.

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

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

Delay:	Verzögerung auf der Übertragungsstrecke, z. B. durch Switch, andere Übertragungsmedien, z. B. 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.

i

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

9.2.2 Response Time

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

Für die Parametrierung muss eine durch die physikalischen Gegebenheiten der Übertragungsstrecke erwartete *Response Time* vorgegeben und ein geeignetes **safeethernet** Profil ausgewählt werden.

Die vorgegebene *Response Time* hat Einfluss auf die Konfiguration aller Parameter der **safeethernet** Verbindung. Die *Response Time* ist wie folgt zu ermitteln:

$Response \text{ Time} \leq ReceiveTMO / n$

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

Das Verhältnis der *ReceiveTMO* und der *Response Time* 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:

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

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

i

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

i

Der Anwender muss sicherstellen, dass die Übertragungsstrecke die parametrisierte 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 parametrisierte Response Time erhöht werden.

Die Receive Timeout ist der neu parametrisierten Response Time anzupassen.

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

Die maximale Reaktionszeit T_R vom Wechsel eines Eingangs des ersten HIMatrix M45-PES oder Remote I/O (z. B. F3 DIO 20/8 01) bis zur Reaktion des Ausgangs des zweiten HIMatrix M45-PES oder Remote I/O kann wie folgt berechnet werden:

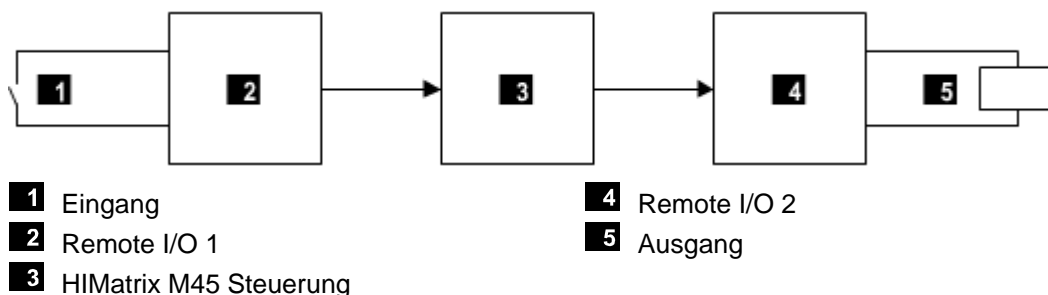


Bild 4: Reaktionszeit mit Remote I/Os

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

T_R Worst Case Reaction Time

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

t_2 ReceiveTMO₁

t_3 2 * Watchdog-Zeit der HIMatrix M45-Steuerung

t_4 ReceiveTMO₂

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

Anmerkung: Die beiden Remote I/Os 1 und 2 können auch identisch sein. Die Zeiten gelten auch dann, wenn statt eines Remote I/O eine HIMatrix M45 Steuerung eingesetzt wird.

9.2.4 Berechnung der max. Reaktionszeit, zwei HIMatrix M45, eine HIMax Steuerung

Die maximale Reaktionszeit T_R vom Wechsel eines Eingangs des ersten HIMatrix M45-PES bis zur Reaktion des Ausgangs des zweiten HIMatrix M45-PES kann wie folgt berechnet werden:

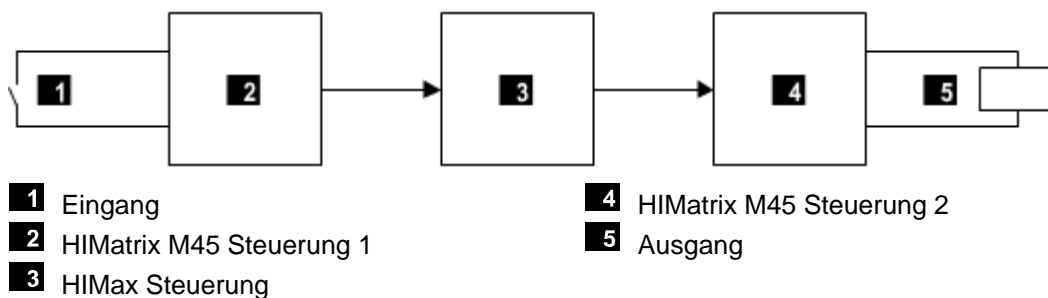


Bild 5: Reaktionszeit mit zwei HIMatrix M45 Steuerungen und einer HIMax-Steuerung

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

T_R Worst Case Reaction Time

t_1 2 * Watchdog-Zeit der HIMatrix M45-Steuerung 1

t_2 ReceiveTMO₁

t_3 2 * Watchdog-Zeit der HIMax-Steuerung

t_4 ReceiveTMO₂

t_5 2 * Watchdog-Zeit der HIMatrix M45-Steuerung 2

Anmerkung: Die beiden HIMatrix M45 Steuerungen 1 und 2 können auch identisch sein.

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 sicherheitsgerichtete Kommunikation geschlossen.

Production Rate Mindestabstand zwischen zwei Datensendungen.

Watchdog-Zeit Maximal zulässige Dauer des RUN-Zyklus einer Steuerung

Worst Case Reaction Time Maximale Reaktionszeit für die Übertragung der Änderung des Signals eines physikalischen Einganges einer Steuerung 1 bis zur Änderung des physikalischen Ausgangs einer Steuerung 2.

9.2.6 Vergabe der safeethernet-Adressen

Bei der Vergabe der Netzwerkadressen (IP-Adressen) für safeethernet auf folgende Punkte achten:

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

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

Anhang

Glossar

Begriff	Beschreibung
ARP	Address Resolution Protocol: Netzwerkprotokoll zur Zuordnung von Netzwerkadressen zu Hardware-Adressen
AI	Analog Input, analoger Eingang
AO	Analog Output, analoger Ausgang
COM	Kommunikationsmodul
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
ICMP	Internet Control Message Protocol: Netzwerkprotokoll für Status- und Fehlermeldungen
IEC	Internationale Normen für die Elektrotechnik
MAC-Adresse	Hardware-Adresse eines Netzwerkanschlusses (Media Access Control)
PADT	Programming and Debugging Tool (nach IEC 61131-3), PC mit SILworX
PE	Protective Earth: Schutzterde
PELV	Protective Extra Low Voltage: Funktionskleinspannung mit sicherer Trennung
PES	Programmierbares Elektronisches System
R	Read: Systemvariable/-signal liefert Wert, z. B. an Anwenderprogramm
rückwirkungsfrei	Es seien zwei Eingangsschaltungen an dieselbe Quelle (z. B. Transmitter) angeschlossen. Dann wird eine Eingangsschaltung <i>rückwirkungsfrei</i> genannt, wenn sie die Signale der anderen Eingangsschaltung nicht verfälscht.
R/W	Read/Write (Spaltenüberschrift für Art von Systemvariable/-signal)
SB	Systembus
SELV	Safety Extra Low Voltage: Schutzkleinspannung
SFF	Safe Failure Fraction, Anteil der sicher beherrschbaren Fehler
SIL	Safety Integrity Level (nach IEC 61508)
SILworX	Programmierwerkzeug für HIMatrix Systeme
SNTP	Simple Network Time Protocol (RFC 1769)
SRS	System.Rack.Slot Adressierung eines Moduls
SW	Software
TMO	Timeout
W	Write: Systemvariable wird mit Wert versorgt, z. B. vom Anwenderprogramm
w _s	Scheitelwert der Gesamt-Wechselspannungskomponente
Watchdog (WD)	Zeitüberwachung für Module oder Programme. Bei Überschreiten der Watchdog-Zeit geht das Modul oder Programm in den Fehlerstopp.
WDZ	Watchdog-Zeit

Abbildungsverzeichnis

Bild 1:	Darstellung der Funktionsblöcke des M-CPU 01	24
Bild 2:	Line Control	28
Bild 3:	Taktsignale T1, T2	28
Bild 4:	Reaktionszeit mit Remote I/Os	49
Bild 5:	Reaktionszeit mit zwei HIMatrix M45 Steuerungen und einer HIMax-Steuerung	49

Tabellenverzeichnis

Tabelle 1:	Umgebungsbedingungen	10
Tabelle 2:	Systemdokumentation HIMatrix M45	12
Tabelle 3:	Wertebereich der Watchdog-Zeit	15
Tabelle 4:	Normen für EMV-, Klima- und Umweltaanforderungen	20
Tabelle 5:	Klimatische Bedingungen	20
Tabelle 6:	Mechanische Prüfungen	21
Tabelle 7:	Prüfungen der Störfestigkeit gemäß IEC 61131-2, Zone C	21
Tabelle 8:	Prüfungen der Störfestigkeit gemäß IEC 61326-3-1	22
Tabelle 9:	Prüfungen der Störfestigkeit gemäß IEC 61326-3-2	22
Tabelle 10:	Prüfungen der Störaussendung	22
Tabelle 11:	Prüfung der Unempfindlichkeit gegenüber Fehlern bei der Versorgungsspannung	23
Tabelle 12:	Übersicht über die Eingänge des HIMatrix M45 Systems	27
Tabelle 13:	Übersicht über die Ausgänge des HIMatrix M45 Systems	30
Tabelle 14:	Die Systemparameter der Ressource	36
Tabelle 15:	Wirkung des Sollzykluszeit-Modus	37
Tabelle 16:	Systemvariable der Hardware	38
Tabelle 17:	Systemvariable zum Ab- und Aufschließen des PES	42
Tabelle 18:	Online-änderbare Parameter	45
Tabelle 19:	Standardprotokolle	47

Index

Cyber-Security 18
Einsatzbedingungen
 ESD-Schutz 11
Fehlerreaktionen 27, 30
Funktionstest der Steuerung 33
Hardware-Editor 38
IT-Sicherheit 18
Multitasking 46
Prüfbedingungen 20
 EMV 21
 klimatisch 20
 mechanisch 21
 Versorgungsspannung 23
Ruhestromprinzip 10
Sicherheitszeit 14
Steuerung abschließbar machen 42
Watchdog-Zeit
 Anwenderprogramm 15
 Ressource 15
Wiederholungsprüfung 15

HI 800 652 D
© 2015 HIMA Paul Hildebrandt GmbH
® = eingetragene Warenzeichen der
HIMA Paul Hildebrandt GmbH

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28 | 68782 Brühl
Telefon +49 6202 709-0 | Telefax +49 6202 709-107
info@hima.com | www.hima.de



SAFETY
NONSTOP



Eine detaillierte Liste aller Niederlassungen und Vertretungen
finden Sie unter: www.hima.de/kontakt

