SEW EURODRIVE

Sicherheitshandbuch

Dezentrale Sicherheitssteuerung

MOVISAFE® HM31

(Version PFF-HM31A)

Ausgabe 05/2014

21230587 / DE

Inhaltsverzeichnis

21230587 / DE – 05/2014

21230587 / DE – 05/2014

21230587 / DE – 05/2014

1 Allgemeine Hinweise

Dieses Handbuch enthält Informationen für den bestimmungsgemäßen Gebrauch der Sicherheitssteuerung.

Voraussetzung für die risikolose Installation, Inbetriebnahme und für die Sicherheit bei Betrieb und Instandhaltung 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 SEW-EURODRIVE keine Haftung übernehmen kann:

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

SEW-EURODRIVE entwickelt, fertigt und prüft Sicherheitssteuerungen 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

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

Das Handbuch beschreibt folgende Variante:

Programmierwerkzeug	Prozessor-Betriebssystem	Kommunikations-Betriebssystem
SILworX®	Ab CPU-BS V.8	Ab COM-BS V.13

1.2 Zielgruppe

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

21230587 / DE – 05/2014

1.3 Darstellungskonventionen

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

Schreibweise	Bedeutung
Fett	Hervorhebung wichtiger Textteile. Bezeichnungen von Schaltflächen, Menüpunkten und Registern im Programmierwerkzeug, auf die Sie klicken können.
Kursiv	Parameter und Systemvariablen.
`Courier`	Wörtliche Benutzereingaben.
RUN	Bezeichnungen von Betriebszuständen in Großbuchstaben.
Kap. 1.2.3	Querverweise auf andere Kapitel

1.4 Aufbau der Warnhinweise

1.4.1 Bedeutung der Signalworte

Die folgende Tabelle zeigt die Abstufung und Bedeutung der Signalworte der Warnhinweise.

Signalwort	Bedeutung	Folgen bei Missachtung
⚠ **GEFAHR**	Unmittelbar drohende Gefahr	Tod oder schwere Verletzungen
⚠ **WARNUNG**	Mögliche, gefährliche Situation	Tod oder schwere Verletzungen
⚠ **VORSICHT**	Mögliche, gefährliche Situation	Leichte Verletzungen
ACHTUNG	Mögliche Sachschäden	Beschädigung des Antriebssystems oder seiner Umgebung
HINWEIS	Nützlicher Hinweis oder Tipp: Erleichtert die Handhabung des Antriebssystems.	

1.4.2 Aufbau der abschnittsbezogenen Warnhinweise

Die abschnittsbezogenen Warnhinweise gelten nicht nur für eine spezielle Handlung, sondern für mehrere Handlungen innerhalb eines Themas. Die verwendeten Gefahrensymbole weisen entweder auf eine allgemeine oder spezifische Gefahr hin.

Hier sehen Sie den formalen Aufbau eines abschnittsbezogenen Warnhinweises:

SIGNALWORT!

Art der Gefahr und ihre Quelle.

Mögliche Folge(n) der Missachtung.

- Maßnahme(n) zur Abwendung der Gefahr.

21230587 / DE – 05/2014

1.4.3 Aufbau der eingebetteten Warnhinweise

Die eingebetteten Warnhinweise sind direkt in die Handlungsanleitung vor dem gefährlichen Handlungsschritt integriert.

Hier sehen Sie den formalen Aufbau eines eingebetteten Warnhinweises:

- ⚠ **SIGNALWORT!** Art der Gefahr und ihre Quelle.

  Mögliche Folge(n) der Missachtung.

  – Maßnahme(n) zur Abwendung der Gefahr.

21230587 / DE – 05/2014

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

2.1.1 Anwendungsbereich

Die sicherheitsgerichtete Steuerung ist einsetzbar bis zum Sicherheits-Integritätslevel SIL 3 gemäß IEC 61508 und PL e gemäß EN ISO 13849-1.

Die Sicherheitssteuerung MOVISAFE® HM31 ist für Schutzsysteme und Maschinensteuerungen zertifiziert.

Bei der Verwendung der sicherheitsgerichteten Kommunikation zwischen verschiedenen Geräten ist zu beachten, dass die Gesamtreaktionszeit des Systems nicht die Fehlertoleranzzeit überschreitet. Die im Kapitel "Konfiguration der Kommunikation" aufgeführten Berechnungsgrundlagen sind anzuwenden.

An die Kommunikations-Schnittstellen dürfen nur Geräte angeschlossen werden, die eine sichere elektrische Trennung gewährleisten.

Ruhestromprinzip / Arbeitsstromprinzip

Die Automatisierungsgeräte sind für das Ruhestromprinzip konzipiert. Ein System, das nach dem Ruhestromprinzip funktioniert, nimmt im Fehlerfall den spannungs- oder stromlosen Zustand („deenergize to trip“) ein, um seine Sicherheitsfunktion auszuführen. Als sicherer Zustand im Fehlerfall wird damit bei Eingangs- und Ausgangssignalen der spannungs- oder stromlose Zustand eingenommen.

Die Sicherheitssteuerungen können auch in Arbeitsstrom-Anwendungen eingesetzt werden. Ein System, das nach dem Arbeitsstromprinzip funktioniert, schaltet z. B. einen Aktor ein, um seine Sicherheitsfunktion auszuführen („energize to trip“).

Bei der Konzeption der Steuerung sind die Anforderungen aus den Anwendungsnormen zu beachten, z. B. kann eine Leitungsdiagnose der Ein- und Ausgänge, oder eine Rückmeldung der ausgelösten Sicherheitsfunktion, erforderlich sein.

2.1.2 Nicht bestimmungsgemäßer Einsatz

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

2.2 Einsatzbedingungen

Der Einsatz der Sicherheitssteuerung ist nur zulässig unter Umgebungsbedingungen, die innerhalb der im Folgenden genannten Bedingungen liegen.

21230587 / DE – 05/2014

Die Sicherheitssteuerung wurde für die Einhaltung der Anforderungen der folgenden Normen für EMV, Klima- und Umweltanforderungen entwickelt:

Norm	Inhalt
EN 61800-5-1:2007	Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl - Teil 5-1: Anforderungen an die Sicherheit - Elektrische, thermische und energetische Anforderungen.
EN 61800-3:2004	Drehzahlveränderbare elektrische Antriebe - Teil 3: EMV-Anforderungen einschließlich spezieller Prüfverfahren .
EN 62061:2005	Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme.

Für den Einsatz des sicherheitsgerichteten Steuerungssystems MOVISAFE® HM31 sind die nachfolgenden allgemeinen Bedingungen einzuhalten:

Art der Bedingung	Inhalt der Bedingung
Aufstellhöhe (Industriestandard	< 2000 m Durch SEU-Effekte (Single Event Upset) kann es in SRAM-basierenden Zellen zu Bitfehlern kommen. Je höher die Aufstellhöhe, desto größer sind diese Effekte.
Schutzart	IP54 (gemäß EN 60529)

2.2.1 Klimatische Bedingungen

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

EN 61800-5-1	Klimaprüfungen
	Betriebstemperatur: −5 °C bis +50 °C
	Lagertemperatur: −25 °C bis +70 °C
	Trockene Wärme (konstant) Beständigkeitsprüfungen gemäß IEC 60068-2-2:2007 (Prüfung Bd)
	Feuchte Wärme (konstant) Beständigkeitsprüfungen gemäß IEC 60068-2-78:2001 (Prüfung Cab)

2.2.2 Mechanische Bedingungen

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

EN 61800-5-1	Mechanische Prüfungen
	Unempfindlichkeitsprüfung gegen Schwingungen gemäß IEC 60068-2-6:2007 (Prüfung Fc)

2.2.3 EMV-Bedingungen

Für die Sicherheitssteuerung MOVISAFE® HM31 werden erhöhte Pegel bei der Störbeeinflussung gefordert. Die Sicherheitssteuerung MOVISAFE® HM31 erfüllt die Störaussendungsanforderungen gemäß EN 61800-3:2004 (Grenzwertklasse C2) und die Störfestigkeitsanforderungen gemäß EN 62061:2005 und EN 61800-3:2004 (zweite Umgebung).

21230587 / DE – 05/2014

2.2.4 Spannungsversorgung

Die wichtigsten Prüfungen und Grenzwerte für die Spannungsversorgung der Sicherheitssteuerung sind in nachstehender Tabelle aufgelistet:

IEC/EN 61131-2	Nachprüfung der Eigenschaften der Gleichstromversorgung
	Die Spannungsversorgung muss folgende Normen erfüllen: IEC/EN 61131-2: SELV (Safety Extra Low Voltage) oder PELV (Protective Extra Low Voltage)
	Die Absicherung der Sicherheitssteuerung muss gemäß den Angaben dieses Handbuchs erfolgen.
	Prüfung des Spannungsbereichs: 24 VDC, −20 % bis +25 % (19.2 V bis 30.0 V)
	Prüfung auf Unempfindlichkeit gegen Kurzzeitunterbrechung der externen Stromversorgung: DC, PS 2: 10 ms
	Polaritätsumkehr der Versorgungsspannung: Hinweis im entsprechenden Kapitel des Systemhandbuchs oder im Datenblatt der Stromversorgung.

2.2.5 ESD-Schutzmaßnahmen

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

ACHTUNG

Elektrostatische Entladungen können die in der Sicherheitssteuerung eingebauten elektronischen Bauteile zerstören!

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

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 Sicherheitssteuerung in Automatisierungsanlagen und in Gesamtanlagen gewährleistet ist.

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

21230587 / DE – 05/2014

2.4 Weitere Systemdokumentationen

- Betriebsanleitung "Dezentrale Sicherheitssteuerung MOVISAFE® HM31"
- Systemhandbuch "Dezentrale Sicherheitssteuerung MOVISAFE® HM31"

Sie finden die jeweils aktuelle Version der Dokumentation auf der SEW-Homepage (www.sew-eurodrive.de) in der Rubrik "Dokumentationen".

2.5 Checkliste zur Projektierung, Programmierung und Inbetriebnahme

Diese Checkliste ist eine Empfehlung für den Anwender

- zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsgerichteten Ein- und Ausgängen
- zur Erstellung eines Anwenderprogramms mit dem Programmierwerkzeug SILworX®

Durch das Ausfüllen der Checkliste 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 *PFF_HM31A_Checkliste_DE.pdf* kann als PDF-Dokument auf der SEW-Homepage (www.sew-eurodrive.de) unter der Rubrik "Dokumentationen" im Bereich "safetyDRIVE" heruntergeladen werden.

21230587 / DE – 05/2014

3 Sicherheitskonzept für den Einsatz von MOVISAFE® HM31

Dieses Kapitel behandelt wichtige allgemeine Fragen der funktionellen Sicherheit der Sicherheitssteuerung MOVISAFE® HM31:

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

3.1 Sicherheit und Verfügbarkeit

Die Sicherheitssteuerung ist für Schutzsysteme und Maschinensteuerungen zertifiziert.

Von der Sicherheitssteuerung gehen keine unmittelbaren Gefahren aus.

⚠ WARNUNG

Gefahr durch falsch angeschlossene oder falsch programmierte sicherheitsgerichtete Automatisierungssysteme.

Tod oder schwere Körperverletzung.

3.1.1 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 die defekte Sicherheitssteuerung oder den defekten E/A-Kanal ab.

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

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

Zusätzlich kann das Anwenderprogramm verschiedene Systemvariablen auswerten, die den Zustand der Sicherheitssteuerung 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.

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

21230587 / DE – 05/2014

3.1.2 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 installiert ist.

3.2 Für die Sicherheit wichtige Zeiten

Diese sind:

- Fehlertoleranzzeit
- Watchdog-Zeit
- Sicherheitszeit
- Reaktionszeit

3.2.1 Fehlertoleranzzeit (FTZ)

Die Fehlertoleranzzeit ist eine Eigenschaft des Prozesses und beschreibt die Zeitspanne, in der der Prozess durch fehlerhafte Signale beaufschlagt werden kann, ohne dass ein gefährlicher Zustand eintritt.

3.2.2 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).

Betriebssystem-Version	Sicherheitszeit im Bereich
Ab CPU-BS V.8	20 – 22500 ms

3.2.3 Sicherheitszeit des Anwenderprogramms

Die Sicherheitszeit des Anwenderprogramms lässt sich nicht unmittelbar einstellen. Die Sicherheitssteuerung MOVISAFE® HM31 errechnet die Sicherheitszeit eines Anwenderprogramms aus den Parametern *Sicherheitszeit der Ressource* und *Maximale Zyklenanzahl*. Zu Einzelheiten siehe Kapitel "Multitasking".

3.2.4 Mehrfehlereintrittszeit

Die Eintrittszeit für Mehrfachfehler ist die Zeitspanne, in der die Wahrscheinlichkeit für das Auftreten von Mehrfachfehlern, die in Kombination sicherheitskritisch sind, hinreichend gering ist.

Die Mehrfehlereintrittszeit ist im Betriebssystem mit 24 Stunden definiert.

21230587 / DE – 05/2014

3.2.5 Reaktionszeit

Die maximale Reaktionszeit von zyklisch arbeitenden Sicherheitssteuerungen ist die doppelte Zykluszeit dieser Systeme, wenn nicht durch Parametrierung oder die Logik des Anwenderprogramms eine Verzögerung erfolgt.

Die Zykluszeit einer Steuerung besteht aus folgenden wesentlichen Teilen:

- Lesen der Eingänge
- Verarbeiten des Anwenderprogramms
- Schreiben der Ausgänge
- Prozessdaten-Kommunikation
- Ausführen der Testroutinen

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

3.2.6 Watchdog-Zeit des Prozessorsystems

Die Watchdog-Zeit wird als Zeit 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 parametriert wurde. Falls Autostart nicht parametriert wurde, geht das System in den Zustand STOPP/GÜLTIGE KONFIGURATION.

Die Watchdog-Zeit des Prozessorsystems darf eingestellt werden auf:

Max. 0,5 × Sicherheitszeit des PES

Betriebssystem-Version	Wertebereich Watchdog-Zeit	Standardwert Steuerungen
Ab CPU-BS V.8	4 – 5000 ms	200 ms

3.2.7 Watchdog-Zeit des Anwenderprogramms

Jedes Anwenderprogramm hat einen eigenen Watchdog und eine eigene Watchdog-Zeit.

Die Watchdog-Zeit des Anwenderprogramms lässt sich nicht unmittelbar einstellen. Die Sicherheitssteuerung MOVISAFE® HM31 errechnet die Watchdog-Zeit eines Anwenderprogramms aus den Parametern *Max. Watchdog-Zeit* der Ressource und *Maximale Zyklenanzahl*.

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

3.3 Wiederholungsprüfung

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.

SEW-Sicherheitssysteme müssen in Intervallen einer Wiederholungsprüfung unterzogen werden. Durch eine Analyse der realisierten Sicherheitskreise mittels Berechnung kann das Intervall häufig verlängert werden.

21230587 / DE – 05/2014

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 Sicherheitssteuerung MOVISAFE® HM31 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 Sicherheitssteuerung. Wenn der Anwender den kompletten Sicherheitskreis wegen des Feldgeräts prüft, dann ist die Sicherheitssteuerung in diesen Test automatisch eingeschlossen. Es sind dann keine zusätzlichen Wiederholungsprüfungen für die Sicherheitssteuerung erforderlich.

Falls die Wiederholungsprüfung der Feldgeräte die Sicherheitssteuerung nicht mit einbezieht, dann muss diese für SIL 3 mindestens einmal in 20 Jahren ersetzt werden. Dies wird erreicht, indem die Sicherheitssteuerung ausgetauscht wird (siehe Betriebsanleitung "Dezentrale Sicherheitsteuerung MOVISAFE® HM31, Kapitel "Sicherheitskennwerte MOVISAFE® HM31").

3.4 Sicherheitsauflagen

Für den Einsatz der sicherheitsgerichteten PES des Systems MOVISAFE® HM31 gelten folgende Sicherheitsauflagen.

3.4.1 Hardware-Projektierung

Personen, die die Hardware der Sicherheitssteuerung MOVISAFE® HM31 projektieren, müssen die folgenden Sicherheitsauflagen beachten.

Produktunabhängige Auflagen

- Für sicherheitsgerichteten Betrieb darf nur hierfür zugelassene, fehlersichere Hardware und Software verwendet werden. Die zugelassene Hardware und Software ist aufgeführt in der Versionsliste der Sicherheitssteuerung MOVISAFE® HM31, Zertifikatsnummer 968/EZ 529.00/11.
- Die spezifizierten Einsatzbedingungen (siehe Kapitel "Einsatzbedingungen") bezüglich EMV, mechanischen, chemischen und klimatischen Einflüssen müssen eingehalten werden.
- Nicht fehlersichere, jedoch rückwirkungsfreie Hardware und Software darf für die Verarbeitung nicht sicherheitsrelevanter Signale eingesetzt werden, nicht jedoch für die Bearbeitung sicherheitstechnischer Aufgaben
- Bei allen extern an das System angeschlossenen Sicherheitsstromkreisen ist das Ruhestromprinzip einzuhalten

21230587 / DE – 05/2014

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.

Applikationsabhängige Auflagen

Durch konstruktive Maßnahmen des Applikationsaufbaus oder organisatorische Maßnahmen muss auf ein punktuell vermindertes Sicherheitsniveau reagiert werden. Um die Wahrscheinlichkeit von Fehlern gemeinsamer Ursache gering zu halten, sind folgende Vorgaben einzuhalten. Darüber hinaus sind je nach Applikation weitere anerkannte Maßnahmen zur Erhöhung der Sicherheit zu berücksichtigen.

- Die Signalkabel müssen für alle Kanäle an allen Stellen getrennt geführt werden.
- Alle Signal- und Energieleitungen müssen voneinander getrennt verlegt werden.
- Die Ein- und Ausgänge müssen vor möglichen Überspannungen und Überströmen geschützt werden.
- Alle mechanischen Komponenten sind so zu dimensionieren, dass die Anforderung bezüglich funktionaler Sicherheit erfüllt werden. Dies kann z. B. durch Überdimensionierung mit Faktor 2 oder höher erreicht werden.
- Alle Ausfälle im Feld sind vollständig zu analysieren und den Herstellern umgehend mitzuteilen, damit diese im Zuge ihrer QM-Prozesse ggf. Verbesserungsmaßnahmen einleiten können. Dabei ist ein dokumentierter Nachweis des Verfahrens notwendig.
- Es ist eine schriftliche Arbeitsanweisung zu erstellen, die gewährleistet, dass alle Bauteilausfälle (oder Verschlechterungen) erkannt, deren Ursachen festgestellt und ähnliche Objekte im Hinblick auf mögliche ähnliche Ausfallursachen überprüft werden.
- Nach Wartungs-, Reparatur- und Instandhaltungsarbeiten an sicherheitsrelevanten Komponenten (z. B. Geber, Bremsen usw.) muss die Anlage neu kalibriert und die einwandfreie Funktion (d. h. einwandfreier Durchlauf der Diagnosetests) geprüft werden. Diese Arbeiten müssen für die voneinander unabhängigen Kanäle zeitlich versetzt erfolgen.
- In den Instandhaltungsanweisungen muss vorgeschrieben sein, dass alle Teile der redundanten Systeme (z. B. Kabel usw.), die voneinander unabhängig sein müssen, nicht geändert werden dürfen.
- Die Instandhaltung aller Komponenten (z. B. Leiterplatten) sind in einem qualifizierten Reparaturzentrum durchzuführen. Alle reparierten Einheiten sind vor der Installation einem vollständigen Test zu unterziehen.
- Die Instandhalter müssen dazu ausgebildet werden (mit Ausbildungsdokumentation), die Ursachen und Folgen von Ausfällen infolge gemeinsamer Ursache zu verstehen.
- Der Zutritt für Personal ist einzuschränken (z. B. durch verschlossene Bereiche, unzugängliche Position/Orte).
- Das System darf nur innerhalb des Temperatur-, Feuchte-, Korrosions-, Staub- und Vibrationsbereiches, für das es getestet worden ist, eingesetzt werden.
- Die Systemkomponenten müssen auf Beständigkeit gegen alle wichtigen Umgebungseinflüsse (z. B. EMV, Temperatur, Vibration, Schock, Feuchte) entsprechend eines angemessenen, in anerkannten Normen festgelegten Niveaus, getestet worden sein.

21230587 / DE – 05/2014

3.4.2 Programmierung

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

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.

Produktabhängige Auflagen

Auflagen für die Verwendung des Programmierwerkzeugs.

- Zur Programmierung muss das Werkzeug SILworX® verwendet werden.
- Nach der Applikationserstellung ist durch manuelles doppeltes Kompilieren und Vergleich der CRCs sicherzustellen, dass die Kompilierung korrekt erfolgte.
- Die korrekte Umsetzung der Spezifikation der Applikation ist zu validieren und zu verifizieren. Es muss eine vollständige Prüfung der Logik durch Erprobung erfolgen
- Nach jeder Änderung der Applikation ist diese Prozedur zu wiederholen
- Die Fehlerreaktion des Systems bei Fehlern in den fehlersicheren Eingangsbaugruppen, Ausgangsbaugruppen und Remote I/Os 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 Fehlertoleranzzeit überschreitet. Die im Kapitel 8.2 aufgeführten Berechnungsgrundlagen sind anzuwenden.
- Eine Übertragung der sicherheitsrelevanten Daten über öffentliche Netze (z. B. Internet) ist ohne zusätzliche Sicherheitsmaßnahmen, z. B. VPN-Tunnel nicht zulässig.
- 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. 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 Kommunikations-Schnittstellen dürfen nur Geräte angeschlossen werden, die eine sichere elektrische Trennung gewährleisten.

3.4.4 Wartungseingriffe

- Für Wartungseingriffe die jeweils aktuelle Version des Dokuments „Maintenance Override“ des TÜV Rheinland und TÜV Product Service (www.tuvasi.com) beachten
- Erforderlichenfalls muss der Betreiber in Absprache mit der für die Applikation zuständigen Abnahmestelle administrative Maßnahmen für den Zugangsschutz zu den Systemen festlegen

21230587 / DE – 05/2014

3.5 Zertifizierung

Die Sicherheitssteuerung MOVISAFE® HM31 (Programmierbares Elektronisches System, PES) ist gemäß den Normen für die funktionale Sicherheit geprüft und vom TÜV zertifiziert, sowie CE-konform.

Das TÜV-Zertifikat kann von der SEW-Homepage (www.sew-eurodrive.de) in der Rubrik "Dokumentationen" im Bereich "safetyDrive" heruntergeladen werden.

21230587 / DE – 05/2014

4 Eingänge der Sicherheitssteuerung MOVISAFE® HM31

Die Sicherheitssteuerung MOVISAFE® HM31 verfügt über 26 sicherheitsgerichtete digitale Eingänge.

- 16 digitale Eingänge, Typ I (EN 61131-2)
- 8 digitale Eingänge, Typ II (EN 61132-2)
- 2 digitale Eingänge sind zur internen Diagnose reserviert

4.1 Allgemeines

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

Die Steuerung liefert Status- und Fehlerinformation auf folgende Weisen:

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

Sicherheitsgerichtete Eingangsbaugruppen führen während des Betriebes automatisch einen hochwertigen, zyklischen Selbsttest durch. Diese Testroutinen sind TÜV-geprüft und überwachen die sichere Funktion der jeweiligen Baugruppe.

Bei einem Fehler stellt die Steuerung dem Anwenderprogramm einen Low-Pegel zur Verfügung – ab CPU-BS V.8 den festgelegten Initialwert – und erzeugt eine Fehlerinformation, wenn möglich. Das Anwenderprogramm kann diese Fehlerinformation durch Auslesen des Fehlercodes auswerten.

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

4.2 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, PL entsprechen.

4.3 Sicherheitsgerichtete digitale Eingänge

4.3.1 Allgemeines

Die digitalen Eingänge werden einmal in jedem Zyklus gelesen und intern gespeichert; sie werden zyklisch auf sichere Funktion getestet. Eingangssignale, die kürzer als die Zeit zwischen zwei Abtastungen (also kürzer als für eine Zykluszeit) anstehen, werden unter Umständen nicht erfasst.

4.3.2 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.

21230587 / DE – 05/2014

4.3.3 Reaktion im Fehlerfall

Wenn die Testroutinen für digitale Eingänge einen Fehler feststellen, verarbeitet das Anwenderprogramm für den fehlerhaften Kanal entsprechend dem Ruhestromprinzip ein Low-Pegel.

Das Anwenderprogramm muss zusätzlich zum Signalwert des Kanals den entsprechenden Fehlercode berücksichtigen.

Die Sicherheitssteuerung MOVISAFE® HM31 aktiviert die LED ERROR.

Durch Verwendung des Fehlercodes bestehen zusätzliche Möglichkeiten, im Anwenderprogramm die externe Beschaltung zu überwachen und Fehlerreaktionen zu programmieren.

Zugang zum Fehlercode	Name des Fehlercodes
Im Register *...Kanäle* in der Detailansicht der Baugruppe oder des Geräteteils.	*->Fehlercode [Byte]* in der Zeile mit der Kanalnummer.

4.3.4 Surge auf digitalen Eingängen

Bedingt durch die kurze Zykluszeit der Sicherheitssteuerung 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 aktivieren, ein Signal muss mindestens zwei Zyklen anstehen, bevor es ausgewertet wird.

HINWEIS

- Die Aktivierung der Störaustastung verlängert die Reaktionszeit der Sicherheitssteuerung.
- 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.
- Ausführliche Informationen zum Thema "EMV" finden Sie in der Druckschrift "Praxis der Antriebstechnik – EMV in der Antriebstechnik". Die aktuelle Version dieser Dokumentation finden Sie auf der SEW-Homepage (www.sew-eurodrive.de) in der Rubrik "Dokumentationen".

4.4 Sicherheitsgerichtete Zähler

4.4.1 Allgemeines

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

Bei der Verwendung als schneller Vorwärts-/Rückwärtszähler sind als Signale der Impulseingang und der Zählrichtungseingang in der Anwendung notwendig. Ein Reset erfolgt nur im Anwenderprogramm.

21230587 / DE – 05/2014

Die Encoder-Auflösung 4- oder 8-Bit gilt für die Zählerbaugruppe CIO 2/4 01 der F60; bei der F35 hat der Encoder 3- oder 6-Bit Auflösung. Ein Reset ist möglich. Die Verknüpfung von zwei unabhängigen 4-Bit-Eingängen zu einem 8-Bit-Eingang (Beispiel für F60) erfolgt ausschließlich per Anwenderprogramm. Eine Schaltmöglichkeit für diesen Zweck ist nicht vorgesehen.

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

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

4.4.2 Reaktion im Fehlerfall

Stellen die Testroutinen im Zählerteil des Geräts oder der Baugruppe einen Fehler fest, setzen sie ein Status-Bit für die Auswertung im Anwenderprogramm. Zusätzlich kann das Anwenderprogramm auch den entsprechenden Fehlercode berücksichtigen.

Die Sicherheitssteuerung MOVISAFE® HM31 aktiviert die LED ERROR. Durch Verwendung des Fehlercodes bestehen zusätzliche Möglichkeiten, im Anwenderprogramm die externe Beschaltung zu überwachen und Fehlerreaktionen zu programmieren.

Zugang zum Fehlercode	Name des Fehlercodes
Im Register *...Kanäle* in der Detailansicht der Baugruppe oder des Geräteteils.	*->Fehlercode [Byte]* in der Zeile mit der Kanalnummer.

4.5 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 *PFF_HM31_Checkliste.doc* steht als Dokument im Format von Microsoft®Word® zur Verfügung. Die Checkliste kann von der SEW-Webseite (www.sew-eurodrive.de) heruntergeladen werden.

21230587 / DE – 05/2014

5 Ausgänge der Sicherheitssteuerung MOVISAFE® HM31

Die Sicherheitssteuerung MOVISAFE® HM31 verfügt über 8 sicherheitsgerichtete 2-polige Ausgänge.

5.1 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 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 der defekten Ausgangsbaugruppe 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.

Diese Funktion ist nur wirksam für alle digitalen Ausgänge der Steuerung. Die Verwendung des jeweiligen Fehlercodes bietet zusätzliche Möglichkeiten, Fehlerreaktionen im Anwenderprogramm zu konfigurieren.

5.2 Sicherheit von Aktoren

In einer sicherheitsgerichteten Anwendung müssen sowohl die Steuerung als auch die daran angeschlossenen Aktoren den Sicherheitsanforderungen und dem spezifizierten SIL entsprechen.

5.3 Sicherheitsgerichtete 2-polige digitale Ausgänge

5.3.1 Testroutinen für 2-polige digitale Ausgänge

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

- Rücklesen des Ausgangssignals des Schaltverstärkers. Die eingesetzten Dioden verhindern ein Rückspeisen von Signalen.
- Prüfen der integrierten (zweifachen) Sicherheitsabschaltung.
- Ein Abschalttest der Ausgänge erfolgt innerhalb der MEZ für jeweils max. 200 µs. Der Mindestabstand zwischen zwei Tests betragt ≥ 20 Sekunden.

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

21230587 / DE – 05/2014

5.3.2 Reaktion im Fehlerfall

Bei Feststellen eines fehlerhaften Signals setzt die Sicherheitssteuerung den betroffenen Ausgang über die Sicherheitsschalter in den sicheren, energielosen Zustand. Ein Modulfehler der Sicherheitssteuerung führt zum Abschalten aller Ausgänge. Beide Fehlerarten zeigt die Sicherheitssteuerung MOVISAFE® HM31 zusätzlich mit der LED ERROR an.

DO x.x_P-Ausgänge

Bei Feststellen eines fehlerhaften Signals setzt die Sicherheitssteuerung den betroffenen Ausgang über die Sicherheitsschalter in den sicheren, energielosen Zustand. Ein Fehler der Sicherheitssteuerung führt zum Abschalten aller Ausgänge. Beide Fehler zeigt die Sicherheitssteuerung MOVISAFE® HM31 zusätzlich mit der LED ERROR an.

5.3.3 Verhalten bei externem Kurzschluss oder Überlast

Bei einem Schluss des Ausgangs nach 0V24 oder Überlast bleibt die Testbarkeit der Sicherheitssteuerung erhalten. Eine Abschaltung über die Sicherheitsabschaltung ist nicht notwendig.

Die Gesamtstromaufnahme der Sicherheitssteuerung wird überwacht. Bei Überschreiten der Schwelle setzt die Sicherheitssteuerung alle Kanäle in den sicheren Zustand.

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

5.4 Taktausgänge (DO-Kanäle des DI-26-Moduls)

Das System besitzt vier nicht sicherheitsgerichtete, strombegrenzte digitale Ausgänge (24 V).

Die Ausgänge sind nicht galvanisch von der Versorgungseinheit getrennt. Mit der Querstromüberwachung (Line Control) der 24-V-Ausgänge besteht die Möglichkeit einer Leitungsbruch- und Leitungsschlusserkennung. Hierzu werden die Taktausgänge einzeln kurzzeitig abgesteuert und die Signale an den zugehörigen digitalen Eingängen gelesen. Für die Querstromüberwachung müssen immer unterschiedliche Taktausgänge verwendet werden.

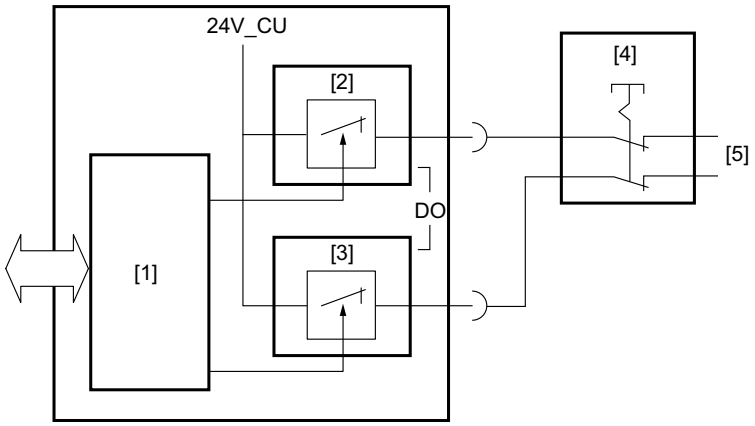
In SILworX® können für die Taktausgänge (zusammen mit den digitalen Eingängen) folgende Parameter eingestellt werden:

- Zuordnung zwischen Taktausgang und digitalem Eingang
- Wartezeit (min. 400 µs) zwischen dem Absteuern des Taktausgangs und dem Lesen des Eingangs, einstellbar über den Parameter *DI Taktverzögerung [µs]*.

  Die Wartezeit verlängert die Zykluszeit um den eingestellten Wert.

21230587 / DE – 05/2014

Die folgende Darstellung zeigt Ihnen das Prinzip einer Leitungsüberwachung:



9007204202753163

[1] Anbindung an E/A-Bus

[2] Kanal 1

[3] Kanal 2

[4] Not-Aus-Schalter

[5] Schnittstelle zu den digitalen Eingängen

HINWEIS

Beachten Sie bei der Projektierung:

- Wenn DO02 taktend eingestellt ist, ist DO01 ebenfalls taktend eingestellt.
- Wenn DO04 taktend eingestellt ist, sind DO03, DO02 und DO01 ebenfalls taktend eingestellt.

⚠ WARNUNG

Verlust der Sicherheitsklasse (Performance Level) durch falsche Ansteuerung.

Tod oder schwere Körperverletzung

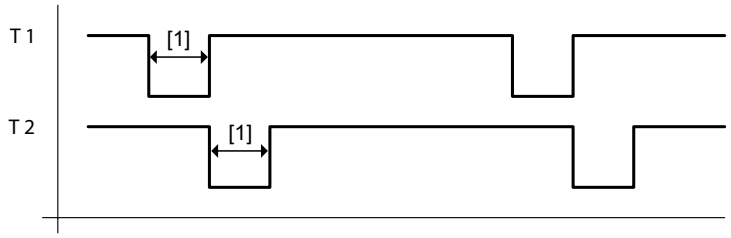
- Taktausgänge dürfen nicht als sicherheitsgerichtete Ausgänge verwendet werden, z. B. zur Ansteuerung von sicherheitsgerichteten Aktoren!

Die Spezifikation der Taktausgänge finden Sie in der Betriebsanleitung im Kapitel "Technische Daten"

21230587 / DE – 05/2014

5.4.1 Taktausgabe

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 im Systemhandbuch).



4784626827

[1] Konfigurator 400 – 2000 µs

21230587 / DE – 05/2014

6 Software für Sicherheitssteuerung MOVISAFE® HM31

Die Software der Sicherheitssteuerung gliedert sich in die folgenden Teile:

- Betriebssystem
- Anwenderprogramm
- Programmiertool 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 Programmiertool 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 Programmiertool.

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

6.1 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 gemeinsam mit dem TÜV erstellt wird.

Ein Auslesen der laufenden Betriebssystemversion ist nur mit dem Programmiertool möglich. Eine Kontrolle durch den Anwender ist erforderlich (vgl. Kapitel "Checkliste zur Projektierung, Programmierung und Inbetriebnahme").

6.2 Arbeitsweise und Funktionen des Betriebssystems

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

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

Hinzu kommen folgende wesentlichen Funktionen:

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

21230587 / DE – 05/2014

6.3 Sicherheitstechnische Aspekte für die Programmierung

6.3.1 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.
- Doppelte Kompilierung mit anschließendem Vergleich der erzeugten CRC-Prüfsummen stellt sicher, dass Verfälschungen der Anwendung durch temporäre Fehlfunktionen des benutzten PCs erkannt werden.

Programm doppelt kompilieren und Ergebnisse vergleichen:

1. Kompilierung starten.

   Bei Abschluss der Kompilierung zeigt das Programmierwerkzeug eine CRC-Prüfsumme an.

2. Kompilierung erneut starten.

   Bei Abschluss der Kompilierung zeigt das Programmierwerkzeug eine CRC-Prüfsumme an.

Sind beide CRC-Prüfsummen gleich, hat keine Verfälschung bei der Kompilierung stattgefunden.

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

Funktionstest der Steuerung

3. Überprüfung der korrekten Umsetzung der Steuerungsaufgabe anhand der Daten und Signalflüsse.
4. Vollständige Funktionsprüfung der Logik durch Erprobung (siehe Überprüfung der Konfiguration und des Anwenderprogramms).

Die Steuerung und das Anwenderprogramm sind hinreichend überprüft.

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

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

21230587 / DE – 05/2014

6.3.2 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. Das Programmiertool und die 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.

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.

Diese Vorgehensweise betrifft die Ersterstellung eines Anwenderprogramms ebenso wie dessen Änderungen.

6.3.3 Archivierung eines Projekts

SEW-EURODRIVE empfiehlt, nach jedem Laden des Programms in die Steuerung das Projekt zu archivieren. Dies gilt für Download wie für Reload.

Erstellung eines Projekt-Archivs:

1. Ausdrucken des Anwenderprogramms zum Vergleich der Logik mit den Vorgaben.
2. Übersetzen des Anwenderprogramms zum Erzeugen des Konfigurations-CRC der CPU.
3. Notieren der Version des Konfigurations-CRC der CPU.
4. Archiv des Projekts auf Speichermedium erstellen und mit Namen der Anwenderprogramme, Konfigurations-CRCs der CPUs und Datum versehen. Diese Empfehlung ersetzt nicht die internen Dokumentationserfordernisse des Anwenders.

Das Projektarchiv ist erstellt.

SILworX® legt ein Projekt in einer Projektdatei an. Diese kann auf einem Speichermedium (z. B. USB-Stick) gespeichert werden.

6.3.4 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.

21230587 / DE – 05/2014

6.4 Parameter der Ressource

⚠ WARNUNG

Fehlerhafte Konfiguration.

Tod oder schwere Körperverletzungen.

- System-ID
- Sicherheitszeit
- Watchdog-Zeit
- Hauptfreigabe
- Autostart
- Start erlaubt
- Laden erlaubt
- Reload erlaubt
- Globales Forcen erlaubt

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.

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

6.4.1 Systemparameter der Ressource

Diese Parameter legen das Verhalten der Steuerung während des Betriebs fest und werden in SILworX eingestellt.

Parameter/Schalter	Beschreibung	Standardwert	Einstellung für sicheren Betrieb
Name	Name der Ressource		Beliebig
System ID [SRS]	System-ID der Ressource 1 – 65 535 Die System ID muss einen anderen Wert als den Standardwert erhalten, sonst ist das Projekt nicht ablauffähig!	60 000	Eindeutiger Wert innerhalb des Netzwerks der Steuerungen, die potenziell miteinander verbunden sind.
Sicherheitszeit [ms]	Sicherheitszeit in Millisekunden. 20 – 22 500 ms	600 ms	Applikationsspezifisch
Watchdog-Zeit [ms]	Watchdog-Zeit in Millisekunden. 8 – 5000 ms	200 ms bei Steuerungen	Applikationsspezifisch

21230587 / DE – 05/2014

Parameter/Schalter	Beschreibung	Standardwert	Einstellung für sicheren Betrieb
Hauptfreigabe	**ON:** Folgende Schalter/Parameter sind im Betrieb (= RUN) mit dem PADT änderbar: • System-ID • Watchdog-Zeit der Ressource • Sicherheitszeit • Sollzykluszeit • Sollzykluszeit-Modus • Autostart • Globales Forcen erlaubt • Globale Force-Timeout-Reaktion • Laden erlaubt • Reload erlaubt • Start erlaubt **OFF:** Die Parameter sind nicht im Betrieb änderbar. **Hinweis:** Nur bei gestopptem PES ist es möglich, *Hauptfreigabe* auf ON zu setzen!	ON	OFF empfohlen
Autostart	**ON:** Wird das Prozessorsystem an die Versorgungsspannung angeschlossen, startet das Anwenderprogramm automatisch. **OFF:** Kein automatischer Start nach Zuschalten der Versorgungsspannung.	OFF	Applikationsspezifisch
Start erlaubt	**ON:** Kaltstart oder Warmstart durch PADT im Zustand RUN oder STOPP erlaubt. **OFF:** Kein Start erlaubt.	ON	Applikationsspezifisch

21230587 / DE – 05/2014

Parameter/Schalter	Beschreibung	Standardwert	Einstellung für sicheren Betrieb
Laden erlaubt	**ON:** Download des Anwenderprogramms erlaubt. **OFF:** Download des Anwenderprogramms nicht erlaubt.	ON	Applikationsspezifisch
Reload erlaubt	**ON:** Reload des Anwenderprogramms erlaubt. **OFF:** Reload des Anwenderprogramms nicht erlaubt. Ein laufendes Reload wird beim Umschalten auf OFF nicht abgebrochen.	ON	-
Globales Forcen erlaubt	**ON:** Globales Forcen für diese Ressource erlaubt. **OFF:** Globales Forcen für diese Ressource nicht erlaubt.	ON	Applikationsspezifisch
Globale Force-Timeout-Reaktion	Legt fest, wie sich die Ressource beim Ablauf des globalen Force-Timeout verhält: • Forcen beenden • Ressource stoppen	Forcen beenden	Applikationsspezifisch
Max. Kom. Zeitscheibe ASYNC [ms]	Höchstwert in ms der Zeitscheibe, die innerhalb des Zyklus der Ressource für Kommunikation verwendet wird, 2...5000 ms	60 ms	Applikationsspezifisch
Max. Dauer Konfigurationsverbindungen [ms]	Definiert, wie viel Zeit innerhalb eines CPU-Zyklus für die Prozessdaten-Kommunikation zur Verfügung steht, 6 – 5 000 ms	6 ms	
Sollzykluszeit [ms]	Gewünschte oder maximale Zykluszeit, siehe *Sollzykluszeit- Modus*, 0 – 7 500 ms. Die Sollzykluszeit darf höchstens so groß sein wie die eingestellte Watchdog-Zeit (6 ms), andernfalls lehnt das PES sie ab.	0 ms	-

21230587 / DE – 05/2014

Parameter/Schalter	Beschreibung	Standardwert	Einstellung für sicheren Betrieb
Multitasking Modus	**Mode 1:** Die Länge eines Zyklus der CPU richtet sich nach der benötigten Ausführungsdauer aller Anwenderprogramme. **Mode 2:** Prozessor stellt von Anwenderprogrammen niederer Priorität nicht benötigte Ausführungszeit den Anwenderprogrammen hoher Priorität zur Verfügung. Betriebsart für hohe Verfügbarkeit. **Mode 3:** Prozessor wartet nicht benötige Ausführungszeit von Anwenderprogrammen ab und verlängert so den Zyklus.	Mode 1	
Sollzykluszeit-Modus	Verwendung der *Sollzykluszeit [ms]*. **fest:** Das PES hält die Sollzykluszeit ein und verlängert den Zyklus, falls nötig. Dies gilt nicht, falls die Abarbeitungszeit der Anwenderprogramme die Sollzykluszeit überschreitet. **fest-tolerant:** Wie bei fest, aber beim 1. Aktivierungszyklus des Reload findet die Sollzykluszeit keine Beachtung. **dynamisch-tolerant:** Das PES hält möglichst die *Sollzykluszeit* ein, führt aber den Zyklus in möglichst kurzer Zeit aus.Beim 1. Aktivierungszyklus des Reload findet die *Sollzykluszeit* keine Beachtung.	fest	-

21230587 / DE – 05/2014

Parameter/Schalter	Beschreibung	Standardwert	Einstellung für sicheren Betrieb
Minimale Konfigurationsversion	Aufbau der Konfigurationsdateien und Codegenerierung wie bei der genannten SILworX®-Version (außer bei neueren Funktionen). Mit dieser Einstellung ist die Kompatibilität zu späteren Versionen gesichert.	SILworX V4	-
Maximale Systembus-Latenzzeit [µs]	Für die Sicherheitssteuerung MOVISAFE® HM31 nicht anwendbar!	0 ms	-
safeethernet-CRC	**Aktuelle Version:** Die Bildung des CRC für safeethernet erfolgt mit dem aktuellen Algorithmus.	Aktuelle Version	Applikationsspezifisch

6.4.2 Systemvariablen 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/Schalter	Funktion	Standardwert	Einstellung für sicheren Betrieb
Force-Deaktivierung	Dient zum Verhindern und unmittelbaren Abschalten des Forcens.	FALSE	Applikationsspezifisch
Leer 0 – Leer 16	Keine Funktion.	-	-
NOTAUS 1 – NOTAUS 4	Notausschalter zum Abschalten der Steuerung in von Anwenderprogramm erkannten Störfallen.	FALSE	Applikationsspezifisch
Read-only in RUN	Nach dem Starten der Steuerung ist keine Bedienaktion (Stopp, Start, Download) über SILworX® mehr möglich, Ausnahmen: Forcen und Reload.	FALSE	Applikationsspezifisch
Reload-Deaktivierung	Verhindert ein Laden der Steuerung mittels Reload.	FALSE	Applikationsspezifisch
User-LED 1 – 2	Steuert die entsprechende LED an, sofern vorhanden.	FALSE	Applikationsspezifisch

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

21230587 / DE – 05/2014

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.

6.5 Schutz vor Manipulationen

Der Anwender muss zusammen mit der zuständigen Prüfstelle definieren, welche Maßnahmen zum Schutz vor Manipulation angewendet werden.

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

- Eine Änderung des Anwenderprogramms oder der Konfiguration führt zu einem neuen CRC.
- Die Bedienmöglichkeiten sind abhängig vom Anmelden des Anwenders beim PES.
- Das Programmiertool benötigt für die Verbindung zum PES beim Anmelden des Anwenders ein Passwort.
- Eine Verbindung zwischen PADT und PES ist während des RUN-Betriebs nicht notwendig und kann unterbrochen 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.

HINWEIS

Nur befugtes Personal darf Zugriff auf die Sicherheitssteuerung haben!

Zum Schutz vor unbefugten Änderungen an der Steuerung folgende Maßnahmen ergreifen:

- Standardeinstellungen für Benutzername und Passwort ändern.
- Jeder Benutzer muss sein Passwort geheim halten.
- Das PADT nach Abschluss der Inbetriebnahme von der Steuerung trennen und nur dann erneut verbinden, wenn Änderungen erforderlich sind.

Der Zugang zu Daten des PES ist nur möglich, wenn das verwendete PADT über das Programmiertool und das Anwenderprojekt in der aktuell laufenden Version (Archiv-Pflege!) verfügt.

Die Verbindung zwischen PADT und PES ist nur für den Download des Anwenderprogramms oder für das Auslesen von Variablen notwendig. Während des normalen Betriebs ist das PADT nicht notwendig. Eine Trennung von PADT und PES in der normalen Betriebsphase schützt vor unzulässigen Eingriffen.

21230587 / DE – 05/2014

7 Sicherheitstechnische Aspekte für das Anwenderprogramm

Allgemeiner Ablauf der Programmierung der Sicherheitssteuerung MOVISAFE® HM31 für sicherheitstechnische Anwendungen:

- Spezifikation der Steuerungsfunktion
- Schreiben des Anwenderprogramms
- Kompilieren des Anwenderprogramms mit dem C-Code-Generator
- Zweimaliges Übersetzen des Anwenderprogramms, beide Ergebnisse (CRC) sind zu vergleichen
- Das Programm ist fehlerfrei erzeugt und lauffähig
- Verifikation und Validation

Anschließend kann das PES den sicherheitsgerichteten Betrieb aufnehmen.

7.1 Rahmen für den sicherheitsgerichteten Einsatz

(Vorgaben und Regeln, Erläuterungen zu den Sicherheitsauflagen siehe Kapitel "Sicherheitsauflagen")

Das Anwenderprogramm mit dem zulässigen Programmiertool SILworX® eingeben.

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

Das Programmiertool SILworX® enthält im Wesentlichen:

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

7.1.1 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 (Ablaufsteuerungen)
  - 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, NOTAUS usw.

21230587 / DE – 05/2014

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

7.1.2 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 Ein- und Ausgänge arbeiten generell im Ruhestromprinzip, d. h. ihr sicherer Zustand ist 0. Dies ist bei der Programmierung zu berücksichtigen.
- Das Anwenderprogramm enthält sinnvolle logische und/oder arithmetische Funktionen ohne Rücksicht auf das Ruhestromprinzip der physikalischen Ein- und Ausgänge.
- 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 Ein-/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.

21230587 / DE – 05/2014

7.1.3 Variablendeklaration

Eine Variable ist ein Platzhalter für einen Wert innerhalb der Programmlogik. Über den Variablennamen (max. 31 Zeichen) wird der Speicherplatz mit dem gespeicherten Wert symbolisch adressiert. Eine Variable wird in der Variablendeklaration des Programms oder eines Funktionsbausteins erstellt.

Die Verwendung von symbolischen Namen an Stelle der physikalischen Adresse hat zwei wesentliche Vorteile:

- Im Anwenderprogramm können die Anlagenbezeichnungen von Eingängen und Ausgängen verwendet werden.
- Änderungen der Zuordnung der Variablen zu den Eingangs- und Ausgangskanälen haben keinen Einfluss auf das Anwenderprogramm.

Nicht initialisierte Variable haben nach einem Kalt- oder Warmstart den Initialwert 0 oder FALSE (gilt nicht, wenn sie RETAIN-Attribute haben).

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

7.1.4 Abnahme durch Genehmigungsbehörden

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

7.2 Vorgehensweisen

Dieses Kapitel beschreibt eine typische Vorgehensweise bei der Entwicklung von Anwenderprogrammen für die Sicherheitssteuerung MOVISAFE® HM31.

7.2.1 Zuordnung von Variablen zu Ein-/Ausgängen

Die erforderlichen Testroutinen für die sicherheitsgerichteten Ein- und Ausgänge 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.

7.2.2 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.

21230587 / DE – 05/2014

Zum Verriegeln dienen drei Systemvariablen:

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.

Sind alle drei Systemvariablen ON, dann ist kein Zugriff auf die Steuerung mehr möglich. In diesem Fall kann die Steuerung nur durch Neustart wieder in den Zustand STOPP/GÜLTIGE KONFIGURATION versetzt werden. Dann ist ein Neuladen eines Anwenderprogramms möglich.

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 Eingangsgerät oder der Eingangsbaugruppe ist die Steuerung aufgeschlossen.

7.2.3 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, Ein-/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, Code zweimal erzeugen. Der Konfigurations-CRC muss bei beiden Durchläufen gleich sein.

Code für sicherheitsgerichteten Betrieb erzeugen

1. Codegenerator starten, um Code mit Konfigurations-CRC zu erzeugen.

   Ablauffähiger Code 1 mit CRC 1.
2. Codegenerator erneut starten, um Code mit Konfigurations-CRC zu erzeugen.

   Ablauffähiger Code 2 mit CRC 2.
3. CRC 1 mit CRC 2 vergleichen.

   Beide sind gleich.

Der erzeugte Code ist für den sicherheitsgerichteten Betrieb benutzbar, auch zur Zertifizierung durch Prüfstellen.

21230587 / DE – 05/2014

7.2.4 Laden und Starten des Anwenderprogramms

Der Ladevorgang (Download) eines PES der Sicherheitssteuerung MOVISAFE® HM31 kann nur erfolgen, wenn es zuvor in STOPP gesetzt worden ist.

Anzahl der Anwenderprogramme pro Steuerung
1 – 32

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

HINWEIS

SEW-EURODRIVE 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.

SEW-EURODRIVE empfiehlt eine regelmäßige Datensicherung, auch unabhängig vom Laden des Programms.

7.2.5 Optionale Funktionen Multitasking und Reload

HINWEIS

Die optionalen Funktionen können in MOVISAFE® HM31 ohne Aktivierung für 5000 Betriebsstunden zu Testzwecken verwendet werden. Bei der Verwendung der nicht aktivierten Funktionen leuchtet die System-LED "ERROR" dauerhaft rot.

Nach Ablauf der 5000 Betriebsstunden läuft die Steuerung nicht mehr an.

- Bestellen Sie rechtzeitig die Lizenz zur Freischaltung der benötigten Funktionen.

- **Multitasking:**

  Multitasking bezeichnet die Fähigkeit der Sicherheitssteuerung, bis zu 32 Anwenderprogramme innerhalb des Prozessormoduls abzuarbeiten.

  Dadurch lassen sich Teilfunktionen eines Projekts voneinander trennen. Die einzelnen Anwenderprogramme lassen sich unabhängig voneinander starten, stoppen, laden (auch durch Reload) und löschen.

21230587 / DE – 05/2014

ACHTUNG

Gegenseitige Beeinflussung von Anwenderprogrammen möglich!

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

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

- **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.

HINWEIS

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.

- 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!

HINWEIS

Beim Reload von Actions zu beachten:

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

- 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.

21230587 / DE – 05/2014

7.2.6 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!

Tod oder schwere Körperverletzung möglich.

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

Weitere Informationen finden Sie im Systemhandbuch.

7.2.7 Online-Änderung von Systemparametern

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

Parameter, die online änderbar sind:

- System-Id
- Watchdog-Zeit der Ressource
- Sicherheitszeit
- Sollzykluszeit
- Sollzykluszeit-Modus
- Hauptfreigabe
- Autostart
- Start erlaubt
- Laden erlaubt
- Reload erlaubt
- Globales Forcen erlaubt
- Globale Force Timeout-Reaktion

Vor dem Setzen der Parameter durch ein Online-Kommando ist zu bedenken, ob diese Parameteränderung zu einem gefährlichen Zustand führen kann. Falls nötig, sind organisatorische und/oder technische Maßnahmen zu treffen, um einen Schadensfall zu vermeiden.

Hauptfreigabe erlaubt das Ändern der übrigen Parameter. *Hauptfreigabe* kann nur im Zustand STOPP auf TRUE gesetzt werden.

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

21230587 / DE – 05/2014

7.2.8 Programm-Dokumentation für sicherheitsgerichtete Anwendungen

Das Programmiertool 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 Sicherheitssteuerung, die bereits baumustergeprüft ist.

7.2.9 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 Sicherheitssteuerung, die bereits baumustergeprüft ist.

21230587 / DE – 05/2014

8 Konfiguration der Kommunikation

Neben den physikalischen Eingangs- und Ausgangsvariablen können Variablen auch über eine Datenverbindung mit einem anderen System ausgetauscht werden. Hierzu werden die Variablen der jeweiligen Ressource im Protokolleditor des Programmiertools deklariert. Dieser Datenaustausch kann sowohl lesend als auch schreibend sein.

8.1 Standardprotokolle

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

⚠ WARNUNG

Verwendung unsicherer Importdaten.

Tod oder schwere Körperverletzung!

Die folgenden Standardprotokolle stehen der Sicherheitssteuerung zur Verfügung:

- SNTP Server/Client
- Modbus TCP Master

8.2 Sicherheitsgerichtetes Protokoll (safeethernet)

Die sicherheitsgerichtete Kommunikation über safe**ethernet** ist bis SIL 3 zertifiziert. Die Überwachung der sicherheitsgerichteten Kommunikation ist im safe**ethernet**-Editor zu parametrieren.

HINWEIS

Weitere ausführliche Informationen finden Sie im Systemhandbuch „MOVISAFE® HM31“ im Kapitel „safeethernet“.

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

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

Für sicherheitsgerichtete Funktionen, die über safe**ethernet** 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 einer Variable muss länger als *ReceiveTMO* anstehen oder über Loop-Back überwacht werden, falls jeder Wert übertragen werden soll.

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

21230587 / DE – 05/2014

8.2.1 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 safe**ethernet** Verbindung verhalten sich gemäß dem eingestellten Parameter *Freeze-Daten bei Verbindungsverlust [ms]*.

Für sicherheitsgerichtete Funktionen, die über safe**ethernet** 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 Sicherheitshandbuch Kapitel 8.2.4) ist, muss die *ReceiveTMO* wie folgt berechnet und im safe**ethernet** Editor eingetragen werden:

ReceiveTMO ≥ 4 × Delay + 5 × max. Zykluszeit

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

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

Max. Zykluszeit: maximale Zykluszeit der beiden Steuerungen

HINWEIS

- Eine erwünschte Fehlertoleranz der Kommunikation kann über eine Erhöhung der *ReceiveTMO* erreicht werden, sofern dies für den Anwendungsprozess zeitlich zulässig ist.
- Der maximal zulässige Wert für *ReceiveTMO* hängt vom Anwendungsprozess ab und wird im safe**ethernet**-Editor zusammen mit der maximal zu erwartenden *Response Time* und dem Profil eingestellt.

8.2.2 Response Time

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

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

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

ResponseTime ≤ ReceiveTMO / n

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

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

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

Min. Response Time ≤ ReceiveTMO / 2 ≥ 2 × Delay + 2,5 × max. Zykluszeit

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

21230587 / DE – 05/2014

HINWEIS

- 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!
- Es ist sicherzustellen, dass das Kommunikationssystem die parametrierte *Response-Time* einhält!Für Fälle, in denen dies nicht immer garantiert 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 *ReceiveT-MO*, muss die parametrierte *Response Time* erhöht werden.Die *Receive Timeout* ist der neu parametrierten *Response-Time* anzupassen.
- In den folgenden Beispielen gelten die Formeln für die Berechnung der maximalen Reaktionszeit im Fall einer Verbindung mit der Sicherheitssteuerung nur dann, wenn auf diesen die Sicherheitszeit = 2 × Watchdog-Zeit eingestellt ist.

8.2.3 Maximale Zykluszeit der Sicherheitssteuerung

Zur Bestimmung der maximalen Zykluszeit für eine Sicherheitssteuerung MOVISAFE® HM31 empfiehlt SEW-EURODRIVE die folgende Vorgehensweise.

Maximale Zykluszeit der Sicherheitssteuerung MOVISAFE® HM31 bestimmen:

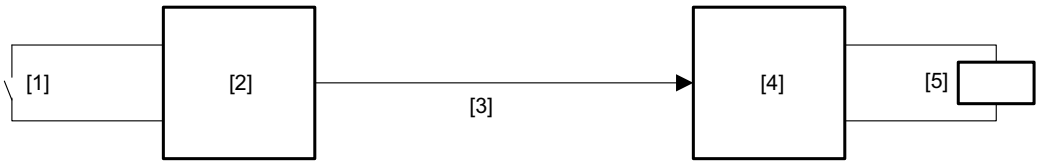
1. System unter voller Last betreiben. Dabei müssen alle Kommunikationsverbindungen in Betrieb sein, sowohl über safe**ethernet** als auch über Standardprotokolle. Die Zykluszeit im Control Panel öfter ablesen, und die maximale Zykluszeit notieren.
2. Schritt 1 für den Kommunikationspartner (zweite Sicherheitssteuerung) wiederholen.
3. Die größere der beiden ermittelten maximalen Zykluszeiten ist die gesuchte maximale Zykluszeit.

Die maximale Zykluszeit ist ermittelt und geht in die nachfolgenden Berechnungen ein.

21230587 / DE – 05/2014

8.2.4 Berechnung der maximalen Reaktionszeit

Die maximale Reaktionszeit T_R (Worst Case) vom Wechsel eines Eingangs des PES 1 bis zur Reaktion des Ausgangs des PES 2 kann wie folgt berechnet werden:



4784751883

[1] Eingang

[2] Sicherheitssteuerung PES 1

[3] Sicherheitsgerichtetes Protokoll

[4] Sicherheitssteuerung PES 2

[5] Ausgang

$T_R = t_1 + t_2 + t_3$

T_R Worst Case Reaction Time

t_1 2 × Watchdog-Zeit der Sicherheitssteuerung 1

t_2 ReceiveTMO

t_3 2 × Watchdog-Zeit der Sicherheitssteuerung 2

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

8.2.5 Begriffe

Begriff	Beschreibung
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 Zustands eines physikalischen Eingangs einer Steuerung 1 bis zur Änderung des physikalischen Ausgangs einer Steuerung 2.

21230587 / DE – 05/2014

8.2.6 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.

21230587 / DE – 05/2014

9 Anhang

9.1 Glossar

Begriff	Beschreibung
DC-24V	Die Sicherheitssteuerung verfügt über folgende DC-24-V-Eingangsspannungspotenziale: 24V_CU: DC-24V-Eingang – Steuerung 24V_L: DC-24V-Eingang – Last 24V_S: DC-24V-Eingang – Sensorversorgung Bezugspotenzial: 0V24
ARP	Address Resolution Protocol (Netzwerkprotokoll zur Zuordnung von Netzwerkadressen zu Hardware-Adressen)
BS	Betriebssystem
BL	Boot-Loader
BWS	Berührungslos Wirkende Schutzeinrichtung
COM	Kommunikationsmodul
COE	CANopen-Softwaremodul
CRC	Cyclic Redundancy Check (Prüfsumme)
CUT	Com-User Task
DCS	Distributed Control System (Prozessleitsystem)
DI	Digital Input (Binäreingang)
DO	Digital Output (Binärausgang)
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Norm
ESD	Electrostatic Discharge (elektrostatische Entladung)
FB	Feldbus-Schnittstelle der Steuerung
FBS	Funktionsbausteinsprache
FIFO	First In First Out (Datenspeicher)
FTA	Field Termination Assembly
FTZ	Fehlertoleranzzeit
ICMP	Internet Control Message Protocol (Netzwerkprotokoll für Status- und Fehlermeldungen)
IEC	Internationale Normen für die Elektrotechnik
IF	InterFace
MAC-Adresse	Hardware-Adresse eines Netzwerkanschlusses (Media Access Control)
PADT	Programming and Debugging Tool (gemäß IEC 61131-3), PC mit SILworX®
NVRAM	Non Volatile Random Access Memory, nicht-flüchtiger Speicher

21230587 / DE – 05/2014

Begriff	Beschreibung
PE	Protective Earth (Schutzerde)
PELV	Protective Extra Low Voltage (Funktionskleinspannung mit sicherer Trennung)
PES	Programmierbares elektronisches System
POE	Programm-Organisationseinheiten (gemäß IEC 61131-1)
PFD	Probability of Failure on Demand (Wahrscheinlichkeit eines Fehlers bei Anforderung einer Sicherheitsfunktion)
PFF-HM31A	Sicherheitssteuerung
PFH	Probability of Failure per Hour (Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
R	Read (Systemvariable liefert Wert, z. B. an Anwenderprogramm)
Rückwirkungsfrei	Es seien zwei Eingangsschaltungen an dieselbe Quelle (z. B. Transmitter) angeschlossen. Dann wird eine Eingangsschaltung rückwirkungsfrei genannt, wenn sie die Signale der anderen Eingangsschaltung nicht verfälscht.
R/W	Read/Write (Spaltenüberschrift für Art von Systemvariable)
SB	Systembus (-modul)
SELV	Safety Extra Low Voltage (Schutzkleinspannung)
SFF	Safe Failure Fraction (Anteil der sicher beherrschbaren Fehler)
SIL	Safety Integrity Level (gemäß IEC 61508)
SILworX®	Programmierwerkzeug für Sicherheitssteuerung PFF-HM31A
SNTP	Simple Network Time Protocol (RFC 1769)
S.R.S	System.Rack.Slot (Adressierung eines Moduls)
SW	Software
S&R	Send und Receive; im Zusammenhang mit TCP-Protokoll
TMO	Timeout
W	Write (Systemvariable wird mit Wert versorgt, z. B. vom Anwenderprogramm)
Watchdog (WD)	Zeitüberwachung für Module oder Programme. Bei Überschreiten der Watchdog-Zeit geht das Modul oder Programm in den Fehlerstopp.
WDZ	Watchdog-Zeit

21230587 / DE – 05/2014

Stichwortverzeichnis

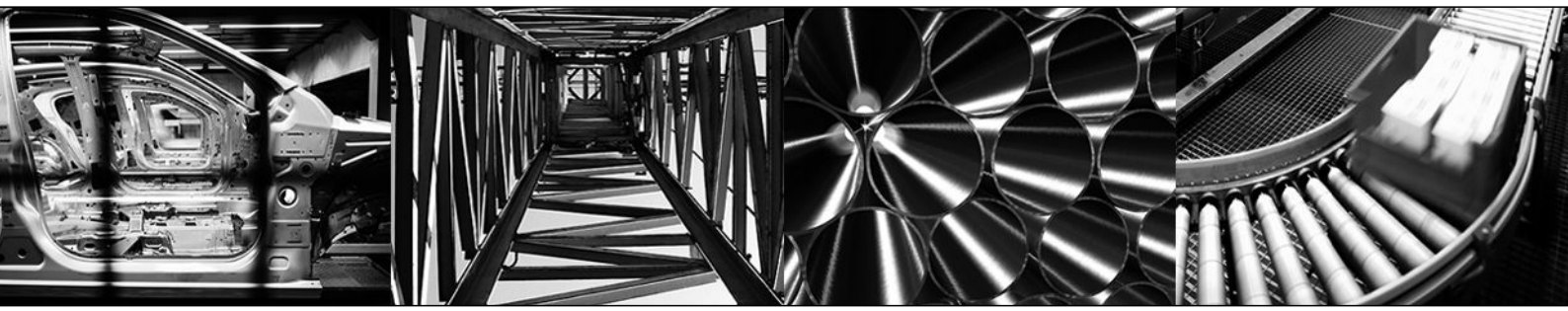
21230587 / DE – 05/14

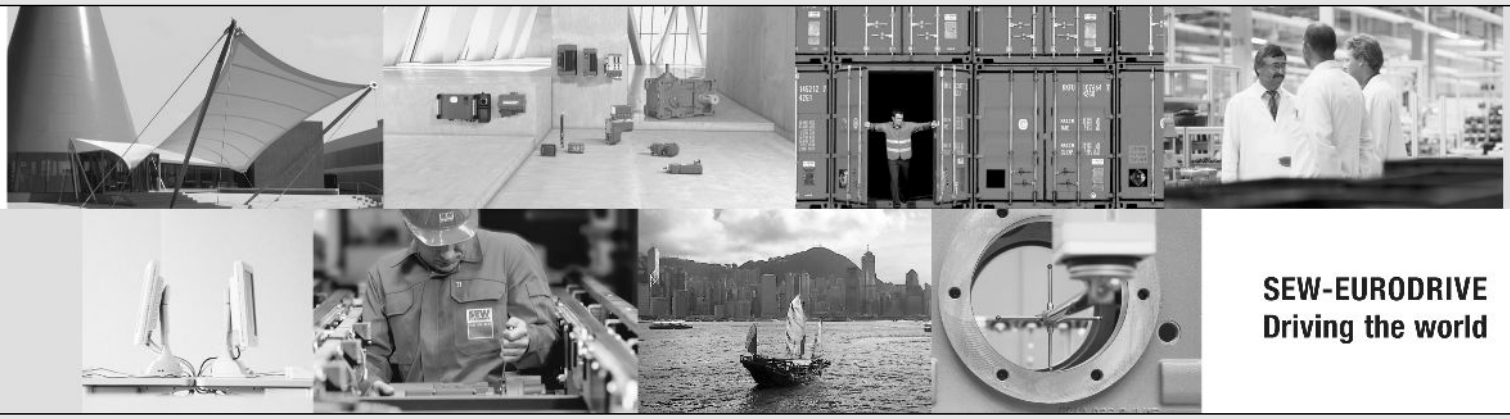
T

W

Z

21230587 / DE – 05/14





SEW-EURODRIVE
Driving the world

SEW-EURODRIVE GmbH & Co KG
P.O. Box 3023
76642 BRUCHSAL
GERMANY
Phone +49 7251 75-0
Fax +49 7251-1970
sew@sew-eurodrive.com
➞ **www.sew-eurodrive.com**