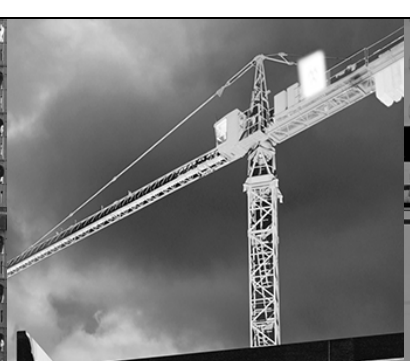
SEW EURODRIVE

Systemhandbuch

Dezentrale Sicherheitssteuerung PFF-HM31A für **MOVIPRO®**

Ausgabe 05/2012

19419600/ DE




KKFU 144794 3
42G1

Inhaltsverzeichnis

1 Allgemeine Hinweise

Dieses Handbuch enthält Informationen für den bestimmungsgemäßen Gebrauch der Sicherheitssteuerung.

Voraussetzung für die gefahrlose 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 Systemhandbuch enthält folgende Themen:

- Allgemeine Hinweise
- Systemeigenschaften
- Kommunikation
- Safeethernet
- Modbus TCP/UDP
- Com-User Task (CUT)
- Betriebssystem
- Anwenderprogramm
- Inbetriebnahme
- Betrieb
- Instandhaltung

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.

1.3 Darstellungskonventionen

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

Schreibweise	Bedeutung
Fett	Hervorhebung wichtiger Textteile.
[...]	Bezeichnungen von Schaltflächen und Menübefehlen im Programmierwerkzeug, auf die Sie klicken können.
Kursiv	Parameter und Systemvariablen.
`Courier`	Wörtliche Benutzereingaben.
RUN	Bezeichnungen von Betriebszuständen in Großbuchstaben.

1.4 Aufbau der Sicherheitshinweise

1.4.1 Bedeutung der Signalworte

Die folgende Tabelle zeigt die Abstufung und Bedeutung der Signalworte für Sicherheitshinweise, Warnungen vor Sachschäden und weitere Hinweise.

Signalwort	Bedeutung	Folgen bei Missachtung
⚠ **GEFAHR!**	Unmittelbar drohende Gefahr	Tod oder schwere Körperverletzungen
⚠ **WARNUNG!**	Mögliche, gefährliche Situation	Tod oder schwere Körperverletzungen
⚠ **VORSICHT!**	Mögliche, gefährliche Situation	Leichte Körperverletzungen
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 Sicherheitshinweise

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

Hier sehen Sie den formalen Aufbau eines abschnittsbezogenen Sicherheitshinweises:

⚠ SIGNALWORT!

Art der Gefahr und ihre Quelle.

Mögliche Folge(n) der Missachtung.

- Maßnahme(n) zur Abwendung der Gefahr.

1.4.3 Aufbau der eingebetteten Sicherheitshinweise

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

Hier sehen Sie den formalen Aufbau eines eingebetteten Sicherheitshinweises:

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

  Mögliche Folge(n) der Missachtung.

  – Maßnahme(n) zur Abwendung der Gefahr.

1.5 Mängelhaftungsansprüche

Die Einhaltung der Dokumentation ist die Voraussetzung für den störungsfreien Betrieb und die Erfüllung eventueller Mängelhaftungsansprüche. Lesen Sie deshalb zuerst die Dokumentation, bevor Sie mit dem Gerät arbeiten!

1.6 Haftungsausschluss

Die Beachtung der Dokumentation ist Grundvoraussetzung für den sicheren Betrieb und für das Erreichen der angegebenen Produkteigenschaften und Leistungsmerkmale. Für Personen-, Sach- oder Vermögensschäden, die wegen Nichtbeachtung der Betriebsanleitung entstehen, übernimmt SEW-EURODRIVE keine Haftung. Die Sachmängelhaftung ist in solchen Fällen ausgeschlossen.

1.7 Mitgeltende Unterlagen

Beachten Sie die folgenden mitgeltenden Unterlagen:

- Betriebsanleitung "Dezentrale Sicherheitssteuerung PFF-HM31A für MOVIPRO®"
- Sicherheitshandbuch "Dezentrale Sicherheitssteuerung PFF-HM31A für MOVIPRO®"
- Praxis der Antriebstechnik - EMV in der Antriebstechnik

Wenn Sie die CUT-Funktionalität nutzen möchten, beachten Sie zusätzlich die folgenden mitgeltenden Unterlagen:

- Handbuch "Com-User Task für PFF-HM31A"
- Handbuch "MOVIVISION® Parameter- und Diagnosetool Version 2.0"

Sie benötigen Software, die **nicht** im Lieferumfang ist. Sie können die Software zusammen mit der Dokumentation auf einem Datenträger (CD/DVD) von SEW-EURODRIVE unter folgenden Bestellangaben beziehen:

Bezeichnung	Sachnummer
SILWorX für PFF-HM31A • Hardware: SILWorX Lizenz Dongle • Software: SILWorX ab 4.64.0	1 950 011 4
Motion Library PFF-HM31 Bausteinbibliothek für die sichere Wegmessung /Function block library for safety related position detection	1 710 640 0

Beachten Sie darüber hinaus die mitgeltenden Unterlagen in Abhängigkeit zu der angeschlossenen Antriebstechnik

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

1.8 Urheberrechtsvermerk

1.9 Produktnamen und Marken

Die in dieser Dokumentation genannten Produktnamen sind Marken oder eingetragene Marken der jeweiligen Titelhalter.

2 Systemeigenschaften

Die Sicherheitssteuerung enthält in einem Gehäuse ein sicherheitsgerichtetes Prozessorsystem, eine Anzahl Eingänge und Ausgänge sowie Kommunikationsanschlüsse.

Details entnehmen Sie der Betriebsanleitung "Dezentrale Sicherheitssteuerung PFF-HM31A für MOVIPRO®".

2.1 Überwachung der Betriebsspannung

Das Gerät überwacht die Spannung 24 VDC während des Betriebs. Reaktionen erfolgen entsprechend der aufgelisteten Spannungspegel:

Spannungspegel	Reaktion der Geräte
DC 24 V -20% / +25% (19.2 V – 30 V)	Normalbetrieb
< 18,0 V (softwareseitig ausgelesene Spannung auf der Platine)	Alarmzustand (interne Variable werden beschrieben und an die Eingänge und Ausgänge gegeben)
< 12,0 V (softwareseitig ausgelesene Spannung auf der Platine)	Abschaltung der Eingänge und Ausgänge

Die Systemvariable Stromversorgungszustand erlaubt es, den Zustand der Betriebsspannung mit dem Programmierwerkzeug oder im Anwenderprogramm auszuwerten.

2.2 Überwachung des Temperaturzustandes

Die Temperatur wird durch Sensoren an relevanten Stellen im Innern des Gerätes oder des Systems gemessen und softwareseitig ausgegeben.

Diese hat einen Delta-Betrag zu der Umgebungstemperatur, welcher von vielen Faktoren abhängt. Bei definierten Temperaturen (zwei Schaltschwellen) der Platine geht die Sicherheitssteuerung in den sicheren Zustand über.

Überschreitet die geräteintern gemessene Temperatur die definierten Schaltschwellen, ändert sich der Wert der Systemvariable "Temperaturzustand" wie folgt:

Temperatur (geräteintern)	Temperaturbereich	Temperaturzustand [BYTE]
< 60 °C	Normal	0x00
60 °C…70 °C	Hohe Temperatur	0x01
> 70 °C	Sehr hohe Temperatur	0x03
Rückkehr auf 64 °C – 54 °C[1)]	Hohe Temperatur	0x01
Rückkehr auf < 54 °C[1)]	Normal	0x00

1) Die Sensoren haben eine Hysterese von 6 °C.

Bei mangelnder oder fehlender Luftzirkulation und nicht ausreichender Eigenkonvektion kann die Schwelle zum Bereich "Hohe Temperatur" in der Sicherheitssteuerung schon bei Umgebungstemperaturen < 35 °C ansprechen. Ursachen können lokale Erwärmungen oder eine ungünstige Wärmeableitung sein. Insbesondere bei digitalen Ausgängen ist die Erwärmung stark von der Belastung abhängig. Die Systemvariable Temperaturzustand ermöglicht dem Anwender die interne Temperatur auszulesen.

HINWEIS

Der Übergang in den Zustand hohe Temperatur oder sehr hohe Temperatur bedeutet nicht, dass die Sicherheit des Systems beeinträchtigt ist.

2.3 Alarm- und Ereignisaufzeichnung

Die Sicherheitssteuerung verfügt über die Fähigkeit, Alarme und Ereignisse aufzuzeichnen (Sequence of Events Recording, SER).

2.3.1 Alarme und Ereignisse

Ereignisse sind Änderungen des Zustands von Anlage oder Steuerung, die mit einem Zeitstempel versehen sind.

Alarme sind solche Ereignisse, die eine Erhöhung des Gefahrenpotentials signalisieren.

Die Sicherheitssteuerung zeichnet als Ereignisse die Zustandsänderungen zusammen mit dem Zeitpunkt ihres Auftretens auf.

Die Sicherheitssteuerung unterscheidet boolesche und skalare Ereignisse.

Boolesche Ereignisse:

- Änderungen von Booleschen Variablen, z. B. von digitalen Eingängen.
- Alarm- und Normalzustand, diese sind den Zuständen der Variablen beliebig zuzuordnen

Skalare Ereignisse:

- Übergänge über Grenzwerte, die für eine skalare Variable definiert sind.
- Skalare Variable haben einen numerischen Datentyp, z. B. INT, REAL.
- Es sind zwei obere und zwei untere Grenzen möglich.
- Für die Grenzwerte muss gelten:

  Oberste Grenze = obere Grenze = Normalbereich = untere Grenze = unterste Grenze.
- Eine Hysterese kann in folgenden Fällen wirken:
  - Bei Unterschreitung einer oberen Grenze.
  - Bei Überschreitung einer unteren Grenze.

Die Angabe einer Hysterese vermeidet eine unnötig große Menge an Ereignissen, wenn die globale Variable stark um einen Grenzwert schwankt.

Die Sicherheitssteuerung kann nur dann Ereignisse bilden, wenn diese in SILworX definiert sind, siehe Kapitel "Konfigurieren von Alarmen und Ereignissen". Bis zu 4 000 Alarme und Ereignisse sind definierbar.

2.3.2 Bildung von Ereignissen

Das Prozessorsystem ist in der Lage, Ereignisse zu bilden. Das Prozessorsystem bildet die Ereignisse aus globalen Variablen und legt sie im Puffer ab, siehe "Aufzeichnung von Ereignissen". Die Ereignisbildung findet im Zyklus des Anwenderprogramms statt. Jedes gelesene Ereignis kann durch ein neu aufgetretenes Ereignis überschrieben werden.

Systemereignisse:

Außer den Ereignissen, die Änderungen von globalen Variablen oder Eingangssignalen registrieren, bilden die Prozessorsysteme folgende Arten von Systemereignissen:

- Überlauf: Es sind infolge von Pufferüberlauf Ereignisse nicht gespeichert worden. Der Zeitstempel des Überlauf-Ereignisses entspricht dem des Ereignisses, das den Überlauf erzeugt hat.
- Init: Der Ereignispuffer wurde initialisiert.

Systemereignisse enthalten die SRS-Identifikation des Geräts, das sie ausgelöst hat. Statusvariable stellen dem Anwenderprogramm den Ereigniszustand skalarer Ereignisse zur Verfügung. Jedem der folgenden Zustände kann als Statusvariable eine globale Variable vom Typ BOOL zugeordnet sein:

- Normal.
- Untere Grenze unterschritten.
- Unterste Grenze unterschritten. Obere Grenze überschritten.
- Oberste Grenze überschritten.

Die zugeordnete Statusvariable wird TRUE, wenn der betreffende Zustand erreicht ist.

2.3.3 Aufzeichnung von Ereignissen

Das Prozessorsystem sammelt die Ereignisse: Das Prozessorsystem speichert alle Ereignisse in seinem Puffer. Der Puffer ist im nichtflüchtigen Speicher angelegt und fasst 1000 Ereignisse. Ist der Puffer voll, werden keine neuen Ereignisse gespeichert, bis weitere Ereignisse gelesen und dadurch zum Überschreiben markiert wurden.

2.3.4 Weitergabe von Ereignissen

Die Ereignisse können über das MODBUS-Protokoll zur Antriebssteuerung (Beck-PC) oder über safeethernet zur übergeordneten Sicherheitssteuerung übertragen werden. Hierfür müssen zuvor im Anwenderprogramm die entsprechenden Variablen verknüpft werden. Die erweiterte Diagnose erfolgt über das PADT (SILworX).

3 Kommunikation

Die Sicherheitssteuerungen kommuniziert unter Nutzung folgender Protokolle:

- safeethernet

  Sicherheitsgerichtetes Protokoll für die Kommunikation der Steuerungen untereinander
- Feldbusprotokoll Modbus TCP/UDP für den Anschluss externer Geräte oder Systeme
- Kommunikation mit dem Programmiergerät

Das Kommunikationssystem ist an das sicherheitsgerichtete Prozessorsystem angeschlossen.

Es ist mit den Feldbus-Schnittstellen über ein Dual-Port-RAM an das sichere Mikroprozessorsystem angebunden. An die Schnittstellen dürfen nur Geräte angeschlossen werden, die eine sichere elektrische Trennung gewährleisten.

Das Kommunikationssystem steuert die Kommunikation der Steuerung mit anderen Systemen über leistungsfähige Schnittstellen:

Verfügbare Protokolle

Die folgenden Protokolle sind verfügbar:

Protokoll	Schnittstellen	Aktivierung
safeethernet	Ethernet	Funktion ist bei der Geräteoption PFF-HM31A1-E61-I111-00/000/000 standardgemäß freigeschaltet.
SNTP Server/Client	Ethernet	
Modbus TCP Master	Ethernet	
Com-User Task	CAN (X4111_1/2) RS485 (X4011)	

Optionale Protokolle

Die folgenden Protokolle sind auf Anfrage als Geräteoption verfügbar:

Protokoll	Schnittstellen	Aktivierung
Modbus TCP Slave	Ethernet	Auf Anfrage wird eine neue Geräteoption generiert in der das gewünschte Protokoll freigeschaltet ist.
TCP Send/Receive		
PROFINET IO Controller		
PROFINET IO Device		
OPC Server (läuft auf Host-PC)		

HINWEIS

Die optionalen Protokolle können in der Geräteoption PFF-HM31A1-E61-I111-00/000/000 ohne Aktivierung für 5000 Betriebsstunden zu Testzwecken verwendet werden. Bei der Verwendung der nicht aktivierten Protokollen leuchtet die System-LED "ERROR" dauerhaft rot.

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

- Bestellen Sie rechtzeitig die Geräteoption mit den benötigten Protokollen.

3.1 Ethernet

Die Sicherheitssteuerung enthält einen Ethernet-Switch mit Anschlüssen. Über diese Anschlüsse können mithilfe von Ethernet-Kabeln andere Geräte mit der Steuerung verbunden werden.

Es stehen die folgenden Schnittstellen zur Verfügung:

- **2 Ethernet-Schnittstellen:** X4233_1 und X4233_2

  Die beiden Schnittstellen befinden sich auf der Anschlussleiste des Geräts

- **1 Ethernet-Service-Schnittstelle:** X4223

  Zum Anschluss eines Programmiergeräts (PADT)

Switch

- Ein Switch ist im Gegensatz zu einem Hub in der Lage, Datenpakete zu analysieren und kurzfristig zu speichern, um dann eine zeitweilige gezielte Verbindung zwischen zwei Kommunikationspartnern (Sender/Empfänger) für die Übertragung der Daten aufzubauen. Dadurch werden die bei einem Hub üblichen Kollisionen vermieden und das Netzwerk entlastet. Zur gezielten Weiterleitung der Daten benötigt jeder Switch eine Adress-/Port-Zuordnungstabelle. Diese Tabelle wird in einem Selbstlernprozess vom Switch automatisch generiert. In ihr sind MAC-Adressen einem bestimmten Port im Switch zugeordnet. Eingehende Datenpakete werden anhand dieser Tabelle an den entsprechenden Port direkt weitergeleitet.
- Der Switch schaltet automatisch um sowohl zwischen den Übertragungsraten 10 und 100 MBit/s als auch zwischen Voll- und Halbduplex-Verbindungen. Damit steht in jeder Richtung der Datenübertragung die volle Bandbreite zur Verfügung (Vollduplexbetrieb).
- Ein Switch regelt die Kommunikation zwischen verschiedenen Endgeräten. Der Switch kann dabei bis zu 1000 absolute MAC-Adressen ansprechen.
- Autocrossing erkennt den Anschluss von Kabeln mit gekreuzten Adern, und der Switch stellt sich automatisch darauf ein.

HINWEIS

Bei der Konfiguration der sicherheitsgerichteten Kommunikation sind die Hinweise im Sicherheitshandbuch zu beachten.

3.1.1 SNTP - Protokoll

Mit dem SNTP-Protokoll (Simple Network Time Protocol) wird über Ethernet die Uhrzeit der SNTP-Clients durch den SNTP-Server synchronisiert. Die Sicherheitssteuerung kann als SNTP-Server und/oder als SNTP-Client konfiguriert und eingesetzt werden.

Es gilt der SNTP Standard nach RFC 2030 (SNTP-Version 4) mit der Einschränkung, dass nur der Unicast-Modus unterstützt wird.

- Die Funktion ist standardgemäß freigeschaltet.
- Als Übertragungsstandard für das Netzwerk ist Ethernet 10/100/-BaseT erforderlich.

SNTP-Client

Der SNTP-Client benutzt zu seiner Zeitsynchronisation immer nur den erreichbaren SNTP-Server mit der höchsten Priorität.

In jeder Ressource kann ein SNTP-Client zur Zeitsynchronisation konfiguriert werden.

HINWEIS

Zeitsynchronisation einer Sicherheitssteuerung durch eine andere Sicherheitssteuerung.

Wird ein SNTP-Client auf einer Sicherheitssteuerung eingerichtet, so wird der interne SNTP-Server der Sicherheitssteuerung abgeschaltet.

Um weiterhin eine Zeitsynchronisation einer Sicherheitssteuerung durch eine andere Sicherheitssteuerung zu gewährleisten, muss auf dem Kommunikationsmodul, mit welchem die Remote I/O verbunden ist, ein SNTP-Server eingerichtet werden.

So legen Sie einen neuen SNTP-Client an:

1. Im Strukturbaum [Konfiguration] / [Ressource] / [Protokolle] öffnen.
2. Rechtsklick auf Protokolle und im Kontextmenü [Neu] / [SNTP-Client] wählen.

   Ein neuer SNTP-Client wird hinzuzugefügt.
3. Im Kontextmenü von [SNTP-Client] / [Eigenschaften] das COM-Modul auswählen.

Das Dialogfenster des SNTP-Client enthält die folgenden Parameter:

Parameter	Beschreibung
Typ	SNTP-Client
Name	Name für den SNTP-Client maximal 32 Zeichen.
Modul	Auswahl des CPU- oder COM-Moduls, auf dem dieses Protokoll abgearbeitet wird.
Verhalten bei CPU/COM Verbindungsverlust	Bei Verbindungsverlust des Prozessormoduls zum Kommunikationsmodul werden in Abhängigkeit dieses Parameters die Eingangsvariablen entweder initialisiert oder unverändert im Prozessormodul verwendet. (z. B. wenn Kommunikationsmodul bei laufender Kommunikation gezogen wird). **Initialdaten annehmen:** Eingangsvariablen werden auf die Initialwerte zurückgesetzt. **Letzten Wert beibehalten**: Eingangsvariablen behalten den letzten Wert.
Max. µP-Budget aktivieren	Wird vom Betriebssystem des Moduls nicht berücksichtigt. Parameter wurde wegen der CRC- und Reload-Stabilität erhalten.
Max. µP-Budget in [%]	Wird vom Betriebssystem des Moduls nicht berücksichtigt. Parameter wurde wegen der CRC- und Reload-Stabilität erhalten.
Beschreibung	Beliebige eindeutige Beschreibung für den SNTP
Aktuelle SNTP-Version	Anzeige der aktuellen SNTP Version.
Referenz Stratum	Das Stratum eines SNTP-Clients gibt die Genauigkeit seiner lokalen Zeit wieder. Je niedriger das Stratum, desto genauer ist seine lokale Zeit. Null bedeutet ein unspezifiziertes oder nicht verfügbares Stratum (nicht gültig). Der aktuell verwendete SNTP-Server eines SNTP-Clients ist der, welcher erreichbar ist und die höchste Priorität besitzt. Ist das Stratum des aktuellen SNTP-Servers kleiner als das des SNTP-Clients, so übernimmt die Ressource die Zeit des aktuellen SNTP-Servers. Ist das Stratum des aktuellen SNTP-Servers größer als das des SNTP-Clients, so übernimmt die Ressource die Zeit des aktuellen SNTP-Servers nicht. Ist das Stratum des aktuellen SNTP-Servers gleich dem des SNTP-Clients, so sind zwei Fälle zu unterscheiden: • Wenn der SNTP-Client (Ressource) ausschließlich als SNTP-Client arbeitet, so übernimmt die Ressource die Zeit des aktuellen SNTP-Servers. • Wenn der SNTP-Client (Ressource) gleichzeitig auch als SNTP-Server arbeitet, wird pro Anfrage des SNTP-Clients die Hälfte der Zeitdifferenz zum aktuellen SNTP-Server auf der Ressource übernommen (Zeit nähert sich langsam an). Wertebereich: 16 s – 16384 s (Standardwert: 16 s)
Client Zeitanfrage Intervall [s]	Zeitintervall, in dem die Zeitsynchronisation durch den aktuellen SNTP-Server erfolgt. Das Client-Zeitanfrage-Intervall im SNTP-Client muss größer sein als das Timeout im SNTP-Server. Wertebereich: 16 s – 16384 s (Standardwert: 16 s)

SNTP-Client (Server Info)

In der SNTP-Server Info wird die Verbindung zu einem SNTP-Server konfiguriert. Unterhalb eines SNTP-Clients können 1 bis 4 SNTP-Server Infos konfiguriert werden.

So legen Sie einen neuen SNTP- Server Info an:

1. Im Strukturbaum [Konfiguration] / [Ressource] / [Protokolle] / [SNTP Client] öffnen.
2. Rechtsklick auf Protokolle und im Kontextmenü [Neu] / [SNTP-Server Info] wählen.

   Eine neue SNTP-Server Info wird hinzuzugefügt.
3. Im Kontextmenü von [SNTP-Server Info] / [Eigenschaften] das COM-Modul auswählen.

Das Dialogfenster der SNTP-Server Info enthält die folgenden Parameter:

Parameter	Beschreibung
Typ	SNTP-Server-Info
Name	Name für die SNTP-Server-Info. Maximal 31 Zeichen.
Beschreibung	Beschreibung für den SNTP-Server. Maximal 31 Zeichen.
IP-Adresse	IP-Adresse der Ressource oder des PCs, auf dem der SNTP-Server konfiguriert ist. Standardwert: 0.0.0.0
SNTP-ServerPriorität	Priorität mit welcher der SNTP-Client diesen SNTP-Server behandelt. Die für einen SNTP-Client konfigurierten SNTP-Server sollten unterschiedliche Prioritäten besitzen. Wertebereich: 0 (geringste Priorität) bis 4294967295 (höchste Priorität) Standardwert: 1s
SNTP-ServerTimeout [s]	Der Timeout im SNTP-Server muss kleiner eingestellt sein als das Zeitanfragenintervall im SNTP-Client. Wertebereich: 1 s – 16384 s Standardwert: 1 s

SNTP-Server

Der SNTP-Server nimmt die Anforderung von einem SNTP-Client entgegen und sendet seine aktuelle Zeit an den SNTP-Client zurück.

So legen Sie einen neuen SNTP-Server an:

1. Im Strukturbaum [Konfiguration] / [Ressource] / [Protokolle] öffnen.
2. Rechtsklick auf [Protokolle] und im Kontextmenü [Neu] / [SNTP-Server] wählen.

   Ein neuer SNTP Server wird hinzuzugefügt.
3. Im Kontextmenü von [SNTP Server] / [Eigenschaften] das COM-Modul auswählen.

Das Dialogfenster des SNTP-Client enthält die folgenden Parameter:

Parameter	Beschreibung
Typ	SNTP-Client
Name	Name für den SNTP-Client maximal 31 Zeichen.
Modul	Auswahl des CPU- oder COM-Moduls, auf dem dieses Protokoll abgearbeitet wird.
Max. µP-Budget aktivieren	**Aktiviert:** Limit des µP-Budget aus dem Feld Max. µP-Budget in [%] übernehmen. **Deaktiviert:** Kein Limit des µP-Budget, für dieses Protokoll verwenden.
Max. µP-Budget in [%]	Maximale µP-Last des Moduls, welche bei der Abarbeitung des Protokolls produziert werden darf. Wertebereich: 1 – 100 % Standardwert: 30 %
Verhalten bei CPU/COM Verbindungsverlust	Bei Verbindungsverlust des Prozessormoduls zum Kommunikationsmodul werden in Abhängigkeit dieses Parameters die Eingangsvariablen entweder initialisiert oder unverändert im Prozessormodul verwendet. (z. B. wenn Kommunikationsmodul bei laufender Kommunikation gezogen wird). **Initialdaten annehmen:** Eingangsvariablen werden auf die Initialwerte zurückgesetzt. **Letzten Wert beibehalten**: Eingangsvariablen behalten den letzten Wert.
Beschreibung	Beliebige eindeutige Beschreibung für den SNTP
Aktuelle SNTP-Version	Anzeige der aktuellen SNTP Version.
Stratum des Zeitservers	Das Stratum eines SNTP-Clients gibt die Genauigkeit seiner lokalen Zeit wieder. Je niedriger das Stratum, desto genauer ist seine lokale Zeit. Null bedeutet ein unspezifiziertes oder nicht verfügbares Stratum (nicht gültig). Das Stratum des SNTP-Servers muss niedriger oder gleich dem Stratum des anfragenden SNTP-Clients sein. Ansonsten wird die Zeit des SNTP-Servers vom SNTP-Client nicht übernommen. Wertebereich: 1 – 15 Standardwert: 14

3.2 Kommunikation mit dem Programmierwerkzeug

Die Kommunikation der Sicherheitssteuerung mit einem PADT erfolgt über Ethernet. Ein PADT ist ein PC / Laptop, auf dem das Programmierwerkzeug SILworX installiert ist.

Es ist möglich, dass eine Steuerung gleichzeitig mit bis zu 5 PADTs kommuniziert. Dabei kann jedoch nur ein Programmierwerkzeug schreibend auf die Steuerung zugreifen. Alle übrigen können nur Informationen auslesen. Bei jedem weiteren Versuch, eine schreibende Verbindung aufzubauen, erteilt die Steuerung nur einen lesenden Zugriff.

4 safeethernet

Die Sicherheitssteuerung ist safeethernet-fähig. Sie kann sicherheitsgerichtet gemäß SIL 3 über Ethernet (100 Mbit/s) kommunizieren.

Die Ethernet-Schnittstellen der Sicherheitssteuerung sind simultan auch für andere Protokolle nutzbar.

Die safeethernet Kommunikation zwischen den Steuerungen kann über verschiedene Ethernet-Netzwerktopologien erfolgen. Passen Sie die Parameter des safeethernet Protokolls an das verwendete Ethernet-Netzwerk an, um Geschwindigkeit und Effizienz des Datentransfers zu erhöhen.

Diese Parameter können mit Hilfe so genannter Netzwerkprofile eingestellt werden. Diewerkseitige Einstellung der Parameter stellt die Kommunikation sicher, ohne dass sich derAnwender zunächst in Details der Netzwerkkonfiguration einarbeiten muss.

HINWEIS

Das safeethernet Protokoll ist sicherheitsgerichtet und TÜV zertifiziert bis SIL 3 gemäß IEC 61508.

safeethernet-Eigenschaften

Element	Eigenschaften	Beschreibung
Benötigtes Modul/Steuerung	Integriertes Prozessormodul der Steuerung	safeethernet wird auf dem sicherheitsgerichteten Prozessormodul ausgeführt.
Ethernet-Schnittstellen	100 Mbit/s	Die verwendeten Ethernet-Schnittstellen sind simultan auch für andere Protokolle nutzbar.
Verbindungen	128	safeethernet-Verbindungen
Redundante Verbindungen:	128	2 Kanal Betrieb Redundante safeethernet Verbindungen zwischen Steuerungen sind im safeethernet-Editor einstellbar.
Redundante Transportwege	Einschränkung da nur ein Gerät	Redundante safeethernet Transportwege
Prozessdatenmenge pro Verbindung	1100 Bytes	pro safeethernet Verbindung.

4.1 Was ist safeethernet?

Im Bereich der Prozess- und Automatisierungstechnik sind Anforderungen wie Determinismus, Zuverlässigkeit, Austauschbarkeit, Erweiterbarkeit und vor allem Sicherheit zentrale Themen.

safeethernet ist ein Übertragungsprotokoll zur Übertragung von sicherheitsgerichteten Daten bis SIL 3 auf Basis der Ethernet-Technologie.

safeethernet beinhaltet Mechanismen, die folgende Fehler erkennen und darauf sicherheitsgerichtet reagieren:

- Verfälschung von übertragenen Daten (doppelte, verlorene, geänderte Bits)
- Falsche Adressierung von Nachrichten (Sender, Empfänger)
- Falsche Reihenfolge von Daten (Wiederholung, Verlust, Tausch)
- Falsches Zeitverhalten (Verzögerung, Echo)

safeethernet basiert auf dem Standard IEEE 802.3.

safeethernet verwendet „unsichere Datenübertragungskanäle“ (Ethernet) nach dem Black-Channel-Prinzip und überwacht sie bei Sender und Empfänger durch sicherheitsgerichtete Protokollmechanismen. Dadurch sind Ethernet-Netzwerkkomponenten wie Hubs, Switches, Router innerhalb eines sicherheitsgerichteten Netzwerkes verwendbar.

safeethernet nutzt die Fähigkeiten von Standard Ethernet in der Form, dass Sicherheit und Echtzeitfähigkeit ermöglicht werden. Ein spezieller Protokollmechanismus garantiert ein deterministisches Verhalten auch bei Ausfall oder Eintritt von Kommunikationsteilnehmern. Das System bindet neue Komponenten in das laufende System dann automatisch ein. Alle Komponenten eines Netzwerkes sind während des laufenden Betriebs austauschbar. Mit dem Einsatz von Switches lassen sich Übertragungszeiten klar definieren. Somit wird Ethernet echtzeitfähig.

Verbindungen zum firmeninternen Intranet als auch Verbindungen zum Internet sind mit safeethernet möglich. Damit ist nur noch ein Netzwerk für sichere und nicht sichere Datenübertragung nötig.

HINWEIS

Das Netzwerk darf von anderen Teilnehmern mitbenutzt werden, wenn genügend Übertragungskapazität zur Verfügung steht.

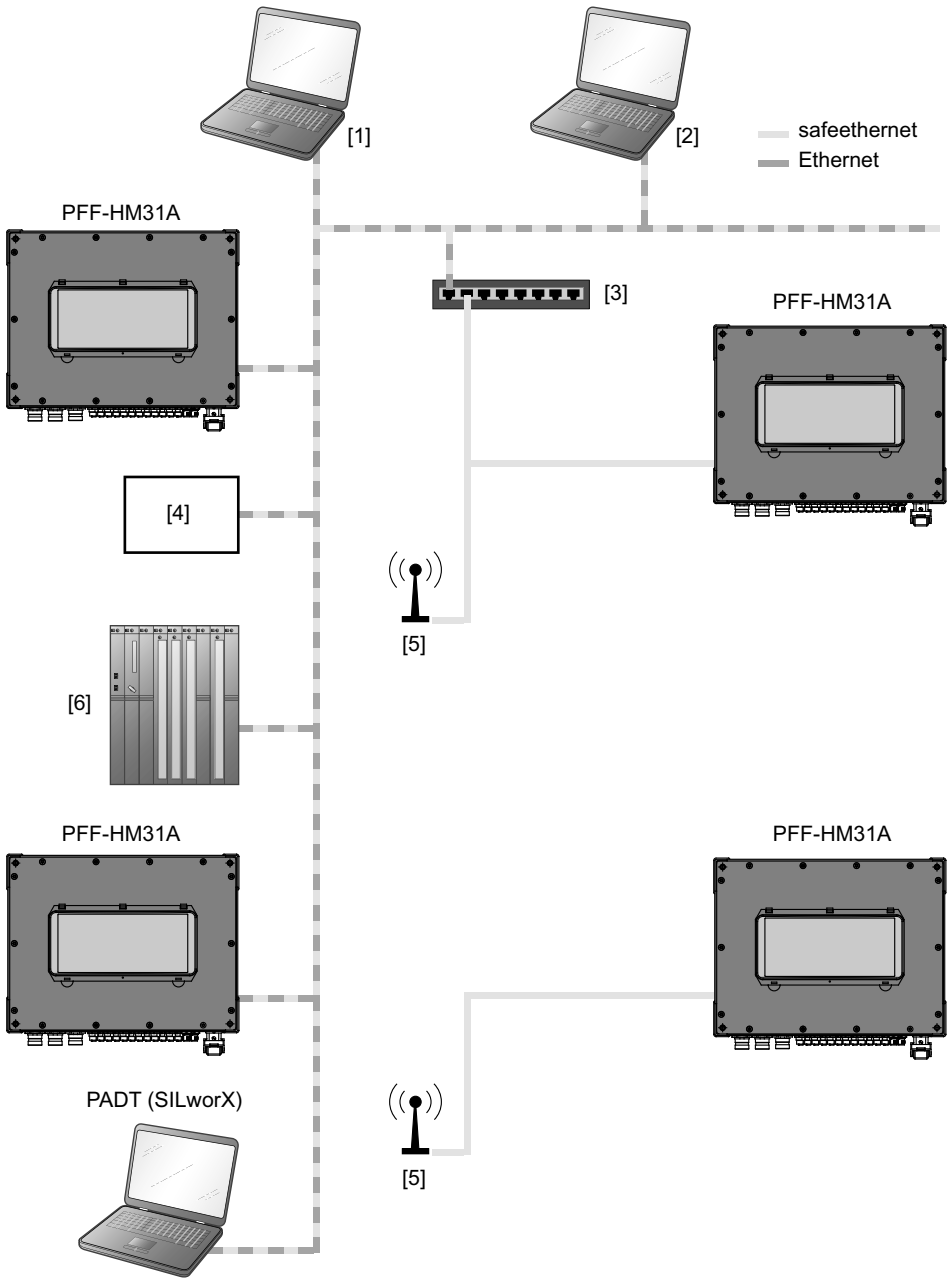
⚠ WARNUNG!

Manipulation der sicherheitsgerichteten Datenübertragung!

Tod oder schwere Körperverletzung.

Der Betreiber hat dafür zu sorgen, dass das für safeethernet verwendete Ethernetausreichend vor Manipulationen (z. B. durch Hacker) geschützt wird.Art und Umfang der Maßnahmen sind mit der abnehmenden Prüfstelle abzustimmen.

safeethernet ermöglicht flexible Systemstrukturen für die dezentrale Automatisierung mit definierten Reaktionszeiten. Je nach Anforderung können Sie die Intelligenz wahlweise zentral oder dezentral auf die Teilnehmer innerhalb des Netzwerkes verteilen.



5519919883

[1] PC des DCS-Leitsystems
[2] PADT (SILworX)
[3] Switch
[4] DCS-Leitsystem
[5] Funk, Satellit, WLAN, Lichtwellenleiter, ISDN oder DSL
[6] SPS

HINWEIS

Unbeabsichtigter Übergang in den sicheren Zustand möglich!

- Bei der Zusammenschaltung ist zu beachten, dass keine Netzschleifen entstehen. Datenpakete dürfen nur auf **einem** Weg zu einer Steuerung gelangen.
- Verwenden Sie beim Aufbau einer Ethernet-Ring-Topologie ausschließlich managementfähige Switche.

4.2 safeethernet-Editor

Im safeethernet-Editor erstellen und konfigurieren Sie die safeethernet-Verbindungen zu den Kommunikationspartnern (Ressourcen).

So öffnen Sie den safeethernet Editor der lokalen Ressource:

1. Im Strukturbaum [Konfiguration] / [Ressource] öffnen.
2. Rechtsklick auf safeethernet und im Kontextmenü [Edit] wählen.

Der safeethernet-Editor enthält den Arbeitsbereich und die Objektauswahl.

Im safeethernet-Editor erstellen und konfigurieren Sie die safeethernet Verbindungen zu den Kommunikationspartnern (Ressourcen). Dazu ziehen Sie die Ressourcen aus der Objektauswahl in den Arbeitsbereich.

Zur Konfiguration der safeethernet-Verbindung müssen Sie die folgenden safeethernet-Protokoll-Parameter einstellen:

Parameter	Beschreibung
Partner	Ressource-Name des Linkpartners
IF CH...	Verfügbare Ethernet-Schnittstellen auf der Ressource (lokal) und Ressource (Ziel)
Profil	Kombination zueinander passender safeethernet Parameter,siehe auch Kapitel "Safeethernet Profile
Response Time [ms]	Zeit bis zur Empfangsbestätigung einer Nachricht beim Absender, siehe auch Kapitel "Response Time".
Receive Timeout [ms]	Überwachungszeit auf PES1, innerhalb der eine korrekte Antwort von PES2 empfangen werden muss, siehe auch Kapitel "Receive Timeout"
Resend Timeout [ms]	Überwachungszeit auf PES1, innerhalb welcher PES2 den Empfang eines Datenpaketes bestätigt haben muss, ansonsten wird das Datenpaket wiederholt, siehe auch Kapitel "Resend Timeout".
Acknowledge Timeout [ms]	Zeit, nach der ein empfangenes Datenpaket von der CPU spätestens bestätigt werden muss, siehe auch Kapitel "Acknowledge Timeout".
Prod.-Rate	Produktionsrate: Kleinstes Zeitintervall zwischen zwei Datenpaketen, siehe auch Kapitel "Production Rate".
Speicher (Queue-Tiefe)	Anzahl der Datenpakete, die ohne Empfangsbestätigung versendet werden können, siehe auch Kapitel "Speicher".
Freeze-Daten bei Verbindungsverlust [ms]	Verhalten der Input Variablen dieser safeethernet Verbindung bei Verbindungsunterbrechung[1]. • Verwende Initialdaten: Für die Input Variablen werden die Initialdaten verwendet. Unbegrenzt Die Input Variablen werden auf dem momentanen Wert eingefroren und bis zur erneuten Verbindungsaufnahme verwendet. • Begrenzt Eingabe: Doppelklick auf Dropdown-Feld und Zeit eingeben. Die Input Variablen werden auf dem momentanen Wert eingefroren und bis nach dem parametrierten Timeout verwendet. Danach werden die Initialdaten verwendet. Der Timeout kann sich um bis zu einem CPU Zyklus verlängern.
Fragmente pro Zyklus	Feste Einstellung: Ein Fragment wird pro Zyklus der Steuerung zum Kommunikationspartner übertragen. Fragment ≤ 900 Byte
Priorität Ereignisse	Funktion wird nicht unterstützt.
Priorität Zustandswerte	
Anzahl ignorierte Warnungen	Ist die Anzahl von Warnungen, die hintereinander in der Zeitspanne Zeitraum Warnungen [ms] auftreten müssen, bis diese in die Diagnose oder in die Kommunikations-Fehlerstatistik eingehen.
Zeitraum Warnungen [ms]	0 ms ist der derzeit einzig zugelassene Wert.
SER aktivieren	Standardwert: deaktiviert

1) Beachten Sie den folgenden Warnhinweis:

⚠ WARNUNG!

Verhalten der Input Variablen bei Verbindungsunterbrechung

Tod oder schwere Körperverletzung.

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

Objektauswahl

Die Objektauswahl stellt alle Ressourcen innerhalb dieses Projektes zur Verfügung, mit denen diese Ressource über safeethernet verbunden werden kann.

4.3 Detailansicht des safeethernet-Editors

Die Detailansicht hat immer den Bezug auf die lokale Ressource, für die Sie den safeethernet-Editor gestartet haben.

So öffnen Sie die Detailansicht einer safeethernet Verbindung:

1. Mit Rechtsklick auf [safeethernet Verbindung] Kontextmenü öffnen.
2. Auf [Detailansicht] klicken.

   Die Detailansicht beinhaltet das Register Systemvariablen, Fragment-Definitionen und Ressource (lokal)<->Ressource (Ziel).

4.3.1 Register: Systemvariablen

Sie können die safeethernet Verbindung im Anwenderprogramm mit Hilfe von Systemvariablen steuern und deren Status auswerten.

Systemvariable	Beschreibung	
Ack-Frame-Nr.	Empfangszähler (Umlaufend).	
Anzahl defekter Nachrichten	Anzahl aller defekter Nachrichten pro Kanal (falscherCRC, falscher Header, sonstige Fehler)	
Anzahl defekter Nachrichtendes Red. Kanal		
Anzahl Verbindungserfolge	Anzahl der Verbindungserfolge seit Reset der Statistik.	
Anzahl verlorener Nachrichten	Anzahl der auf einem der beiden Transportwege ausgefallenen Nachrichten seit Reset der Statistk. Der Zähler wird nur bis zum Komplettausfall eines Kanals geführt.	
Anzahl verlorener Nachrichten des Red.-Kanal		
Early Queue Usage	Anzahl der Nachrichten die in Early Queue gelegt wurden seit Reset der Statistik, siehe auch Kapitel "Speicher".	
Fehlerhafte Nachrichten	Anzahl verworfener Nachrichten seit Reset der Statistik.	
Frame-Nr.	Sendungszähler (Umlaufend)	
Kanalzustand	Aktueller Kanalzustand von Kanal 1. Der Kanalzustand ist der aktuelle Zustand des Kanal 1 zum Zeitpunkt (Seq-No X-1) beim Empfang einer Nachricht mit Seq-No X.	
	Status	**Beschreibung**
	0	Keine Nachricht zum Zustand von Kanal 1.
	1	Kanal 1 OK.
	2	Letzte Nachricht war Fehlerhaft, aktuelle ist OK.
	3	Fehler auf Kanal 1.
Layoutversion	Signatur des in der Kommunikation verwendeten Datenlayouts.	

Systemvariable	Beschreibung		
Letzte Kanal Latenz	Die Kanal Latenz gibt die Verzögerung zwischen beiden redundanten Transportpfaden zum Empfangszeitpunkt von Nachrichten mit identischer SeqNo an. Hierfür wird eine Statistik mit durchschnittlicher, minimaler, maximaler und letzter Latenz geführt. Ist der Min-Wert > dem Max-Wert, so sind die Statistikwerte ungültig. Letzte Kanal Latenz und Mittlere Kanal Latenz sind dann 0.		
Letzte Latenz des Red.-Kanal			
Max. Kanal Latenz			
Max. Kanal Latenz des Red. Kanal			
Min. Kanal Latenz			
Min. Kanal Latenz des Red. Kanal			
Mittlere Kanal Latenz			
Mittlere Kanal Latenz des Red. Kanal			
Monotonie	Nutzdatensendungszähler (Umlaufend).		
Neue Layoutversion	Signatur des neuen Datenlayouts.		
Qualität Kanal 1	Zustand des Haupt-Transportweges.		
	Bit Nr.	**Bit = 0**	**Bit = 1**
	0	Transportweg nicht freigegeben	Transportweg freigegeben
	1	Transportweg nicht genutzt	Transportweg aktiv genutzt
	2	Transportweg nicht verbunden	Transportweg verbunden
	3	-	Transportweg liefert Nachricht zuerst
	4–7	Reserviert	Reserviert
Qualität Kanal 2	Zustand des redundanten Transportweges, siehe Zustand Kanal 1 (Haupt-Transportweg).		
Receive Timeout	Zeit in Millisekunden (ms) auf PES1, innerhalb der eine gültige Antwort von PES2 empfangen werden muss, siehe auch Kapitel "Receive Timeout"		
Response Time	Zeit in Millisekunden (ms) bis zur Empfangsbestätigung einer Nachricht beim Absender, siehe auch Kapitel "Response Time"		
safeethernet-Statistik Zurücksetzen	Statistikwerte für die Kommunikationsverbindung im Anwenderprogramm zurücksetzen (z. B. Anzahl defekter Nachrichten, Kanalzustand, Zeitstempel des letzten Fehlers des Red.-Kanal ..., Wiederholungen).		
	Wert	**Funktion**	
	0	Kein Reset	
	1–255	Reset der safeethernet-Statistik	
Transport-Steuerung Kanal1	Transportsteuerung von Kanal1		
	Bit 0	**Funktion**	
	FALSE	Transportweg für Tests freigegeben	
	TRUE	Transportweg gesperrt	
	Bit 2 – 7 reserviert.		
Transport-Steuerung Kanal2	Siehe Transportsteuerung Kanal 1.		
Verbindungssteuerung	Mit dieser Systemvariablen kann die safeethernet-Verbindung vom Anwenderprogramm gesteuert werden.		
	Befehl	**Beschreibung**	
	Autoconnect (0x0000)	Standardwert: Nach Verlust der safeethernet Kommunikation versucht die Steuerung im nächsten CPU-Zyklus, die Verbindung wieder aufzunehmen.	
	Toggle Mode 0 (0x0100) Toggle Mode 1 (0x0101)	Nach dem Kommunikationsverlust kann durch einen programmgesteuerten Wechsel des Toggle Modus die Verbindung erneut aufgebaut werden. • TOGGLE MODE_0 (0x100) gesetzt: Auf TOGGLE MODE 1 (0x101) setzen um die Verbindung wieder aufzunehmen. • TOGGLE MODE 1 (0x101) gesetzt: Auf TOGGLE_MODE_0 (0x100) setzen um die Verbindung wieder aufzunehmen.	
	Disabled (0x8000)	safeethernet Kommunikation abgeschaltet.	

Systemvariable	Beschreibung	
Verbindungszustand	Der Verbindungszustand wertet den Status der Kommunikation zwischen zwei Steuerungen im Anwenderprogramm aus.	
	Status/Wert	**Beschreibung**
	Closed (0)	Verbindung ist geschlossen und es wird auch nicht versucht sie zu öffnen.
	Try_open (1)	Verbindung wird versucht zu öffnen, sie ist jedoch noch nicht geöffnet. Dieser Zustand gilt gleichermaßen für die aktive und auch für die passive Seite.
	Connected (2)	Die Verbindung ist hergestellt und in Betrieb (aktive Zeitüberwachung und Datenaustausch)
Wiederholungen	Anzahl der Wiederholungen seit Reset der Statistik.	
Zeitstempel des letzten Fehlers des Red.-Kanal [ms]	Millisekunden Anteil des Zeitstempels (aktuelle Systemzeit).	
Zeitstempel des letzten Fehlers des Red.-Kanals [s]	Sekunden Anteil des Zeitstempels (aktuelle Systemzeit).	
Zeitstempel des letzten Fehlers [ms]	Millisekunden Anteil des Zeitstempels (aktuelle Systemzeit).	
Zeitstempel des letzten Fehlers [s]	Sekunden Anteil des Zeitstempels (aktuelle Systemzeit).	
Zustand des Red.-Kanal	Aktueller Kanalzustand von Kanal 2. Der Kanalzustand ist der aktuelle Zustand des Kanal 2 zum Zeitpunkt (Seq-No X-1) beim Empfang einer Nachricht mit Seq-No X.	
	Status	**Beschreibung**
	0	Keine Nachricht zum Zustand von Kanal 2
	1	Kanal 2 OK
	2	Letzte Nachricht war Fehlerhaft, aktuelle ist OK.
	3	Fehler auf Kanal 2.

4.4 safeethernet Parameter

Die sicherheitsgerichtete Kommunikation richten Sie im safeethernet-Editor ein. Dazu müssen Sie die in diesem Kapitel beschriebenen Parameter 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, siehe Kapitel "Maximale Komunikationsscheibe"

4.4.1 Maximale Zykluszeit der Sicherheitssteuerung

Zur Bestimmung der maximalen Zykluszeit für eine Sicherheitssteuerung PFF-HM31A empfiehlt SEW-EURODRIVE die folgende Vorgehensweise.

Maximale Zykluszeit der Sicherheitssteuerung PFF-HM31A 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.

4.4.2 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

HINWEISE

- 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.

4.4.3 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.

HINWEISE

- 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 *ReceiveTMO*, 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.

4.4.4 Sync/Async

Sync: Zurzeit nicht unterstützt.

Async: Ist die Standardeinstellung. Bei der Einstellung Async empfängt die safeethernet Protokolleinstanz in der Input-Phase der CPU und sendet gemäß ihren Senderegeln in der Output-Phase der CPU.

4.4.5 ResendTMO

ResendTMO kann nicht manuell eingegeben werden, sondern wird aus dem Profil und der Response-Time berechnet. Überwachungszeit in Millisekunden (ms) auf PES1, innerhalb welcher PES2 den Empfang eines Datenpaketes bestätigt haben muss, ansonsten wird das Datenpaket wiederholt.

Regel: *ResendTMO* ≤ *Receive-Timeout*

Bei unterschiedlicher Konfiguration der Resend-Timeout bei den Kommunikationspartnern bestimmt der aktive Protokollpartner (kleinere SRS) den tatsächlichen Wert der Resend-Timeout der Protokollverbindung.

4.4.6 Acknowledge Timeout

AckTMO kann nicht manuell eingegeben werden, sondern wird aus dem Profil und der *Response-Time* berechnet. *AckTMO* ist die Zeit, nach der ein empfangenes Datenpaket von der CPU spätestens bestätigt werden muss.

Für ein schnelles Netzwerk ist *AckTMO* null, d. h. der Empfang eines Datenpaketes wird sofort bestätigt. Für ein langsames Netzwerk (z. B. Telefonmodemstrecke) ist *AckTMO* größer null. In diesem Fall wird versucht, die Bestätigungsmeldung zusammen mit Prozessdaten zu übermitteln, um die Netzbelastung durch Vermeidung von Adressierungs- und Sicherungsblöcken zu reduzieren.

Regeln:

AckTMO muss ≤ *Receive-Timeout* sein

AckTMO muss ≤ *Resend-Timeout* sein, wenn *Production-Rate* > *Resend-Timeout* ist.

4.4.7 Production Rate

ProdRate kann nicht manuell eingegeben werden, sondern wird aus dem Profil und der *Response-Time* berechnet.

Kleinstes Zeitintervall in Millisekunden (ms) zwischen zwei Datenpaketen.

Das Ziel von ProdRate ist, die Menge an Datenpaketen auf ein Maß zu begrenzen, welches einen (langsamen) Kommunikationskanal nicht überlastet. Dadurch wird eine gleichmäßige Auslastung des Übertragungsmediums erreicht und der Empfang veralteter Daten auf der Empfängerseite vermieden.

Regeln:

- ProdRate ≤ *Receive-Timeout*
- ProdRate ≤ *Resend-Timeout*, wenn *Acknowledge-Timeout* > *Resend-Timeout*

HINWEIS

Eine Production Rate von null bedeutet, dass mit jedem Zyklus des Anwenderprogramms Datenpakete übertragen werden können.

4.4.8 Speicher

Speicher kann nicht manuell eingegeben werden, sondern wird aus dem Profil und der Response-Time berechnet.

Speicher (Queue-Tiefe) ist die Anzahl der Datenpakete, die ausgesendet werden können, ohne auf deren Empfangsbestätigung warten zu müssen.

Der Wert ist abhängig von der Übertragungskapazität des Netzwerkes und möglichen Verzögerungen durch Netzwerklaufzeiten.

Alle safeethernet Verbindungen teilen sich den zur Verfügung stehenden Message-Speicher in der CPU.

4.5 Maximale Reaktionszeit für safeethernet

In den folgenden Beispielen gelten die Formeln für die Berechnung der maximalen Reaktionszeit nur dann, wenn die Sicherheitszeit = 2 × Watchdog-Zeit eingestellt ist.

HINWEIS

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

Begriffe	Bedeutung
ReceiveTMO	Überwachungszeit im PES 1, in der eine gültige Antwort vom PES 2 empfangen werden muss. Nach Ablauf der Zeit wird die sicherheitsgerichtete Kommunikation andernfalls geschlossen.
Production Rate	Mindestabstand zwischen zwei Datensendungen.
Watchdog-Zeit	Maximal erlaubte Dauer eines RUN-Zyklus in einer Steuerung. Die Dauer des RUN-Zyklus hängt von Komplexität des Anwenderprogramms und der Anzahl der safeethernet Verbindungen ab. Watchdog-Zeit (WDZ) ist in den Eigenschaften der Ressource einzutragen.
Worst Case Reaction Time	Maximale Reaktionszeit für die Übertragung der Änderung des Signals eines physikalischen Einganges (In) eines PES 1 bis zur Änderung des physikalischen Ausgangs (Out) eines PES 2.
Delay	Verzögerung einer Übertragungsstrecke z. B. bei Modem- oder Satellitenverbindung. Bei direkter Verbindung kann zunächst eine Verzögerung von 2 ms angenommen werden. Die tatsächliche Verzögerung der Übertragungsstrecke kann von dem zuständigen Netzwerkadministrator ausgemessen werden.

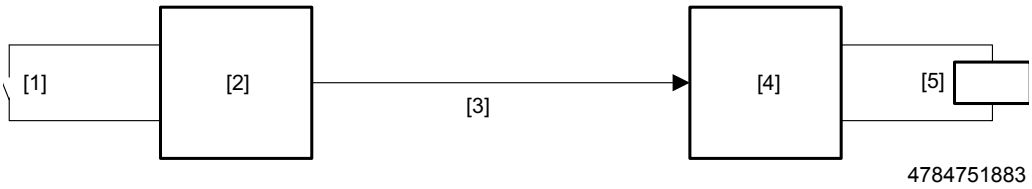
Für die folgenden Berechnungen der zulässigen maximalen Reaktionszeiten gelten folgende Bedingungen:

- Die Signale, die mit safeethernet übertragenen werden, müssen in den jeweiligen Steuerungen innerhalb eines CPU-Zyklus verarbeitet werden.
- Die Reaktionszeiten der Sensoren und Aktoren sind zusätzlich zu addieren.

Die Berechnungen gelten auch für Signale in umgekehrter Richtung.

4.5.1 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:



[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 Reaktion 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.

4.5.2 Safeethernet Profile

Safeethernet Profile sind Kombinationen zueinander passender Parameter, die automatisch bei Auswahl eines der safeethernet Profile eingestellt werden. Für die Parametrierung muss nur die Receive-Timeout und die erwartete Response-Time einzeln konfiguriert werden.

Das Ziel eines safeethernet Profils besteht darin, den Datendurchsatz im Netzwerk unter Berücksichtigung der physikalischen Gegebenheiten zu optimieren.

Voraussetzung für die Wirksamkeit der Optimierung sind die nachfolgenden Bedingungen:

- Kommunikations-Zeitscheibe muss ausreichend groß sein, damit in einem CPU-Zyklus alle safeethernet Verbindungen abgearbeitet werden.
- Mittlere CPU Zykluszeit < Response-Time.
- Mittlere CPU Zykluszeit < ProdRate oder ProdRate = 0

ACHTUNG!

Unpassende Kombinationen von CPU-Zyklus, Kommunikations-Zeitscheibe, Response-Time und ProdRate werden bei der Codegenerierung und beim Download/Reload nicht abgelehnt. Diese Kombinationen können aber zu Störungen bis hin zum Ausfall der safeethernet Kommunikation führen.

Mögliche Beschädigung des Antriebssystems.

- In den Control Panels der beiden Steuerungen die Anzeigen **"Fehlerhafte Nachrichten"** und **"Wiederholungen"** überprüfen.

Sechs safeethernet Profile stehen zur Verfügung, aus denen das für die Übertragungsstrecke geeigneten safeethernet Profil ausgewählt werden kann. Beachten Sie dazu den folgenden Warnhinweis:

⚠ WARNUNG!

Lediglich die **Noisy-Profile** sind für sicherheitsgerichtete Prozessdatenkommunikation geeignet!

Tod oder schwere Körperverletzung.

Verwenden Sie für eine sicherheitsgerichtete Prozessdatenkommunikation nur die Noisy-Profile:

- Fast&Noisy, Medium&Noisy und Slow&Noisy

Die folgende Tabelle zeigt Ihnen die verfügbaren Profile:

Profil	Verwendung
Fast & Cleanroom	Nur für störungsfreies Netzwerk empfohlen.
Fast & Noisy	Empfohlen, für eine hohe Verfügbarkeit der safeethernet Verbindung.
Medium & Cleanroom	Nur für störungsfreies Netzwerk empfohlen.
Medium & Noisy	Empfohlen, für eine hohe Verfügbarkeit der safeethernet Verbindung.
Slow & Cleanroom	Nur für störungsfreies Netzwerk empfohlen.
Slow & Noisy	Empfohlen, für eine hohe Verfügbarkeit der safeethernet Verbindung.

4.5.3 Profil I (Fast & Cleanroom)

⚠ WARNUNG!

Lediglich die **Noisy-Profile** sind für sicherheitsgerichtete Prozessdatenkommunikation geeignet!

Tod oder schwere Körperverletzung.

Verwenden Sie für eine sicherheitsgerichtete Prozessdatenkommunikation nur die Noisy-Profile:

- Fast&Noisy, Medium&Noisy und Slow&Noisy

Verwendung

Das Profil **Fast & Cleanroom** ist geeignet für Anwendungen, in idealer Umgebung z. B. Labor.

- Für schnellsten Datendurchsatz
- Für Anwendungen, die eine schnelle Datenübermittlung erfordern
- Für Anwendungen, die eine möglichst geringe Worst Case ReactionTime erfordern

Netzwerkanforderungen
- Fast: 100-Mbit-Technologie (100 Base TX), 1-Gbit-Technologie
- Clean: Störungsfreies Netzwerk.
- Datenverlust durch Netzüberlastung, Einflüsse von außen oder Netzwerkmanipulationen müssen vermieden werden.
- LAN-Switches erforderlich!

Charakteristika des Kommunikationspfads
- Minimale Verzögerungen
- Erwartete ResponseTime ≤ ReceiveTMO

  (anderenfalls FEHLER bei Parametrierung)

4.5.4 Profil II (Fast & Noisy)

Verwendung

Das Profil **Fast & Noisy** ist das SILworX Standardprofil für die Kommunikation über safeethernet.
- Für schnellsten Datendurchsatz
- Für Anwendungen, die eine schnelle Datenübermittlung erfordern
- Für Anwendungen, die eine möglichst geringe Worst Case ReactionTime erfordern

Netzwerkanforderungen
- Fast: 100-Mbit-Technologie (100 Base TX), 1-Gbit-Technologie
- Noisy: Netzwerk ist nicht störungsfrei. Geringe Wahrscheinlichkeit für Verlust von Datenpaketen Zeit für ≥1 Wiederholung
- LAN-Switches erforderlich!

Charakteristika des Kommunikationspfads
- Minimale Verzögerungen
- Erwartete ResponseTime ≤ ReceiveTMO / 2

  (anderenfalls FEHLER bei Parametrierung)

4.5.5 Profil III (Medium & Cleanroom)

⚠ WARNUNG!

Lediglich die **Noisy-Profile** sind für sicherheitsgerichtete Prozessdatenkommunikation geeignet!

Tod oder schwere Körperverletzung.

Verwenden Sie für eine sicherheitsgerichtete Prozessdatenkommunikation nur die Noisy-Profile:
- Fast&Noisy, Medium&Noisy und Slow&Noisy

Verwendung

Das Profil **Medium & Cleanroom** ist für Anwendungen in einem Störungsfreien Netzwerk, die eine nur mäßig schnelle Datenübermittlung erfordern.
- Für mittleren Datendurchsatz
- Geeignet für Virtual Private Networks (VPN), in denen der Datenaustausch durch zwischengeschaltete Sicherheitseinrichtungen (Firewalls, Verschlüsselung) langsam, aber fehlerfrei ist.
- Geeignet für Anwendungen, in denen die Worst Case ReactionTime kein kritischer Faktor ist.

Netzwerkanforderungen
- Medium: 10-Mbit- (10 Base T), 100-Mbit- (100 Base TX), 1-Gbit-Technologie
- LAN-Switches erforderlich!
- Clean: Störungsfreies Netzwerk.

  Datenverlust durch Netzüberlastung, Einflüsse von außen oder Netzwerkmanipulationen müssen vermieden werden.

  Zeit für ≥ 0 Wiederholungen

Charakteristika des Kommunikationspfads
- Moderate Verzögerungen
- Erwartete ResponseTime ≤ ReceiveTMO

  (anderenfalls FEHLER bei Parametrierung)

4.5.6 Profil IV (Medium & Noisy)

Verwendung

Das Profil **Medium & Noisy** ist für Anwendungen, die eine nur mäßig schnelle Datenübermittlung erfordern.
- Für mittleren Datendurchsatz
- Für Anwendungen, die nur eine mäßig schnelle Datenübermittlung erfordern
- Geeignet für Anwendungen, in denen die Worst Case ReactionTime kein kritischer Faktor ist.

Netzwerkanforderungen
- Medium: 10-Mbit- (10 Base T), 100-Mbit- (100 Base TX), 1-Gbit-Technologie
- LAN-Switches erforderlich!
- Noisy: Netzwerk ist nicht störungsfrei.

  Geringe Wahrscheinlichkeit für Verlust von Datenpaketen,

  Zeit für ≥ 1 Wiederholung

Charakteristika des Kommunikationspfads
- Moderate Verzögerungen
- Erwartete ResponseTime ≤ ReceiveTMO / 2

  (anderenfalls FEHLER bei Parametrierung)

4.5.7 Profil V (Slow & Cleanroom)

⚠ WARNUNG!

Lediglich die **Noisy-Profile** sind für sicherheitsgerichtete Prozessdatenkommunikation geeignet!

Tod oder schwere Körperverletzung.

Verwenden Sie für eine sicherheitsgerichtete Prozessdatenkommunikation nur die Noisy-Profile:
- Fast&Noisy, Medium&Noisy und Slow&Noisy

Verwendung

Das Profil **Slow & Cleanroom** ist für Anwendungen in einem störungsfreien Netzwerk, die nur eine langsame Datenübermittlung erfordern.
- Für langsamen Datendurchsatz

- Für Anwendungen, die nur eine langsame Datenübermittlung zu (möglicherweise weit entfernten) Steuerungen erfordern, und dort, wo die Bedingungen der Kommunikationsstrecke nicht vorhersagbar sind.

Netzwerkanforderungen
- Slow: Datentransfer über ISDN, Standleitung oder Richtfunkverbindung.
- Clean: Störungsfreies Netzwerk.

  Datenverlust durch Netzüberlastung, Einflüsse von außen oder Netzwerkmanipulationen müssen vermieden werden.

  Zeit für ≥ 0 Wiederholungen

Charakteristika des Kommunikationspfads
- Moderate Verzögerungen
- Erwartete ResponseTime ≤ ReceiveTMO

  (anderenfalls FEHLER bei Parametrierung)

4.5.8 Profil VI (Slow & Noisy)

Verwendung

Das Profil **Slow & Noisy** ist für Anwendungen, die nur eine langsame Datenübermittlung zu (möglicherweise weit entfernten) Steuerungen erfordern.

- Für langsamen Datendurchsatz
- Für Anwendungen, Hauptsächlich für Datentransfer über schlechte Telefonleitungen oder gestörte Richtfunkstrecken.

Netzwerkanforderungen
- Slow: Datentransfer über Telefon, Satellit, Funk usw.
- Noisy: Netzwerk ist nicht Störungsfrei.

  Geringe Wahrscheinlichkeit für Verlust von Datenpaketen,

  Zeit für ≥ 1 Wiederholung

Charakteristika des Kommunikationspfads
- Moderate bis lange Verzögerungen
- Erwartete ResponseTime ≤ ReceiveTMO / 2

  (anderenfalls FEHLER bei Parametrierung)

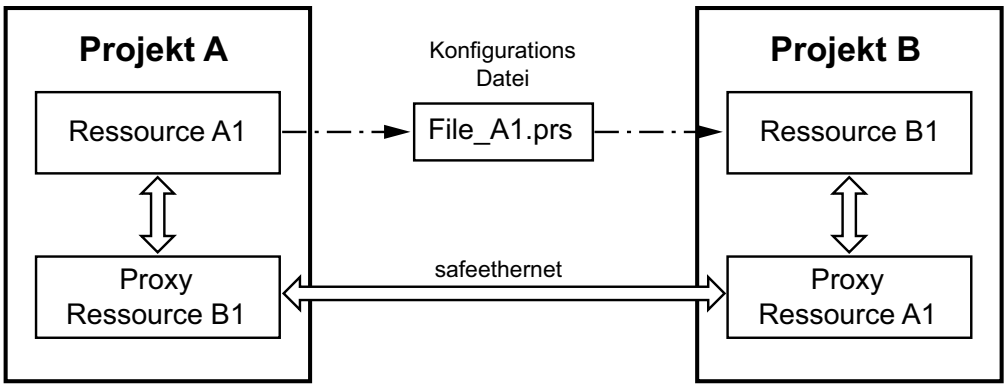
4.6 Projektübergreifende Kommunikation

Die projektübergreifende Kommunikation wird für Folgendes verwendet:

- Um Ressourcen aus verschiedenen Projekten miteinander zu verbinden.
- Um Steuerungen mit SILworX Betriebssystem und Steuerungen über safeethernet miteinander zu verbinden.

Die Kommunikation zwischen den beiden Projekten erfolgt über safeethernet und wird im safeethernet-Editor konfiguriert.

Safeethernet Verbindung zwischen Ressource A1 im Projekt A und der Ressource B1 im Projekt B:



5306777483

Als lokales Projekt wird das Projekt bezeichnet, in dem Sie die Konfiguration der safeethernet Verbindung durchführen und die Konfigurationsdatei erstellen.

Als Ziel-Projekt wird das Projekt bezeichnet, in das Sie die Konfigurationsdatei importieren.

Beim Datenaustausch sind das lokale Projekt und das Ziel-Projekt gleichberechtigte Kommunikationspartner.

Die jeweilige Proxy-Ressource dient als Platzhalter für die jeweilige Ressource aus dem externen Projekt und wird für den Import und Export der safeethernet Verbindungen genutzt.

Die *Proxy-Ressource B1* im Projekt A ist der Platzhalter der *Ressource B1* aus dem Projekt B.

Die *Proxy-Ressource A1* im Projekt B ist der Platzhalter der *Ressource A1* aus dem Projekt A.

Im lokalen Projekt (hier *Projekt A*) müssen Sie die Proxy-Ressource (hier *Proxy-Ressource B1*) manuell erstellen und konfigurieren. Nach der Konfiguration die Konfigurationsdatei (hier `File_A1.prs`) im Ziel-Projekt (hier von *Ressource B1*) importieren.

Die Konfigurationsdatei `File_A1.prs` enthält die komplette Beschreibung der Ressource A1 für die safeethernet Verbindung mit der *Ressource B1*. Nach dem Import der Konfigurationsdatei `File_A1.prs` in die *Ressource B1* wird die *Proxy-Ressource A1* automatisch im Projekt B angelegt.

4.6.1 Varianten zur projektübergreifenden Kommunikation

In den folgenden beiden Varianten kommunizieren die Projekte A und B über safeethernet miteinander.

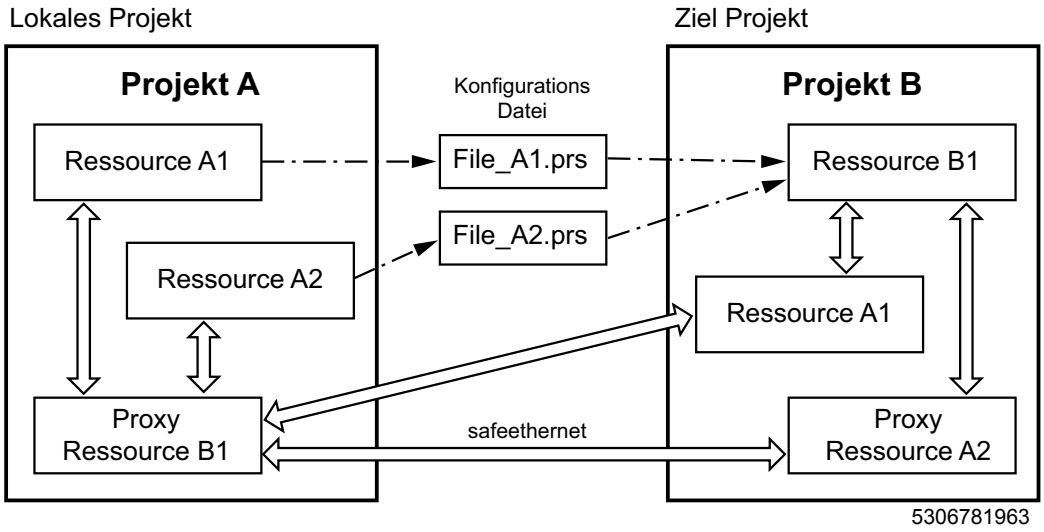
Dabei ist in der ersten Variante das Projekt A das lokale Projekt und in der zweiten Variante das Projekt B das lokale Projekt. Grundsätzlich bleibt es dem Anwender überlassen, in welchem der beiden Projekte er die Konfiguration erstellt.

Der Aufwand für beide Wege der Konfiguration ist ungefähr gleich und führt zur gleichen Konfiguration.

Lokales Projekt A

Im lokalen Projekt A konfigurieren Sie die Kommunikation zum Ziel-Projekt B und erstellen die Konfigurationsdateien. Das hat den Vorteil, dass Sie nur die *Proxy-Ressource B1* im lokalen Projekt manuell anlegen müssen.

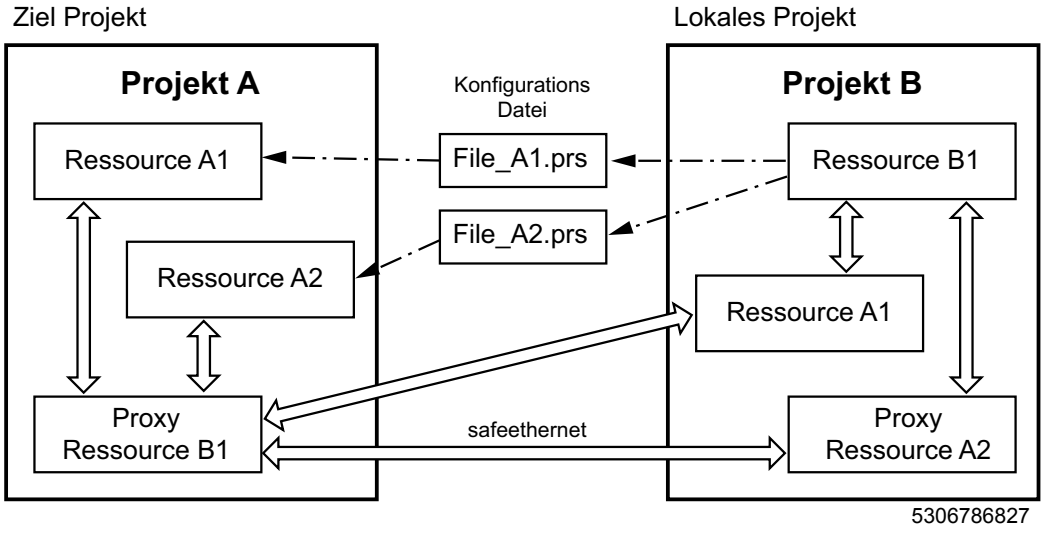
Variante Projekt A als lokales Projekt:



Lokales Projekt B

Im lokalen Projekt B konfigurieren Sie die Kommunikation zum Ziel-Projekt A und erstellen die Konfigurations-Files. Das hat den Nachteil, dass Sie zwei *Proxy-Ressourcen* (*A1* und *A2*) im lokalen Projekt B manuell anlegen müssen.

Variante Projekt B als lokales Projekt:



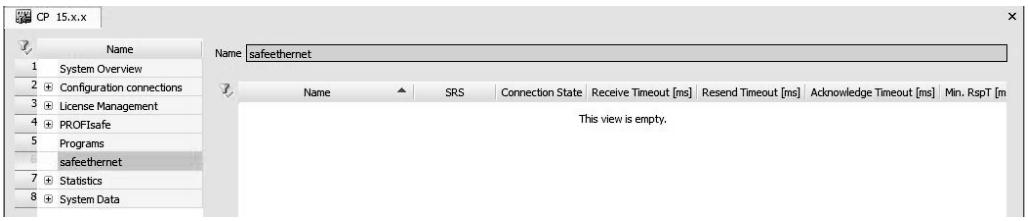
4.7 Control Panel (safeethernet)

Im Control Panel kann der Anwender die Einstellungen der safeethernet-Verbindung überprüfen und steuern. Zudem werden aktuelle Statusinformationen (z. B. Zykluszeit, Bus-Zustand usw.) der safeethernet-Verbindung angezeigt.

So öffnen Sie das Control Panel zur Überwachung der safeethernet Verbindung:

1. Im Strukturbaum [Ressource] wählen.
2. Aus dem Kontextmenü der Ressource [Online] wählen.
3. Im System-Login, Zugangsdaten eingeben um das Control Panel der Ressource zu-öffnen.

4. Im Strukturbaum des Control Panels [safeethernet] wählen.



5428388235

Statistikwerte zurücksetzen:

Mit der Kontextmenüfunktion können Sie die statistischen Daten (Zykluszeit min, max usw.) auf null zurücksetzen.

So setzen Sie die statistischen Daten der safeethernet Verbindung zurück:

- Im Strukturbaum safeethernet Verbindung selektieren.
- Aus dem Kontextmenü der safeethernet Verbindung, [safeethernet Statistik] zurücksetzen wählen.

4.7.1 Anzeigefeld (safeethernet-Verbindung)

In dem Anzeigefeld werden die folgenden Werte der selektierten safeethernet-Verbindung angezeigt:

Element	Beschreibung
Name	Ressource-Name des Kommunikationspartners
SRS	System.Rack.Slot
Verbindungszustand	Zustand der safeethernet-Verbindung (siehe auch Kapitel "Detailansicht des safeethernet-Editors"
Receive-Timeout [ms]	siehe Kapitel "safeethernet-Parameter"
Resend-Timeout [ms]	siehe Kapitel "safeethernet-Parameter"
Acknowledge Timeout [ms]	siehe Kapitel "safeethernet-Parameter"
Min. RspT [ms]	Tatsächliche Response-Time als Minimal-, Maximal-, Letzte- und Durchschnittswert (siehe Kapitel "safeethernet-Parameter").
Max. RspT [ms]	
Letzte RspT [ms]	
Mittel RspT [ms]	
Fehlerhafte Nachrichten	
Wiederholungen	Anzahl verworfener Nachrichten seit Reset der Statistik.
Anzahl Verbindungserfolge	Anzahl der Verbindungserfolge seit Reset der Statistik.
Early Queue Usage	Anzahl der Nachrichten die in Early Queue gelegt wurden seit Reset der Statistik (siehe Kapitel "safeethernet-Parameter").
Frame-Nr.	Umlaufender Sendungszähler
Ack-Frame-Nr.	Umlaufender Empfangszähler
Monotonie	Umlaufender Nutzdatensendungszähler
Layoutversion	Signatur des aktuellen Kommunikationsendpunkts
Neue Layoutversion	Signatur des neuen Kommunikationsendpunkts
Verbindungssteuerung	Status der Verbindungssteuerung
Transport-Steuerung Kanal 1	Freigabe von Transportweg Kanal 1 (siehe Kapitel "safeethernet-Parameter")
Transport-Steuerung Kanal 2	Freigabe von Transportweg Kanal 2 (siehe Kapitel "safeethernet-Parameter")
Qualität Kanal 1	Zustand von Transportweg Kanal 1 (siehe Kapitel "safeethernet-Parameter")
Qualität Kanal 2	Zustand von Transportweg Kanal 2 (siehe Kapitel "safeethernet-Parameter")
Spät erhaltene redundante Nachrichten	Bei redundanten Transportwegen. Anzahl der verspätet empfangenen Nachrichten seit Reset der Statistik.

Element	Beschreibung
Verlorene redundante Nachrichten	Bei redundanten Transportwegen. Anzahl der auf nur einem der beiden Transportwege empfangenen Nachrichten seit Reset der Statistik.
Protokollversion	2: Neue Protokollversion für CPU Betriebssystem ab V7

4.8 Maximale Kommunikationszeitscheibe

Die maximale Kommunikationszeitscheibe ist die zugeteilte Zeit in Millisekunden (ms) pro Zyklus, innerhalb welcher das Prozessorsystem die Kommunikationsaufgaben abarbeitet. Können nicht alle in einem Zyklus anstehenden Kommunikationsaufgaben ausgeführt werden, erfolgt die komplette Übertragung der Kommunikationsdaten über mehrere Zyklen (Anzahl der Kommunikationszeitscheiben > 1).

HINWEIS

Es gilt die Bedingung, dass die Anzahl der Kommunikationszeitscheiben = 1 ist. Die Dauer der Kommunikationszeitscheibe ist so hoch einzustellen, dass der Zyklus die vom Prozess vorgegebene Watchdog-Zeit nicht überschreiten kann, wenn er die Kommunikationszeitscheibe ausnutzt (siehe auch Kapitel "Maximale Reaktionszeit für safeethernet".

4.9 Anschlüsse für safeethernet/Ethernet

Für die Vernetzung über safeethernet/Ethernet verfügt die Sicherheitssteuerung über die folgenden Schnittstellen:

Es stehen die folgenden Schnittstellen zur Verfügung:

- **2 Ethernet-Schnittstellen:** X4233_1 und X4233_2

  Die beiden Schnittstellen befinden sich auf der Anschlussleiste des Geräts

- **1 Ethernet-Service-Schnittstelle:** X4223

  Zum Anschluss eines Programmiergeräts (PADT)

Die unterschiedlichen Systeme können beliebig über Ethernet miteinander vernetzt werden (stern- oder linienförmig). Auch der Anschluss eines Programmiergeräts (PADT) ist an jeder Stelle möglich.

HINWEIS

Störungen des Ethernet-Betriebs möglich!

- Bei der Zusammenschaltung ist zu beachten, dass keine Netzringe entstehen.
- Datenpakete dürfen nur auf **einem** Weg zu einem System gelangen.

5 Modbus TCP/UDP

5.1 Modbus Master

Die Datenübertragung zwischen dem Modbus Master und den Modbus Slaves erfolgt über TCP/UDP (Ethernet).

Die folgende Tabelle zeigt Ihnen die Eigenschaften des Modbus Masters:

Eigenschaft	Beschreibung				
Modbus Master	Es kann pro COM-Modul / Steuerung ein Modbus Master konfiguriert werden. Der Modbus Master kann simultan • mit TCP/UDP-Slaves Daten austauschen				
Max. Anzahl Modbus Slaves	Ein Modbus Master kann bis zu 247 Slaves bedienen. • 64 TCP Slaves über TCP/IP-Verbindung • 247 UDP Slaves über UDP/IP-Verbindung Die maximale Anzahl UDP Slaves ist limitiert, da die Slaves auf der Master Seite verwaltet werden müssen.				
Max. Anzahl Anforderungstelegramme	Es können bis zu 988 Anforderungstelegramme pro Modbus Master konfiguriert werden.				
Max. Prozessdatenlänge pro Anforderungstelegramm	Die Prozessdatenlänge beträgt bei SEW-spezifischen Anforderungstelegrammen 1100 Byte, siehe Kapitel "SEW spezifische Funktionscodes"				
Max. Größe der Sendedaten	64 kB senden				
Max. Größe der Empfangsdaten	64 kB empfangen Hinweis: Die Statusbytes des Masters und die Statusbytes von jedem zugeordneten Slave müssen von der max. Größe der Sendedaten subtrahiert werden.				
Darstellungsformat der Modbus-Daten	Die Sicherheitssteuerung verwendet das Big Endian Format. Beispiel: 32 Bit Daten (z. B. DWORD, DINT):				
	32 Bit Daten (hex)	0x12345678			
	Speicher-Offset	0	1	2	3
	Big Endian	12	34	56	78
	Middle Endian	56	78	12	34
	Little Endian	78	56	34	12

5.1.1 Anlegen eines Modbus Masters

HINWEIS

Befinden sich der Modbus Master und der Modbus Slave in verschiedenen Subnetzen, müssen in der Routing-Tabelle die entsprechenden benutzerdefinierten Routen eingetragen werden.

Konfiguration des Modbus TCP Master

So legen Sie den Modbus Master an:

1. Im Strukturbaum [Konfiguration] / [Ressource] / [Protokolle] öffnen.
2. Im Kontextmenü von Protokolle [Neu] / [Modbus Master] wählen um einen neuen Modbus Master hinzuzufügen.
3. Im Kontextmenü vom Modbus Master [Eigenschaften] / [Allgemein] wählen.
4. [COM Modul] auswählen.

   Die restlichen Parameter behalten die Standardwerte.

So erstellen Sie im Modbus Master die Verbindung zu dem Modbus TCP Slave:

1. Im Strukturbaum [Ressource] / [Protokolle] / [Modbus Master] / [Ethernet Slaves] öffnen.

2. Rechtsklick auf [Ethernet Slaves] und im Kontextmenü [Neu] wählen.
3. Aus der Liste "TCP/UDP-Slave" wählen und mit [OK] bestätigen.
4. Konfiguration des TCP/UDP-Slave im Modbus Master:
   - [Edit] zum Zuweisen der Systemvariablen wählen, siehe Kapitel "Systemvariablen Gateway-Slave".
   - [Eigenschaften] zum Konfigurieren der Eigenschaften wählen, siehe Kapitel "Eigenschaften Gateway-Slave".

     In den Eigenschaften des Slaves die IP Adresse des TCP/UDP-Slaves eintragen.

     Die restlichen Parameter behalten die Standardwerte.

5.1.2 Menüfunktionen des Modbus Master

Edit

Das Dialogfenster "Edit" des Modbus-Masters enthält die folgende Registerkarte:

Systemvariablen

Die Registerkarte "Systemvariablen" stellt Systemvariablen bereit, die es erlauben, den Zustand des Modbus Masters im Anwenderprogramm auszuwerten und den Modbus Master zu steuern.

Element	Beschreibung
Anzahl fehlerhafte Slave-Verbindungen	Anzahl der fehlerhaften Verbindungen mit Modbus Slaves, die im Zustand aktiviert sind. Deaktivierte Modbus Slaves werden hier nicht berücksichtigt.
Modbus-Master Aktivierungssteuerung	Hiermit kann der Modbus Master vom Anwenderprogramm gestoppt oder gestartet werden. 0: Aktivieren 1: Deaktivieren(Flankengetriggert! Modbus Master kann über PADT auch dann aktiviert werden wenn Modbus-Master Aktivierungssteuerung = 1.)
Modbus-Master Busfehler	Busfehler, z. B. Telegrammfehler (unbekannte Codes etc.), Längenfehler.
Modbus-Master Zustand	Der Modbus Master Zustand zeigt den momentanen Protokollzustand an: 1: OPERATE 0: OFFLINE
Reset aller Slave-Fehler	Mit einem Wechsel von FALSE->TRUE werden alle Slave-Fehler und Busfehler zurückgesetzt.

Eigenschaften

Die Menüfunktion "Eigenschaften" aus dem Kontextmenü des Modbus Master öffnet den Dialog Eigenschaften.

Der Dialog enthält die folgenden Register:

Allgemein

Im Register "Allgemein" werden der Name und die Beschreibung für den Modbus Master eingegeben. Zudem werden hier die Parameter eingestellt, wenn der Modbus Master zusätzlich als TCP und/oder UDP Gateway arbeiten soll.

Parameter	Beschreibung
Typ	Modbus Master
Name	Name für den Modbus Master
Modul	Auswahl des COM-Moduls, auf dem dieses Protokoll abgearbeitet wird.
Max. µP-Budget aktivieren	**Aktiviert:** Limit des µP-Budget aus dem Feld Max. µP-Budget in [%] uebernehmen. **Deaktiviert:** Kein Limit des µP-Budget, fur dieses Protokoll verwenden.
Max. µP-Budget in [%]	Maximale µP-Last des Moduls, welche bei der Abarbeitung des Protokolls produziert werden darf. Wertebereich: 1 – 100 % Standardwert: 30 %

Parameter	Beschreibung
Verhalten bei CPU/COM Verbindungsverlust	Bei Verbindungsverlust des Prozessormoduls zum Kommunikationsmodul werden in Abhängigkeit dieses Parameters die Eingangsvariablen entweder initialisiert oder unverändert im Prozessormodul verwendet. (z. B. wenn Kommunikationsmodul bei laufender Kommunikation gezogen wird). **Initialdaten annehmen:** Eingangsvariablen werden auf die Initialwerte zurückgesetzt. **Letzten Wert beibehalten**: Eingangsvariablen behalten den letzten Wert.
TCP-Gateway aktivieren	Diese Funktion darf nicht aktiviert werden, weil die RS485-Schnittstelle von der ComUserTask verwendet wird.
TCP-Server-Port	Standard: 502 Es können auch andere TCP-Ports konfiguriert werden. Dabei ist die Port-Belegung bei der *Internet Corporation for Assigned Names and Numbers (ICANN)* zu beachten.
Maximale Anzahl TCP-Verbindungen als Server	Maximale Anzahl gleichzeitig offener TCP-Verbindungen als Server. Wertebereich:1 – 64 Standardwert: 5
UDP-Gateway aktivieren	Diese Funktion darf nicht aktiviert werden, weil die RS485-Schnittstelle von der ComUserTask verwendet wird.
UDP-Port	Standard: 502 Es können auch andere TCP-Ports konfiguriert werden. Dabei ist die Port-Belegung bei der *Internet Corporation for Assigned Names and Numbers (ICANN)* zu beachten.
Maximale Länge der Queue	Länge der Gateway-Warteschlange für noch nicht beantwortete Anforderungstelegramme von anderen Mastern. Dies wird nur beachtet, wenn ein Gateway aktiviert ist. Wertebereich: 1 – 20 Standardwert: 3

CPU/COM

Die Standardwerte für die Parameter sorgen für den schnellstmöglichen Datenaustausch der Modbus-Daten zwischen dem COM-Modul und dem CPU-Modul in der Sicherheitssteuerung.

Diese Parameter sollten nur dann geändert werden, wenn eine Reduzierung der COM und/oder CPU-Auslastung für eine Anwendung erforderlich ist und der Prozess dies zulässt.

HINWEIS

Die Änderung der Parameter wird nur dem erfahrenen Programmierer empfohlen. Eine Erhöhung der COM- und CPU-Aktualisierungszeit bedeutet auch, dass die tatsächliche Aktualisierungszeit der Modbus-Daten erhöht wird.

- Die Zeitanforderungen der Anlage sind zu prüfen.

Parameter	Beschreibung
Aktualisierungsintervall der Prozessdaten [ms]	Aktualisierungszeit in Millisekunden, mit der die Daten des Protokolls zwischen COM und CPU ausgetauscht werden. Ist das Aktualisierungsintervall der Prozessdaten Null oder kleiner als die Zykluszeit der Steuerung, dann erfolgt der Datenaustausch so schnell wie möglich. Wertebereich: 0 – (2^{31}-1) Standardwert: 0
Prozessdaten-Konsistenz erzwingen	**Aktiviert:** Transfer der gesamten Daten des Protokolls von der CPU zur COM innerhalb eines Zyklus der CPU. **Deaktiviert:** Transfer der gesamten Daten des Protokolls von der CPU zur COM, verteilt über mehrere CPU Zyklen zu je 1100 Byte pro Datenrichtung. Damit kann eventuell auch die Zykluszeit der Steuerung reduziert werden. Standardwert: Aktiviert

5.1.3 Modbus Funktionscodes des Masters

Mit den Modbus Funktionscodes (Anforderungstelegrammen) haben Sie die Möglichkeit, Variablen in beide Richtungen zu schreiben oder zu lesen. Es können einzelne Variablen oder mehrere aufeinander folgende Variablen gelesen oder geschrieben werden.

So erstellen Sie ein neues Anforderungstelegramm für einen TCP/UDP Slave:

1. Im Strukturbaum [Ressource] / [Protokolle] / [Modbus Master] / [Ethernet-Slaves] einen TCP/UDP Slave wählen.
2. Rechtsklick auf TCP/UDP Slave und im Kontextmenü [Neu] wählen.
3. Aus dem Dialog "Neues Objekt" ein Anforderungstelegramm auswählen.

Modbus Standard Funktionscodes

Folgende Modbus Standard Funktionscodes werden vom Modbus Master unterstützt.

Element	Code	Typ	Bedeutung
READ COILS	01	BOOL	Lesen mehrerer Variablen (BOOL) aus dem Slave.
READ DISCRETE INPUTS	02	BOOL	Lesen mehrerer Variablen (BOOL) aus dem Slave.
READ HOLDING REGISTERS	03	WORD	Lesen mehrerer Variablen beliebigen Typs aus dem Slave.
READ INPUT REGISTERS	04	WORD	Lesen mehrerer Variablen beliebigen Typs aus dem Slave.
WRITE SINGLE COIL	05	BOOL	Schreiben eines einzelnen Signals (BOOL) in den Slave.
WRITE SINGLE REGISTER	06	WORD	Schreiben eines einzelnen Signals (WORD) in den Slave.
WRITE MULTIPLE COILS	15	BOOL	Schreiben mehrerer Variablen (BOOL) in den Slave.
WRITE MULTIPLE REGISTERS	16	WORD	Schreiben mehrerer Variablen beliebigen Typs in den Slave.
READ WRITE HOLDING REGISTERS	23	WORD	Schreiben und Lesen mehrerer Variablen beliebigen Typs in und aus dem Slave.

HINWEIS

Weitere Informationen zu Modbus finden Sie in der Spezifikation Modbus Application Protocol Specification *www.modbus.org*

SEW-spezifische Funktionscodes

Die SEW-spezifischen Funktionscodes entsprechen den Standard Modbus Funktionscodes. Die zwei Unterschiede sind die maximal zulässige Prozessdatenlänge von 1100 Bytes und das Format von Request und Response-Header.

Element	Code	Typ	Bedeutung
Read Coils Extended	100 (0x64)	BOOL	Entspricht dem Functioncode 01 Lesen mehrerer Variablen (BOOL) aus dem Import- oder Export)-Bereich des Slaves. Maximale Länge der Prozessdaten: 1100 Bytes
Read Discrete Inputs Extended	101 (0x65)	BOOL	Entspricht dem Functioncode 02 Lesen mehrerer Variablen (BOOL) aus dem Import- oder Export)-Bereich des Slaves. Maximale Länge der Prozessdaten: 1100 Bytes
Read Holding Registers Extended	102 (0x66)	WORD	Entspricht dem Functioncode 03 Lesen mehrerer Variablen (BOOL) aus dem Import- oder Export)-Bereich des Slaves. Maximale Länge der Prozessdaten: 1100 Bytes
Read Input Registers Extended	103 (0x67)	WORD	Entspricht dem Functioncode 04 Lesen mehrerer Variablen (BOOL) aus dem Import- oder Export)-Bereich des Slaves. Maximale Länge der Prozessdaten: 1100 Bytes

Element	Code	Typ	Bedeutung
Write Multiple Coils Extended	104 (0x68)	BOOL	Entspricht dem Functioncode 15 Schreiben mehrerer Variablen (BOOL) in den Import-Bereich des Slaves. Maximale Länge der Prozessdaten: 1100 Bytes
Write Multiple Registers Extended	105 (0x69)	WORD	Entspricht dem Functioncode 16 Schreiben mehrerer Variablen (BOOL) in den Import-Bereich des Slaves. Maximale Länge der Prozessdaten: 1100 Bytes
Read/Write Multiple Registers Extended	106 (0x6A)	WORD	Entspricht dem Functioncode 23 Schreiben und Lesen mehrerer Variablen beliebigen Typs in und aus dem Import-Bereich oder Export-Bereich des Slaves. Maximale Länge der Prozessdaten: 1100 Bytes (Anforderungstelegramm vom Modbus Master) 1100 Bytes (Antwort an den Master).

5.1.4 Format der Request und Response Header

Die Request und Response Header der SEW-spezifischen Modbus-Funktionscodes sind wie folgt aufgebaut:

Code	Request	Response
100 (0x64)	1 byte Functionscode 0x64 2 bytes Startadresse 2 bytes Anzahl von Coils 1 – 8800(0x2260)	1 byte Functionscode 0x64 2 bytes Anzahl von Bytes= N N bytes Coil-Daten (8 Coils werden in ein Byte gepackt)
101 (0x65)	1 byte Functionscode 0x65 2 bytes Startadresse 2 bytes Anzahl von Discrete Inputs 1 – 8800(0x2260)	1 byte Functionscode 0x65 2 bytes Anzahl von Bytes = N N bytes Discrete Inputs -Daten (8 Discrete Inputs werden in ein Byte gepackt)
102 (0x66)	1 byte Functionscode 0x66 2 bytes Startadresse 2 bytes Anzahl von Register 1 – 550(0x226)	1 byte Functionscode 0x66 2 bytes Anzahl von Bytes = N N bytes Register-Daten
103 (0x67)	1 bytes Functionscode 0x67 2 bytes Startadresse 2 bytes Anzahl von Register 1 – 550(0x226)	1 byte Functionscode 0x67 2 bytes Anzahl von Bytes = N N bytes Register-Daten
104 (0x68)	1 byte Functionscode 0x68 2 bytes Startadresse 2 bytes Anzahl von Coils 1 – 8800(0x2260) 2 bytes Anzahl von Bytes = N N bytes Coil-Daten	1 byte Functionscode 0x68 2 bytes Startadresse 2 bytes Anzahl von Coils 1 – 8800(0x2260)
105 (0x69)	1 byte Functionscode 0x69 2 bytes Startadresse 2 bytes Anzahl von Registern 1 – 550(0x226) 2 bytes Anzahl von Bytes = N N bytes Register-Daten	1 byte Functionscode 0x69 2 bytes Startadresse 2 bytes Anzahl von Registern 1 – 550(0x226)
106 (0x6A)	1 byte Functionscode 0x6a 2 bytes Lese-Startadresse 2 bytes Anzahl von Leseregistern 1 – 550(0x226) 2 bytes Schreib-Startadresse 2 bytes Anzahl von Schreibregistern 1 – 550(0x226) 2 bytes Anzahl von Bytes zum Schreiben=N N bytes Register-Daten	1 byte Functionscode 0x6a 2 bytes Anzahl von Bytes = N N bytes Register-Daten

5.1.5 Anforderungstelegramme zum Lesen

Mit den Read-Funktionscodes können Variablen aus dem Slave gelesen werden. Ein Anforderungstelegramm des Modbus Master enthält neben der Modbus Funktion die Startadresse des Lese-/Schreibbereichs.

Zum Lesen von Variablen sendet der Modbus Master ein Anforderungstelegramm zum Lesen an den Modbus Slave. Der Modbus Slave sendet daraufhin ein Antworttelegramm mit den angeforderten Variablen an den Modbus Master zurück.

So konfigurieren Sie ein Anforderungstelegramm zum Lesen:

1. Im Strukturbaum [Anforderungstelegramm] zum Konfigurieren auswählen.
2. Rechtsklick auf Anforderungstelegramm und im Kontextmenü [Edit] wählen.
3. In der Objektauswahl eine Globale Variable wählen, die als Modbus-Empfangsvariablen dienen soll und diese per Drag & Drop auf eine leere Stelle im Bereich Eingangssignale ziehen.
4. Diesen Schritt für jede weitere Modbus Empfangsvariable wiederholen.
5. Kontextmenü durch einen Rechtsklick auf eine leere Stelle im Bereich "Eingangssignale" öffnen und [Neue Offsets] wählen, um die Offsets der Variablen neu zu nummerieren.

Die folgenden Anforderungstelegramme zum Lesen stehen zur Verfügung:

Read Coils (01) und Extended (100)

Lesen mehrerer Variablen (BOOL) aus dem Slave.

Element	Bedeutung
Typ	Modbus-Funktion Read Coils
Name	Beliebiger, eindeutiger Name, für die Modbus -Funktion
Beschreibung	Beschreibung für die Modbus -Funktion
Startadresse des Lesebereichs	0 – 65535

Read Discrete Inputs (02) und Extended (101)

Lesen mehrerer Variablen (BOOL) aus dem Slave.

Element	Bedeutung
Typ	Modbus -Funktion Read Discrete Inputs
Name	Beliebiger, eindeutiger Name, für die Modbus -Funktion
Beschreibung	Beschreibung für die Modbus -Funktion
Startadresse des Lesebereichs	0 – 65535

Read Holding Registers (03) und Extended (102)

Lesen mehrerer Variablen beliebigen Typs aus dem Slave.

Element	Bedeutung
Typ	Modbus -Funktion Read Holding Registers
Name	Beliebiger, eindeutiger Name, für die Modbus -Funktion
Beschreibung	Beschreibung für die Modbus -Funktion
Startadresse des Lesebereichs	0 – 65535

Read Input Registers (04) und Extended (103)

Lesen mehrerer Variablen beliebigen Typs aus dem Slave

Element	Bedeutung
Typ	Modbus Funktion Read Input Registers
Name	Beliebiger, eindeutiger Name, für die Modbus Funktion
Beschreibung	Beschreibung für die Modbus Funktion
Startadresse des Lesebereichs	0 – 65535

5.1.6 Anforderungstelegramm zum Lesen und Schreiben

Zum Lesen und Schreiben von Variablen sendet der Modbus Master ein Anforderungstelegramm zum Lesen und Schreiben an den Modbus Slave.

Zuerst schreibt der Modbus Master die definierten Schreibvariablen in den definierten Import-Bereich des Modbus Slave.

Anschließend liest der Modbus Master die definierten Lesevariablen aus dem definierten Export-Bereich des Modbus Slave.

HINWEIS

Die Funktionen Schreiben und Lesen sind auch bei dem Anforderungstelegramm zum Lesen und Schreiben voneinander unabhängig, sie werden nur in einem gemeinsamen Anforderungstelegramm gesendet.

Eine häufige Anwendung für das Anforderungstelegramm zum Lesen und Schreiben ist jedoch, dass die geschriebenen Variablen des Modbus Master wieder zurückgelesen werden. Damit wird überprüft, ob die gesendeten Variablen korrekt geschriebenen wurden.

So konfigurieren Sie ein Anforderungstelegramm zum Lesen und Schreiben:

1. Im Strukturbaum [Anforderungstelegramm] zum konfigurieren auswählen.
2. Rechtsklick auf Anforderungstelegramm und im Kontextmenü [Edit] wählen.

So konfigurieren Sie die Variablen zum Lesen:

1. Wählen Sie in der Objektauswahl eine Globale Variable, die Sie mit der neuen Modbus Empfangsvariablen verbinden wollen und ziehen Sie diese per Drag & Drop in die Spalte "Globale Variable" der Modbus Empfangsvariablen.
2. Schritt 1 für jede weitere Modbus Empfangsvariable wiederholen.
3. Kontextmenü durch einen Rechtsklick auf eine leere Stelle im Bereich "Eingangssignale" öffnen und [Neue Offsets wählen], um die Offsets der Variablen neu zu nummerieren.

So konfigurieren Sie die Variablen zum Schreiben:

1. Wählen Sie in der Objektauswahl eine Globale Variable, die Sie mit der neuen Modbus Sendevariablen verbinden wollen und ziehen Sie diese per Drag & Drop in die Spalte Globale Variable der Modbus Sendevariablen.
2. Schritt 1 für jede weitere Modbus Sendevariable wiederholen.
3. Kontextmenü durch einen Rechtsklick auf eine leere Stelle im Bereich "Ausgangssignale" öffnen und [Neue Offsets] wählen, um die Offsets der Variablen neu zu nummerieren.

Read Write Holding Register (23) und Extended (106)

Schreiben und Lesen mehrerer Variablen beliebigen Typs in und aus dem Import-Bereich des Slaves.

Element	Bedeutung
Typ	Modbus-Funktion *Read Write Holding Registers*
Name	Beliebiger, eindeutiger Name, für die Modbus-Funktion
Beschreibung	Beschreibung für die Modbus-Funktion
Startadresse des Lesebereichs	0 – 65535
Startadresse des Schreibbereichs	0 – 65535

5.1.7 Anforderungstelegramm zum Schreiben

Mit den Write-Funktionscodes werden Variablen nur in den Importbereich eines Slaves geschrieben.

Ein Anforderungstelegramm des Modbus Master enthält neben der Modbus-Funktion die Startadresse des Lese-/Schreibbereichs.

Zum Schreiben von Variablen sendet der Modbus Master ein Anforderungstelegramm zum Schreiben an den Modbus Slave. Der Modbus Slave schreibt die empfangenen Variablen in seinen Import-Bereich.

Im Dialog Variablen zuweisen eines Anforderungstelegramms zum Schreiben müssen die Variablen eingefügt werden, die der Modbus Master zum Modbus Slave schreibt.

So konfigurieren Sie ein Anforderungstelegramm zum Schreiben:

1. Im Strukturbaum [Anforderungstelegramm] zum Konfigurieren auswählen.
2. Rechtsklick auf Anforderungstelegramm und im Kontextmenü [Edit] wählen.
3. In der Objektauswahl eine Globale Variable wählen, die als Modbus Sendevariable dienen soll und diese per Drag & Drop auf eine leere Stelle im Bereich "Sendesignale" ziehen.
4. Schritt 3 für jede weitere Modbus Sendevariable wiederholen.
5. Kontextmenü durch einen Rechtsklick auf eine leere Stelle im Bereich "Sendesignale" öffnen und [Neue Offsets] wählen, um die Offsets der Variablen neu zu nummerieren.

Die folgenden Anforderungstelegramme zum Schreiben stehen zur Verfügung:

Write Multiple Coils (15) und Extended (104)

Schreiben mehrerer Variablen (BOOL) in den Import-Bereich des Slaves.

Element	Bedeutung
Typ	Modbus Funktion *Write Multiple Coils*
Name	Beliebiger, eindeutiger Name, für die Modbus -Funktion
Beschreibung	Beschreibung für die Modbus -Funktion
Startadresse des Schreibbereichs	0 – 65535

Write Multiple Registers (16) und Extended (105)

Schreiben mehrerer Variablen beliebigen Typs in den Import-Bereich des Slaves.

Element	Bedeutung
Typ	Modbus Funktion *Write Multiple Registers*
Name	Beliebiger, eindeutiger Name, für die Modbus -Funktion
Beschreibung	Beschreibung für die Modbus -Funktion
Startadresse des Schreibbereichs	0 – 65535

Write Single Coil (05)

Schreiben einer einzelnen Variablen (BOOL) in den Import-Bereich des Slaves.

Element	Bedeutung
Typ	Modbus Funktion *Write Single Coil*
Name	Beliebiger, eindeutiger Name, für die Modbus -Funktion
Beschreibung	Beschreibung für die Modbus -Funktion
Startadresse des Schreibbereichs	0 – 65535

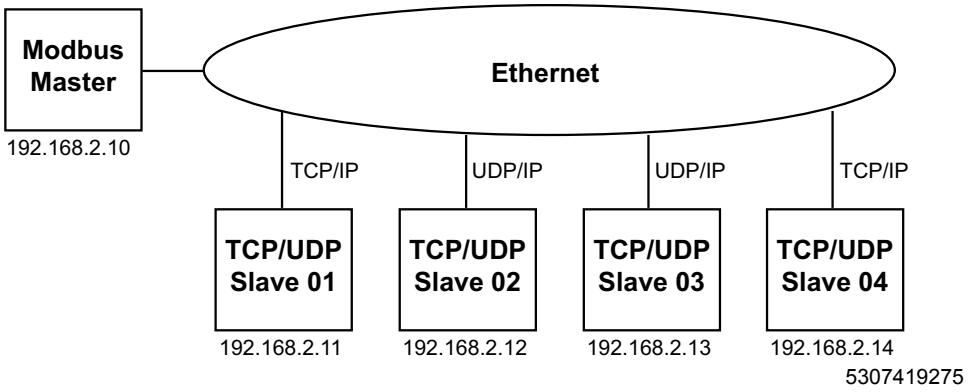
Write Single Register (06)

Schreiben einer einzelnen Variablen (WORD) in den Import-Bereich des Slaves.

Element	Bedeutung
Typ	Modbus Funktion *Write Single Register*
Name	Beliebiger, eindeutiger Name, für die Modbus -Funktion
Beschreibung	Beschreibung für die Modbus -Funktion
Startadresse des Schreibbereichs	0 – 65535

5.1.8 Ethernet Slaves (TCP/UDP-Slaves)

Der Modbus Master kann mit bis zu 64 TCP/IP und 247 UDP/IP Slaves kommunizieren.



So erstellen Sie im Modbus Master eine neue Verbindung zu einem TCP/UDP Slave:

1. Im Strukturbaum [Ressource] / [Protokolle] / [Modbus Master] / [Ethernet-Slaves] öffnen.
2. Rechtsklick auf Ethernet-Slaves und im Kontextmenü [Neu] wählen.
3. Aus der Liste "TCP/UDP-Slaves" wählen und mit [OK] bestätigen.
4. Konfiguration des TCP/UDP-Slave im Modbus Master:

   [Edit] zum Zuweisen der Systemvariablen, siehe Kapitel "Systemvariablen der TCP/UDP-Slaves"

   [Eigenschaften] wählen zum Konfigurieren der Eigenschaften, siehe Kapitel "Eigenschaften TCP/UDP-Slaves".

HINWEIS

Befinden sich die TCP/UDP-Slaves und der Modbus Master in verschiedenen Subnetzen, müssen in der Routing-Tabelle die entsprechenden benutzerdefinierten Routen eingetragen werden.

Der Modbus TCP Master sendet mit seinen Telegrammen an den Modbus TCP Slave zusätzlich zur IP-Adresse immer eine Modbus Slave Adresse (Unit Identifier) mit. Diese Adresse ist immer FF_{Hex} (255).

Systemvariablen der TCP/UDP-Slaves

Das Register Systemvariablen stellt Systemvariablen bereit, die es erlauben, den Zustand des TCP/UDP Slave im Anwenderprogramm auszuwerten und zu steuern.

Der Status des TCP/UDP Slave kann im Anwenderprogramm mit den folgenden Statusvariablen ausgewertet werden:

Element	Beschreibung	
Modbus-Slave Aktivierungssteuerung	Hiermit kann der TCP/UDP Slave vom Anwenderprogramm deaktiviert oder aktiviert werden.	0: Aktivieren 1: Deaktivieren (Flankengetriggert! Modbus Slave kann über PADT auch dann aktiviert werden wenn Modbus-Slave Aktivierungssteuerung = 1.)
Modbus-Slave Fehler	Fehlercode	Die Fehlercodes 0x01 – 0x0b entsprechen den Exception Codes der Modbus-Protokollspezifikation. 0x00: Kein Fehler
	Exception Codes:	0x01: Ungültiger Funktionscode 0x02: Ungültige Adressierung 0x03: Ungültige Daten 0x04: (nicht verwendet) 0x05: (nicht verwendet) 0x06: Device Busy (nur Gateway, nicht unterstützt) 0x08: (nicht verwendet) 0x0a: (nicht verwendet) 0x0b: No Response from Slave (nur Gateway, nicht unterstützt)
	SEW-spezifische Codes	0x10: Defekter Frame empfangen 0x11: Frame mit falscher Transaktions ID empfangen 0x12: Unerwartete Antwort empfangen 0x13: Antwort über falsche Verbindung erhalten 0x14: Falsche Antwort auf einen Schreibauftrag 0xff: Slave Timeout
Modbus-Slave Zustand	Verbindungsstatus des TCP/UDP Slave	0: Deaktiviert 1: Nicht verbunden 2: Verbunden

Eigenschaften TCP/UDP-Slaves

Zur Konfiguration der Verbindung zum TCP/UDP Slave müssen im Modbus Master die folgenden Parameter eingestellt werden:

Parameter	Beschreibung
Typ	TCP/UDP Slave
Name	Beliebiger eindeutiger Name für den TCP/UDP Slave
Beschreibung	Beliebige eindeutige Beschreibung für den TCP/UDP Slave
Master-Slave Datenaustausch [ms]	Intervall für den Datenaustausch mit diesem Slave 1 bis (2^{31}-1). Konnte der Slave nach Maximale Anzahl Sendewiederholungen nicht erreicht werden, wird das Intervall Master-Slave Datenaustausch um das Vierfache hochgesetzt.
TCP-Verbindung nur bei Bedarf	Wenn das Transportprotokoll TCP ist wird hier eingestellt, ob die Verbindung zu diesem Slave nach jedem Datenaustausch automatisch abgebaut werden soll. TRUE: Die Verbindung abbauen. FALSE: Die Verbindung nicht abbauen. Standardwert: FALSE
Receive Timeout [ms]	Receive Timeout für diesen Slave [ms]. Nach dieser Zeit wird ein neuer Sendeversuch gestartet.
IP-Adresse	IP-Adresse des TCP/UDP Slave
Port	Standard: 502 Es können auch andere TCP/UDP-Ports konfiguriert werden. Dabei ist die Port-Belegung bei der *Internet Corporation for Assigned Names and Numbers (ICANN)* zu beachten.
Kommunikationsart IP-Protokoll	TCP oder UDP Standardwert: TCP

Parameter	Beschreibung
Maximale Anzahl Sendewiederholungen	Maximale Anzahl an Sendewiederholungen, falls Slave nicht antwortet. Die Anzahl der Sendewiederholungen kann beliebig eingestellt werden (0 – 65535). Bei TCP/IP immer null, nicht änderbar. Empfohlen wird eine Anzahl von null bis acht Sendewiederholungen.

5.1.9 Control-Panel (Modbus Master)

Im Control-Panel kann der Anwender die Einstellungen des Modbus Master überprüfen und steuern. Zudem werden aktuelle Statusinformationen (z. B. Master-Zustand usw.) des Masters angezeigt.

So öffnen Sie das Control Panel zur Überwachung des Modbus Master:

1. Im Strukturbaum [Hardware] und im Kontextmenü [Online] wählen.
2. Im System-Login, Zugangsdaten eingeben um die Online Ansicht der Hardware zu öffnen.
3. Doppelklick auf "COM-Modul" und im Strukturbaum [Modbus Master] wählen.

Kontextmenü (Modbus Master)

Aus dem Kontextmenü des selektierte Modbus Master können die folgenden Kommandos gewählt werden:

Offline: Mit diesem Kommando wird der Modbus Master gestoppt.

Operate: Mit diesem Kommando wird der Modbus Master gestartet.

Statistik zurücksetzen: Setzt die statistischen Daten (z. B. Anzahl Busfehler, Zykluszeit min, max usw.) auf null zurück.

Anzeigefeld (Modbus Master)

In dem Anzeigefeld werden die folgenden Werte des selektierten Modbus Master angezeigt.

Element	Beschreibung
Name	Name des Modbus Masters
Master-Zustand	Der Modbus Master Zustand zeigt den momentanen Protokollzustand an: OPERATE OFFLINE
Anzahl Busfehler	Zähler Anzahl der Busfehler
Gestörte Verbindungen	Zähler Anzahl der gestörte Verbindungen
µP-Last (projektierte)	siehe Eigenschaften im Kapitel "Menüfunktionen des Modbus Master"
µP-Last (tatsächliche)	

5.1.10 Control-Panel (Modbus Master->Slave)

Im Control-Panel kann der Anwender die Einstellungen der Kommunikationspartner des Modbus Master überprüfen und aktivieren/deaktivieren.

Zudem werden aktuelle Statusinformationen (z. B. Slave-Zustand usw.) des Kommunikationspartners angezeigt.

So öffnen Sie das Control Panel zur Überwachung der Modbus Verbindung:

- Im Strukturbaum [Hardware] und im Kontextmenü [Online] wählen.
- Im System-Login, Zugangsdaten eingeben um die Online Ansicht der Hardware zu öffnen.
- Doppelklick auf "COM-Modul" und im Strukturbaum [Modbus Master] / [Slave] wählen.

6 Com-User Task (CUT)

Neben dem Anwenderprogramm, das mit SILworX erstellt wird, kann zusätzlich ein C-Programm auf der Steuerung betrieben werden. Dieses nicht sichere C-Programm läuft als Com-User Task rückwirkungsfrei zum sicheren Prozessormodul auf dem Kommunikationsmodul der Steuerung.

Die Com-User Task hat einen eigenen Zyklus, der unabhängig vom Zyklus der CPU ist.

6.1 Eigenschaften der CUT

Die folgende Tabelle beschreibt die Eigenschaften der CUT

Element	Beschreibung
Com-User Task	Es kann für jede Sicherheitssteuerung eine Com-User Task konfiguriert werden.
Sicherheitsgerichtet	Nein

6.2 Voraussetzung

Um ein SILworX-Programm mit einer Com-User Task zu erstellen, benötigen Sie Folgendes:

- Firmware:

  CUT PFF-HM31, Sachnummer: 28202430.xx

  Beachten Sie hierzu das Handbuch "Com-User Task für PFF-HM31A".

- Software, die **nicht** im Lieferumfang enthalten ist:

  Sie können diese Software zusammen mit der Dokumentation auf einem Datenträger (CD/DVD) von SEW-EURODRIVE unter folgenden Bestellangaben beziehen:

Bezeichnung	Sachnummer
SILWorX für PFF-HM31A • Hardware: SILWorX Lizenz Dongle • Software: SILWorX ab 4.64.0	1 950 011 4
Motion Library PFF-HM31 Bausteinbibliothek für die sichere Wegmessung / Function block library for safety related position detection	1 710 640 0

- Zur Diagnose der Com-User-Task-Anwendungen benötigen Sie als Software das MOVIVISION® Parameter- und Diagnosetool Version 2.0 (ebenfalls nicht im Lieferumfang enthalten).

7 Betriebssystem

Das Betriebssystem enthält alle Grundfunktionen der Sicherheitssteuerung

Welche Anwenderfunktionen das jeweilige PES ausführen soll, ist im Anwenderprogramm vorgegeben. Ein Codegenerator übersetzt das Anwenderprogramm in den Maschinencode. Das Programmierwerkzeug überträgt diesen Maschinencode in den Flash-Speicher der Steuerung.

7.1 Funktionen des Prozessor-Betriebssystems

Die wesentlichen Funktionen des Betriebssystems für das Prozessorsystem und die Verbindungen mit dem Anwenderprogramm sind in nachfolgender Tabelle aufgezeigt.

Funktionen des Betriebssystems	Verbindungen zum Anwenderprogramm
Zyklisches Abarbeiten des Anwenderprogramms.	Wirkt auf Variablen, Funktionsbausteine.
Konfiguration des Automatisierungsgeräts.	Festlegung durch Auswahl der Steuerung.
Prozessor-Tests.	-
Tests von E/A-Modulen.	-
Reaktionen im Fehlerfall.	Fest vorgegeben. Das Anwenderprogramm ist für Prozessreaktion verantwortlich.
Diagnose für Prozessorsystem und Ein-/Ausgänge.	Verwendung der Systemsignale/-variablen für Fehlermeldungen.
Sichere Kommunikation: • Peer-to-Peer Nicht sichere Kommunikation: • Modbus	Festlegung der Verwendung von Kommunikationssignalen/-variablen.
PADT-Schnittstelle: • Zulässige Aktionen	Festlegung im Programmierwerkzeug: • Konfiguration von Schutzfunktionen • Einloggen des Anwenders

Jedes Betriebssystem wird vom zuständigen TÜV geprüft und für den Betrieb mit der sicherheitsgerichteten Steuerung zugelassen. Die jeweils gültigen Versionen des Betriebssystems und die dazugehörigen Signaturen (CRCs) sind auf einer Liste dokumentiert, die SEW-EURODRIVE gemeinsam mit dem TÜV erstellt.

7.2 Verhalten bei Auftreten von Fehlern

Wichtig ist die Reaktion auf Fehler, die durch Tests festgestellt wurden. Zu unterscheiden sind folgende Arten von Fehlern.

- Permanente Fehler bei Eingängen und Ausgängen
- Vorübergehende Fehler bei Eingängen und Ausgängen
- Interne Fehler

7.2.1 Permanente Fehler bei Eingängen und Ausgängen

Ein Fehler, der in einem Eingangs- oder Ausgangskanal auftritt, beeinflusst die Steuerung nicht. Das Betriebssystem betrachtet nur den defekten Kanal als fehlerhaft und nicht die ganze Steuerung. Die übrigen Sicherheitsfunktionen werden davon nicht beeinflusst und bleiben aktiv.

Bei fehlerhaften Eingangskanälen gibt das Betriebssystem den sicheren Wert "0" oder den Initialwert an die Verarbeitung weiter.

Fehlerhafte Ausgangskanäle setzt das Betriebssystem in den energielosen Zustand. Ist es nicht möglich, nur einen Kanal abzuschalten, wird das ganze Ausgangsmodul als fehlerhaft betrachtet.

Das Betriebssystem setzt das Fehlerstatus-Signal und meldet dem Anwenderprogramm die Art des Fehlers.

Kann die Steuerung einen entsprechenden Ausgang nicht abschalten und wird auch der 2. Abschaltweg nicht wirksam, geht die Steuerung in STOPP. Der Watchdog des Prozessorsystems schaltet dann die Ausgänge ab.

Treten in den E/A-Modulen Fehler auf, die länger als 24 Stunden anstehen, schaltet die Steuerung nur die betroffenen E/A-Module permanent ab.

7.2.2 Vorübergehende Fehler bei Eingängen und Ausgängen

Tritt ein Fehler in einem Eingangs- oder Ausgangsmodul auf und verschwindet von selbst wieder, setzt das Betriebssystem den Fehlerstatus zurück und nimmt den normalen Betrieb wieder auf.

Das Betriebssystem wertet die Häufigkeit des Auftretens der Fehler statistisch aus. Es setzt den Status des Moduls ständig auf fehlerhaft, wenn die vorgegebene Fehlerhäufigkeit überschritten wird. Dadurch arbeitet das Modul auch nach Verschwinden des Fehlers nicht mehr. Die Freigabe des Moduls und die Löschung der Fehlerstatistik erfolgt mit dem Wechsel des Betriebszustandes der Steuerung von STOPP auf RUN. Diese Änderung quittiert den Fehler des Moduls.

7.2.3 Interne Fehler

HINWEIS

Sollte der seltene Fall auftreten, dass eine Sicherheitssteuerung einen internen Fehler feststellt, wird folgende Fehlerreaktion ausgeführt:

Die Sicherheitssteuerung läuft automatisch wieder hoch.

Sollte nach dem Hochlaufen innerhalb einer Minute wieder ein interner Fehler auftreten, so bleibt die Sicherheitssteuerung im Zustand STOPP/UNGÜLTIGE KONFIGURATION.

8 Anwenderprogramm

Die Erstellung des Anwenderprogramms für das PES und das Laden müssen mit einem Programmiergerät mit dem installierten Programmierwerkzeug SILworX nach den Erfordernissen der IEC 61131-3 erfolgen.

Zuerst ist mit dem Programmierwerkzeug das Anwenderprogramm zu erstellen und für den sicherheitsgerichteten Betrieb der Steuerung zu konfigurieren. Dabei sind die Vorgaben des Sicherheitshandbuchs "Dezentrale Sicherheitssteuerung PFF-HM31A für MOVIPRO®" zu beachten.

Nach dem anschließenden Kompilieren lädt das Programmiergerät Anwenderprogramm (Logik) und Konfiguration (Verbindungsparameter wie IP-Adresse, Subnet Mask und System-ID) in die Steuerung und startet diese.

Das Programmiergerät bietet folgende Möglichkeiten, während des Betriebs der Steuerung mit dieser zu arbeiten:

- Starten und Stoppen des Anwenderprogramms
- Anzeigen und Forcen von Variablen/Signalen mit dem Force-Editor
- Im Testmodus Ausführen des Anwenderprogramms in Einzelschritten – nicht im sicherheitsgerichteten Betrieb
- Auslesen der Diagnosehistorie

Voraussetzung hierfür ist, dass das Programmiergerät dasselbe Anwenderprogramm enthält wie die Steuerung.

Für das Anwenderprogramm gibt es folgende optionale 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 und auch durch Reload laden.

- **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

Die optionalen Funktionen können in der Geräteoption PFF-HM31A1-E61-I111-00/000/000 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 Geräteoption mit den benötigten Funktionen.

8.1 Betriebsarten des Anwenderprogramms

In eine Steuerung kann nur jeweils ein Anwenderprogramm geladen werden. Für dieses Anwenderprogramm sind folgende Betriebsarten möglich:

Betriebsart	Beschreibung
RUN	Das Prozessorsystem ist in Betriebsart RUN. Das Anwenderprogramm wird zyklisch ausgeführt, E/A-Signale werden verarbeitet.
Testmodus (Einzelschritt)	Das Prozessorsystem ist in Betriebsart RUN. Das Anwenderprogramm wird auf manuelle Anforderung hin zyklusweise ausgeführt, E/A-Signale werden verarbeitet. **Nicht zulässig für sicherheitsgerichteten Betrieb!**
STOPP	Das Prozessorsystem ist in Betriebsart STOPP. Das Anwenderprogramm wird nicht (mehr) ausgeführt, die Ausgänge sind zurückgesetzt.
FEHLER	Ein geladenes Anwenderprogramm ist aufgrund eines Fehlers angehalten worden. Die Ausgänge sind zurückgesetzt. Hinweis: Ein Neustart des Programms ist nur durch das PADT möglich.

8.2 Allgemeines zum Forcen

Forcen bedeutet das Ersetzen des aktuellen Wertes einer Variablen durch einen Force-Wert. Eine Variable kann ihren aktuellen Wert aus folgenden Quellen erhalten:

- Durch einen physikalischen Eingang
- Durch die Kommunikation
- Durch eine logische Verknüpfung

Beim Forcen einer Variablen gibt der Anwender den Wert vor. Das Forcen wird in folgenden Fällen angewendet:

- Testen des Anwenderprogramms, besonders in Fällen, die selten auftreten und auf andere Weise nicht geprüft werden können.
- Simulation nicht verfügbarer Sensoren in Fällen, in denen der Initialwert nicht angemessen ist.

⚠ WARNUNG!

Personenschäden durch geforcte Werte möglich!

Tod oder schwere Körperverletzung möglich.

- Werte nur nach Absprache mit der Prüfstelle für die Anlagenabnahme forcen.
- Einschränkungen des Forcens nur nach Absprache mit der Prüfstelle für die Anlagenabnahme aufheben.

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

⚠ 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.

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

Grundlegende Informationen zum Forcen werden im Dokument „Maintenance Override“ des TÜV gegeben. Das Dokument ist auf folgender Homepage des TÜV bereitgestellt:

http://www.tuv-fs.com oder http://www.tuvasi.com.

8.3 Forcen

Forcen kann auf zwei Ebenen erfolgen:

- Globales Forcen

  Globale Variablen werden für alle Verwendungen geforct

- Lokales Forcen

  Die Werte von lokalen Variablen eines Anwenderprogramms werden geforct

Damit eine globale oder lokale Variable geforct wird, müssen folgende Bedingungen erfüllt sein:

- Der zugehörige Force-Schalter ist gesetzt
- Das Forcen wurde gestartet

Ist das Forcen gestartet, wirkt eine Änderung des Force-Schalters sofort. Ist das Forcen gestartet und der Force-Schalter gesetzt, wirkt eine Änderung des Force-Werts sofort. Das lokale Forcen lässt sich für jedes Anwenderprogramm getrennt starten und stoppen.

8.3.1 Zeitbegrenzung

Für das globale wie für das lokale Forcen sind unterschiedliche Zeitbegrenzungen einstellbar. Nach Ablauf der eingestellten Zeit beendet die Steuerung das Forcen. Das Verhalten der Sicherheitssteuerung nach dem Ablauf der Zeitbegrenzung ist einstellbar.

- Beim globalen Forcen sind folgende Einstellungen wählbar:
  - Die Ressource stoppt
  - Die Ressource läuft weiter
- Beim lokalen Forcen sind folgende Einstellungen wählbar:
  - Das Anwenderprogramm stoppt
  - Das Anwenderprogramm läuft weiter

Es ist auch möglich, ohne Zeitbegrenzung zu forcen. In diesem Fall ist das Forcen von Hand zu beenden. Nach dem Ende des Forcens einer Variablen gilt wieder der Prozesswert.

8.3.2 Force-Editor

Der Force-Editor von SILworX zeigt alle Variablen an, für die Forcen möglich ist. Dabei werden die globalen und lokalen Variablen getrennt in unterschiedlichen Registern angezeigt. In den Registern ist das Einstellen von Force-Werten und Setzen von Force-Schaltern möglich.

8.3.3 Einschränkung des Forcens

Um eventuelle Störungen des sicherheitsgerichteten Betriebs durch unzulässiges Forcen zu vermeiden, können in der Konfiguration folgende Maßnahmen getroffen werden, die die Benutzung des Forcens einschränken.

- Einrichtung unterschiedlicher Benutzerkonten mit und ohne Erlaubnis zum Forcen
- Verbieten des globalen Forcens für eine Ressource
- Verbieten des lokalen Forcens, bzw. der Prozesswert-Eingabe
- Zusätzlich kann das Forcen per Schlüsselschalter unmittelbar abgeschaltet werden. Hierzu muss die Systemvariable *Force-Deaktivierung* mit einem digitalen Eingang verbunden sein, an den ein Schlüsselschalter angeschlossen ist.

  Die Systemvariable *Force-Deaktivierung* verhindert, dass das Forcen für globale und lokale Variable gestartet wird und schaltet bereits gestartetes Forcen unmittelbar ab.

9 Inbetriebnahme

Die Inbetriebnahme der Sicherheitssteuerung besteht aus folgenden Phasen:

- Mechanische Installation. Beachten Sie dazu das Kapitel "Mechanische Installation" in der Betriebsanleitung "Dezentrale Sicherheitssteuerung PFF-HM31A"
- Elektrische Installation. Beachten Sie dazu das Kapitel "Elektrische Installation" in der Betriebsanleitung "Dezentrale Sicherheitssteuerung PFF-HM31A"
- Konfiguration
  - Erstellung des Anwenderprogramms
  - Festlegung von Sicherheits-, Kommunikations- und anderen Parametern

9.1 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_HM31_Checkliste.pdf* kann als PDF-Dokument auf der SEW-Homepage (www.sew-eurodrive.de) unter der Rubrik "Dokumentationen" im Bereich "safetyDrive" heruntergeladen werden.

9.2 Konfiguration mit SILworX

Der Hardware-Editor des Programmierwerkzeugs SILworX zeigt die PFF-HM31A ähnlich einem Basisträger, bestückt mit folgenden Modulen:

- Prozessormodul (CPU)
- Kommunikationsmodul (COM)
- Digitales Eingangsmodul (DI 26)
- Digitales Ausgangsmodul (DO 8)
- Zählermodul (HSC 2)

Durch Doppelklicken auf die Module öffnet sich die Detailansicht mit Registern. In den Registern können die im Anwenderprogramm konfigurierten globalen Variablen den Systemvariablen des jeweiligen Moduls zugeordnet werden.

9.2.1 Prozessormodul

Durch Doppelklicken auf die Module öffnet sich die Detailansicht mit Registern. In den Registern können die im Anwenderprogramm konfigurierten globalen Variablen den Systemvariablen des jeweiligen Moduls zugeordnet werden.

Register Modul

Das Register Modul enthält die folgenden Parameter.

Parameter	Beschreibung
Name	Name des Moduls

Parameter	Beschreibung
Max. µP-Budget für HH-Protokoll verwenden	• Aktiviert: Limit der CPU-Last aus dem Feld *Max. µP-Budget für HH-Protokoll [%]* übernehmen. • Deaktiviert: Kein Limit der CPU-Last für safeethernet verwenden. Standardeinstellung: Deaktiviert
Max. µP-Budget für HH-Protokoll [%]	Maximale CPU-Last des Moduls, welche bei der Abarbeitung des safeethernet Protokolls produziert werden darf. **Hinweis:** Die Maximale Last muss unter allen verwendeten Protokollen aufgeteilt werden, welche dieses Kommunikationsmodul benutzen.
IP Adresse	IP-Adresse der Ethernet-Schnittstelle. Standardwert: 192.168.0.99
Subnet Mask	32-Bit-Adressmaske zur Unterteilung einer IP-Adresse in Netzwerk- und Host-Adresse. Standardwert: 255.255.252.0
Standard-Schnittstelle	Aktiviert: Schnittstelle wird als Standardschnittstelle für ein System-Login verwendet. Standardeinstellung: Deaktiviert
Default-Gateway	IP-Adresse des Default Gateway. Standardwert: 0.0.0.0
ARP Aging Time [s]	Ein CPU- oder COM-Modul speichert die MAC-Adressen seiner Kommunikationspartner in einer MAC-/IP Adresse Zuordnungstabelle (ARP-Cache). Wenn während einer Zeitspanne von 1×…2× *ARP Aging Time* • Nachrichten vom Kommunikationspartner eintreffen, bleibt die MAC-Adresse im ARP-Cache erhalten. • Keine Nachrichten vom Kommunikationspartner eintreffen, wird die MAC-Adresse aus dem ARP-Cache gelöscht. Der typische Wert für die *ARP Aging Time* in einem lokalen Netzwerk ist 5 s – 300 s. Der Inhalt des ARP-Cache kann vom Anwender nicht ausgelesen werden. Bei der Verwendung von Routern oder Gateways *ARP Aging Time* an die zusätzlichen Verzögerungen für Hin- und Rückweg anpassen (erhöhen). Bei zu geringer *ARP Aging Time* löscht das CPU-/COM-Modul die MAC-Adresse des Kommunikationspartners aus dem ARP-Cache und die Kommunikation wird nur verzögert ausgeführt oder bricht ab. Für einen effizienten Einsatz muss die *ARP Aging Time* größer als die *ReceiveTimeouts* der verwendeten Protokolle sein. Wertebereich: 1 s – 3600 s Standardwert: 60 s
MAC Learning	Lernverhalten des ARP-Cache: • konservativ: MAC-Adressen gespeicherter ARP-Einträge werden durch empfangene Meldungen nicht überschrieben. • tolerant: MAC-Adressen gespeicherter ARP-Einträge werden durch empfangene Meldungen überschrieben. Standardeinstellung: konservativ
IP Forwarding	Ermöglicht einem Prozessormodul, als Router zu arbeiten und Datenpakete anderer Netzwerkknoten weiterzuleiten. Standardeinstellung: Deaktiviert
ICMP Mode	Meldungstypen des Internet Control Message Protocol (ICMP), die vom Prozessormodul unterstützt werden: • Keine ICMP-Antworten • Echo Response • Host unerreichbar • Alle implementierten ICMP-Antworten Standardeinstellung: Echo Response
Max. Kom. Zeitscheibe ASYNC [ms]	Höchstwert in ms der Zeitscheibe, die innerhalb des Zyklus der Ressource für Kommunikation verwendet wird. Einstellbereich: 2 – 5000 ms
Max. Dauer Konfigurationsverbindungen [ms]	Definiert, wie viel Zeit innerhalb eines CPU-Zyklus für die Prozessdaten-Kommunikation zur Verfügung steht. Einstellbereich: 6 – 5000 ms
Sollzykluszeit [ms]	Gewünschte oder maximale Zykluszeit, siehe *Sollzykluszeit- Modus*. Die *Sollzykluszeit* darf höchstens so groß sein wie die eingestellte Watchdog-Zeit (6 ms), andernfalls lehnt das PES sie ab. Einstellbereich: 0 – 7500 ms

Parameter	Beschreibung
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 der Reload-Funktion (Funktion als Geräteoption verfügbar) 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 der Reload-Funktion (Funktion als Geräteoption verfügbar) findet die *Sollzykluszeit* keine Beachtung.
Maximale Systembus-Latenzzeit [µs]	Für die Sicherheitssteuerung PFF-HM31A nicht anwendbar!
safeethernet-CRC	**Aktuelle Version:** Die Bildung des CRC für safeethernet erfolgt mit dem aktuellen Algorithmus.

Register Routings

Das Register Routings enthält die folgenden Parameter.

Parameter	Beschreibung
Name	Bezeichnung der Routing-Einstellung
IP Adresse	Ziel IP-Adresse des Kommunikationspartners (bei direktem Host-Routing) oder Netzwerkadresse (bei Subnet Routing). Wertebereich: 0.0.0.0 – 255.255.255.255 Standardwert: 0.0.0.0
Subnet Mask	Definiert Ziel-Adressbereich für einen Routing-Eintrag. 255.255.255.255 (bei direktem Host-Routing) oder Subnet Mask des adressierten Subnet. Wertebereich: 0.0.0.0...255.255.255.255 Standardwert: 255.255.255.255
Gateway	IP-Adresse des Gateways zum adressierten Netzwerk. Wertebereich: 0.0.0.0...255.255.255.255 Standardwert: 0.0.0.1

Register Ethernet-Switch

Das Register Ethernet-Switch enthält die folgenden Parameter.

Parameter	Beschreibung
Name	Name des Ports (Eth1 – Eth4) wie Gehäuseaufdruck; pro Port darf nur eine Konfiguration vorhanden sein.
Speed [Mbit/s]	10 Mbit/s: Datenrate 10 Mbit/s 100 Mbit/s: Datenrate 100 Mbit/s 1000 Mbit/s: Datenrate 1000 Mbit/s (wird nicht unterstützt) Autoneg: Automatische Einstellung der Baudrate Standardwert: Autoneg
Flow-Control	Vollduplex: Kommunikation in beide Richtungen gleichzeitig Halbduplex: Kommunikation in eine Richtung Autoneg: Automatische Kommunikationssteuerung Standardwert: Autoneg
Autoneg auch bei festen Werten	Das *Advertising* (Übermitteln der Speed und Flow-Control Eigenschaften) wird auch bei fest eingestellten Werten von *Speed* und *Flow-Control* durchgeführt. Hierdurch erkennen andere Geräte, deren Ports auf *Autoneg* eingestellt sind, die Einstellung der Ports der Sicherheitssteuerung.
Limit	Eingehende Multicast- und/oder Broadcast-Pakete limitieren. Aus: keine Limitierung Broadcast: Broadcast limitieren (128 kbit/s) Multicast und Broadcast: Multicast und Broadcast limitieren (1024 kbit/s) Standardwert: Broadcast

Register VLAN (Port-Based LAN)

Konfiguriert die Verwendung von Port-based VLAN.

HINWEIS

Soll VLAN unterstützt werden, muss Port-based VLAN abgeschaltet sein, so dass jeder Port mit jedem anderen Port des Switches kommunizieren kann.

Für jeden Port eines Switches kann eingestellt werden, zu welchem anderen Port des Switches empfangene Ethernet Frames gesendet werden dürfen. Die Tabelle im Register VLAN enthält Einträge, mit denen die Verbindung zwischen zwei Ports aktiv oder inaktiv geschaltet werden kann.

	Port				
Port (Ethernet-Schnittstelle an PFF-HM31A)	**Eth 1 (X4233_1)**	**Eth 2 (X4233_2)**	**Eth 3 (X4223)**	**Eth 4**	**COM**
Eth 1 (X4233_1)					
Eth 2 (X4233_2)	aktiv				
Eth 3 (X4223)	aktiv	aktiv			
Eth 4	aktiv	aktiv	aktiv		
COM	aktiv	aktiv	aktiv	aktiv	
CPU	aktiv	aktiv	aktiv	aktiv	aktiv

HINWEIS

Port Eth 4 ist ohne Funktion.

Register LLDP

LLDP (Link Layer Discovery Protocol) sendet per Multicast in periodischen Abständen Informationen über das eigene Gerät (z. B. MAC-Adresse, Gerätename, Portnummer) und empfängt die gleichen Informationen von Nachbargeräten.

Das Prozessor- und das Kommunikationsmodul unterstützen LLDP auf den Ports Eth1, Eth2 und Eth3. Einstellungen für Port Eth4 sind ohne Funktion.

Die folgenden Parameter legen fest, wie der betreffende Port arbeitet.

- Aus

  LLDP ist auf diesem Port deaktiviert.

- Send

  LLDP sendet LLDP Ethernet Frames, empfangene LLDP Ethernet Frames werden gelöscht, ohne diese zu verarbeiten.

- Receive

  LLDP sendet keine LLDP Ethernet Frames, aber empfangene LLDP Frames werden verarbeitet.

- Send/Receive

  LLDP sendet und verarbeitet empfangene LLDP Ethernet Frames.

Register Mirroring

Konfiguriert, ob das Modul Ethernet-Pakete auf einen Port dupliziert, so dass sie von einem dort angeschlossenen Gerät mitgelesen werden können, z. B. zu Testzwecken.

Die folgenden Parameter legen fest, wie der betreffende Port arbeitet.

- Aus

  Dieser Port nimmt am Mirroring nicht teil.

- Egress

Ausgehende Daten dieses Ports werden dupliziert.

- Ingress/Egress

  Ein- und ausgehende Daten dieses Ports werden dupliziert.

- Dest Port

  Duplizierte Daten werden auf diesen Port geschickt.

9.2.2 Kommunikationsmodul

Das Kommunikationsmodul (COM) enthält die Register "Modul" und "Routings" mit denselben Parametern wie das Prozessormodul. Der Standardwert der IP-Adresse ist hier 192.168.0.100.

9.2.3 Konfiguration der Ressource

Es sind die Eigenschaften der Ressource zu konfigurieren und die Ausgangsvariablen der Hardware.

Eigenschaften der Ressource

Diese Parameter legen das Verhalten der Steuerung während des Betriebs fest und werden in SILworX im Dialogfenster "Eigenschaften" der Ressource eingestellt.

Parameter/Schalter	Beschreibung	Standard-wert	Einstellung für sicheren Betrieb
Name	Name der Ressource		Beliebig
System ID [SRS]	System-ID der Ressource. Die System-ID muss einen anderen Wert als den Standardwert erhalten, sonst ist das Projekt nicht ablauffähig. Einstellbereich: 1 – 65535	60000	Eindeutiger Wert innerhalb des Netzwerks der Steuerungen, die potenziell miteinander verbunden sind.
Sicherheitszeit [ms]	Sicherheitszeit in Millisekunden. Einstellbereich: 20 – 22500 ms	600 ms	Applikationsspezifisch
Watchdog-Zeit [ms]	Watchdog-Zeit in Millisekunden. Einstellbereich: 8 – 5000 ms	200 ms	Applikationsspezifisch
Hauptfreigabe	Nur bei gestopptem PES ist es möglich, *Hauptfreigabe* auf "ON" zu setzen! **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* • *Reload-Funktion erlaubt (Funktion als Geräteoption verfügbar)* • *Start erlaubt* **OFF:** Die Parameter sind nicht im Betrieb änderbar.	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

Parameter/Schalter	Beschreibung	Standard-wert	Einstellung für sicheren Betrieb
Start erlaubt	**ON:** Kaltstart oder Warmstart durch PADT im Zustand RUN oder STOPP erlaubt. **OFF:** Kein Start erlaubt.	ON	Applikationsspezifisch
Laden erlaubt	**ON:** Download des Anwenderprogramms erlaubt. **OFF:** Download des Anwenderprogramms nicht erlaubt.	ON	Applikationsspezifisch
Reload	**ON:** Reload-Funktion (Funktion als Geräteoption verfügbar) des Anwenderprogramms erlaubt. **OFF:** Reload-Funktion (Funktion als Geräteoption verfügbar) des Anwenderprogramms nicht erlaubt. Ein laufendes Reload (Funktion als Geräteoption verfügbar) wird beim Umschalten auf OFF nicht abgebrochen.	ON	OFF empfohlen
Globales Forcen erlaubt	**ON:** Globales Forcen für diese Ressource erlaubt. **OFF:** Globales Forcen für diese Ressource nicht erlaubt.	ON	Applikationsspezifisch
Globale Force-Time-out-Reaktion	Legt fest, wie sich die Ressource beim Ablauf des globalen Force-Timeout verhält: • Forcen beenden • Ressource stoppen	Forcen beenden	Applikationsspezifisch
Max. Kom.Zeit-scheibe ASYNC [ms]	Höchstwert in ms der Zeitscheibe, die innerhalb des Zyklus der Ressource für Kommunikation verwendet wird. Einstellbereich: 2 – 5000 ms	60 ms	Applikationsspezifisch
Max. Dauer Konfigu-rationsverbindungen [ms]	Definiert, wieviel Zeit innerhalb eines CPU-Zyklus' für die Prozessdaten-Kommunikation zur Verfügung steht. Einstellbereich: 6 – 5000 ms	6 ms	-
Sollzykluszeit [ms]	Gewünschte oder maximale Zykluszeit, siehe *Sollzykluszeit-Modus*. Die *Sollzykluszeit* darf höchstens so groß sein wie die eingestellte *Watchdogzeit* (6 ms), andernfalls lehnt das PES sie ab. Einstellbereich: 0 – 7500 ms	0 ms	-
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 der Reload-Funktion (Funktion als Geräteoption verfügbar) findet die *Sollzykluszeit* keine Beachtung. **dynamisch-tolerant:** Wie bei dynamisch, aber beim 1. Aktivierungszyklus der Reload-Funktion (Funktion als Geräteoption verfügbar) findet die *Sollzykluszeit* keine Beachtung. **dynamisch:** Die Sicherheitssteuerung hält möglichst die *Sollzykluszeit* ein, führt aber den Zyklus in möglichst kurzer Zeit aus.	fest	-
Minimale Konfigurationsversion	-	SILworX V4	-

Parameter/Schalter	Beschreibung	Standard-wert	Einstellung für sicheren Betrieb
Maximale System-bus-Latenzzeit [µs]	Für die Sicherheitssteuerung nicht anwendbar.	0 ms	-
safeethernet-CRC	In der aktuellen Version erfolgt die Bildung des CRC für safeethernet mit dem aktuellen Algorith-mus.	Aktuelle Version	Applikationsspezifisch

Systemvariablen der Hardware zum Erstellen von Parametern

Diese Variablen dienen dazu, das Verhalten der Steuerung im laufenden Betrieb bei bestimmten Zuständen zu verändern. Diese Variablen befinden sich im Hardware-Editor von SILworX, in der Detailansicht der Hardware.

Variable	Funktion	Standard-einstellung	Einstellung für sicheren Betrieb
Force-Deaktivierung	Dient zum Verhindern und unmittelbaren Abschalten des Forcens.	FALSE	Applikationsspezifisch
Leer 2 – Leer 16	Keine Funktion.	-	-
Notaus 1 – Notaus 4	NOT-AUS-Schalter zum Abschalten der Steuerung in vom Anwenderprogramm erkannten Störfallen.	FALSE	Applikationsspezifisch
Ready-only in RUN	Nach dem Starten der Steuerung ist keine Bedienaktion (Stopp, Start, Download) über SILworX mehr möglich. Ausnahmen: Forcen und Reload-Funktion (Funktion als Geräteoption verfügbar).	FALSE	Applikationsspezifisch
Relaiskontakt 1 – 4	Keine Funktion.	-	-
Reload-Deaktivie-rung	Verhindert ein Laden der Steuerung mit-tels Reload-Funktion (Funktion als Geräteoption verfügbar).	FALSE	Applikationsspezifisch
User-LED 1 – 2	Steuert die entsprechende LED an, sofern vorhanden.	FALSE	Applikationsspezifisch

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

Systemvariablen der Hardware zum Auslesen von Parametern

Diese Systemvariablen sind im Hardware-Editor von SILworX zugänglich. Dazu den grauen Hintergrund außerhalb der (gelben) Baugruppenträger-Darstellung selektieren und die Detailansicht der Hardware durch Doppelklick oder über das Kontextmenü öffnen.

Variable	Beschreibung	Daten-typ
Anzahl I/O-Fehler	Anzahl aktueller E/A-Fehler.	UDINT
Anzahl I/O-Fehler historisch	Aufsummierte Anzahl E/A-Fehler (Zähler rücksetzbar).	UDINT
Anzahl aktueller E/A-Warnungen	Anzahl aktueller E/A-Warnungen.	UDINT
Anzahl aktueller E/A-Warnungen historisch	Aufsummierte Anzahl E/A-Warnungen (Zähler rücksetzbar).	UDINT
Anzahl Kommunikationsfehler	Anzahl aktueller Kommunikationsfehler.	UDINT
Anzahl Kommunikationsfehler his-torisch	Aufsummierte Anzahl Kommunikationsfehler (Zähler rücksetz-bar).	UDINT
Anzahl Kommunikationswarnungen	Anzahl aktueller Kommunikationswarnungen.	UDINT
Anzahl Kommunikationswarnungen historisch	Aufsummierte Anzahl Kommunikationswarnungen (Zähler rück-setzbar).	UDINT
Anzahl Systemfehler	Anzahl aktueller Systemfehler.	UDINT
Anzahl Systemfehler historisch	Aufsummierte Anzahl Systemfehler (Zähler rücksetzbar).	UDINT
Anzahl Systemwarnungen	Anzahl aktueller Systemwarnungen.	UDINT
Anzahl Systemwarnungen histo-risch	Aufsummierte Anzahl Systemwarnungen (Zähler rücksetzbar).	UDINT

Variable	Beschreibung	Datentyp
Autostart CPU Release	**ON:** Das Prozessorsystem startet beim Anlegen der Versorgungsspannung automatisch das Anwenderprogramm. **OFF:** Das Prozessorsystem geht beim Anlegen der Versorgungsspannung in den Zustand STOPP.	BOOL
BS Major	Ausgabe des Betriebssystems im Prozessorsystem.	UINT
BS Minor		UINT
CRC	Prüfsumme der Projektkonfiguration.	UDINT
Datum/Uhrzeit [ms-Anteil]	Systemdatum und -uhrzeit in s und ms seit 01.01.1970.	UDINT
Datum/Uhrzeit [Sek.-Anteil]		UDINT
Force-Deaktivierung	**ON:** Forcen ist deaktiviert. **OFF:** Forcen ist möglich.	BOOL
Forcen aktiv	**ON:** Globales oder lokales Forcen ist aktiv. **OFF:** Globales und lokales Forcen sind nicht aktiv.	BOOL
Force-Schalterzustand	Zustand der Force-Schalter. 0xFFFFFFFE: Kein Force-Schalter gesetzt 0xFFFFFFFF: Mindestens ein Force-Schalter gesetzt	UDINT
Globales Forcen gestartet	**ON:** Globales Forcen ist aktiv. **OFF:** Globales Forcen ist nicht aktiv.	BOOL
Leer 0 – 16	Reserviert	USINT
Leer ein17		BOOL
Letzte I/O-Warnung [ms]	Datum und Uhrzeit der letzten I/O-Warnung in s und ms seit 01.01.1970.	UDINT
Letzte I/O-Warnung [s]		UDINT
Letzte Kommunikationswarnung [ms]	Datum und Uhrzeit der letzten Kommunikationswarnung in s und ms seit 01.01.1970.	UDINT
Letzte Kommunikationswarnung [s]		UDINT
Letzte Systemwarnung [ms]	Datum und Uhrzeit der letzten Systemwarnung in s und ms seit 01.01.1970.	UDINT
Letzte Systemwarnung [s]		UDINT
Letzter I/O-Fehler [ms]	Datum und Uhrzeit des letzten I/O-Fehlers in s und ms seit 01.01.1970.	UDINT
Letzter I/O-Fehler [s]		UDINT
Letzter Kommunikationsfehler [ms]	Datum und Uhrzeit des letzten Kommunikationsfehlers in s und ms seit 01.01.1970.	UDINT
Letzter Kommunikationsfehler [s]		UDINT
Letzter Systemfehler [ms]	Datum und Uhrzeit des letzten Systemfehlers in s und ms seit 01.01.1970.	UDINT
Letzter Systemfehler [s]		UDINT
Lüfterzustand	0xFF: Nicht vorhanden	BYTE
Major CPU Release	Haupt-Freigabeschalter des Prozessorsystems: **ON:** Die untergeordneten Freigabeschalter können verändert werden. **OFF:** Die untergeordneten Freigabeschalter können nicht verändert werden.	BOOL
Read-only in RUN	**ON:** Die Bedienaktionen Stopp, Start, Download sind gesperrt. **OFF:** Die Bedienaktionen Stopp, Start, Download sind nicht gesperrt.	BOOL
Reload Release	**ON:** Steuerung kann mittels Reload-Funktion (Funktion als Geräteoption verfügbar) geladen werden. **OFF:** Die Steuerung kann nicht mittels Reload-Funktion (Funktion als Geräteoption verfügbar) geladen werden.	BOOL

Variable	Beschreibung		Datentyp
Reload-Deaktivierung	**ON:** Laden mittels Reload-Funktion (Funktion als Geräteoption verfügbar) ist gesperrt. **OFF:** Laden mittels Reload-Funktion (Funktion als Geräteoption verfügbar) ist möglich.		BOOL
Reload-Zyklus	TRUE im ersten Zyklus nach einer Reload-Funktion (Funktion als Geräteoption verfügbar), sonst FALSE.		BOOL
Sicherheitszeit CPU [ms]	Für die Steuerung eingestellte Sicherheitszeit in ms.		UDINT
Start CPU Release	**ON:** Start des Prozessorsystems durch das PADT erlaubt. **OFF:** Start des Prozessorsystems durch das PADT nicht erlaubt.		BOOL
Start Cycle	ON während erstem Zyklus nach dem Start, sonst OFF.		BOOL
Stromversorgungszustand	Bitcodierter Zustand der Spannungsversorgung.		BYTE
	Wert	**Zustand**	
	0x00	Normal	
	0x01	Unterspannung bei Versorgungsspannung 24 V.	
	0x02	(Unterspannung bei Batterie) unbenutzt.	
	0x04	Unterspannung bei intern erzeugter Spannung 5 V.	
	0x08	Unterspannung bei intern erzeugter Spannung 3.3 V.	
	0x10	Überspannung bei intern erzeugter Spannung 3.3 V.	
System ID	System ID der Steuerung. Einstellbereich: 1 – 65535		UINT
Systemtick HIGH	Umlaufender Millisekundenzähler (64 Bit).		UDINT
Systemtick LOW			UDINT
Temperaturzustand	Bitcodierter Temperaturzustand des Prozessorsystems.		BYTE
	Wert	**Zustand**	
	0x00	Normale Temperatur	
	0x01	Temperaturschwelle 1 überschritten	
	0x03	Temperaturschwelle 2 überschritten	
	0xFF	Nicht vorhanden	
Verbleibende globale Force-Dauer [ms]	Zeit in ms bis zum Ablaufen der globalen Force-Zeitbegrenzung.		DINT
Watchdog-Zeit CPU [ms]	Höchste zulässige Dauer eines RUN-Zyklus in ms.		UDINT
Zykluszeit, letzte [ms]	Aktuelle Zykluszeit in ms.		UDINT
Zykluszeit, max [ms]	Maximale Zykluszeit in ms.		UDINT
Zykluszeit, min [ms]	Minimale Zykluszeit in ms.		UDINT
Zykluszeit, mittlere [ms]	Mittlere Zykluszeit in ms.		UDINT

Konfiguration des Anwenderprogramms

Die folgenden Schalter und Parameter eines Anwenderprogramms lassen sich im Dialogfenster "Eigenschaften" des Anwenderprogramms einstellen.

Parameter/Schalter	Beschreibung	Standardwert	Einstellung für sicheren Betrieb
Name	Name des Anwenderprogramms.		Beliebig
Sicherheitsintegritätslevel	Sicherheitslevel: SIL0, SIL3	SIL3	Applikationsspezifisch
Start erlaubt	**ON:** Start des Anwenderprogramms durch das PADT erlaubt. **OFF:** Start des Anwenderprogramms durch das PADT nicht erlaubt.	ON	Applikationsspezifisch

Parameter/Schalter	Beschreibung	Standard-wert	Einstellung für sicheren Betrieb
Programm-Hauptfreigabe	Freigabe der Änderung an anderen Anwenderprogramm-Schaltern: Es ist nur der Freigabe-Schalter der Ressource relevant!	ON	Applikationsspezifisch
Autostart	Freigegebene Art des Autostarts: Kaltstart, Warmstart, Aus.	Warmstart	Applikationsspezifisch
Testbetrieb erlaubt	**ON:** Für das Anwenderprogramm ist der Testbetrieb erlaubt. **OFF:** Für das Anwenderprogramm ist der Testbetrieb nicht erlaubt.	OFF	Applikationsspezifisch
Lokales Forcen erlaubt	**ON:** Forcen auf Programmebene erlaubt. **OFF:** Forcen auf Programmebene nicht erlaubt.	OFF	OFF empfohlen
Lokale Force-Timeout-Reaktion	Verhalten des Anwenderprogramms nach Ablauf der Force-Zeit: • Nur Forcen beenden • Programm stoppen	Nur Forcen beenden	Applikationsspezifisch
Reload Erlaubt	**ON:** Reload-Funktion (Funktion als Geräteoption verfügbar) des Anwenderprogramms erlaubt. **OFF:** Reload-Funktion (Funktion als Geräteoption verfügbar) des Anwenderprogramms nicht erlaubt.	ON	Applikationsspezifisch
Maximale CPU-Zyklen Programm	Maximale Anzahl an CPU-Zyklen, die ein Zyklus des Anwenderprogramms dauern darf. Ein Wert > 1 ist zulässig.	1	Applikationsspezifisch
Max. Dauer pro Zyklus [µs]	Maximale Ausführungsdauer pro Zyklus des Prozessormoduls für ein Anwenderprogramm. Einstellbereich: 1 – 7 500000 µs 0: Keine Begrenzung	0 µs	0 µs
Programm ID	ID für die Identifizierung des Programms bei der Anzeige in SILworX. Einstellbereich: 1 – 32	1	Applikationsspezifisch
Watchdog-Zeit [ms] (berechnet)	Nicht änderbare Überwachungszeit des Anwenderprogramms, errechnet aus *Maximale CPU-Zyklen Programm* und *Watchdog-Zeit der Ressource.* **Hinweis:** **Werden Zählereingänge verwendet, ist darauf zu achten, dass die Watchdog-Zeit des Anwenderprogramms ≤ 5 000 ms ist.**		-

9.2.4 Konfiguration der Ein- und Ausgänge

Im Hardware-Editor erfolgt die Konfiguration der Eingänge und Ausgänge dadurch, dass den Systemvariablen für die Eingangs- oder Ausgangskanäle globale Variablen zugewiesen werden.

So gelangen Sie zu den Systemvariablen der Kanäle:

1. Im Hardware-Editor die gewünschte Ressource anzeigen.
2. Durch Doppelklick auf das gewünschte Eingangs- oder Ausgangsmodul die Detailansicht öffnen.
3. In der Detailansicht das Register mit den gewünschten Kanälen öffnen. Die Systemvariablen der Kanäle sind sichtbar.

Verwendung digitaler Eingänge

Folgende Schritte sind notwendig, um den Wert eines digitalen Eingangs im Anwenderprogramm zu verwenden:

1. Eine globale Variable vom Typ BOOL definieren.
2. Bei der Definition einen geeigneten Initialwert angeben.
3. Die globale Variable dem Kanalwert des Eingangs zuweisen.
4. Im Anwenderprogramm eine sicherheitsgerichtete Fehlerreaktion unter Verwendung des Fehlercodes -> *Fehlercode [Byte]* programmieren.

Die globale Variable liefert Werte ins Anwenderprogramm.

Durch Zuweisen globaler Variablen auf *DI.Fehlercode* und *ModulFehlercode* bestehen zusätzliche Möglichkeiten, Fehlerreaktionen im Anwenderprogramm zu programmieren. Einzelheiten zu den Fehlercodes finden Sie im Kapitel "Parameter und Fehlercodes der Ein- und Ausgänge".

Verwendung digitaler Ausgänge

Folgende Schritte sind notwendig, um einen Wert im Anwenderprogramm auf einen digitalen Ausgang zu schreiben:

1. Eine globale Variable vom Typ BOOL definieren, die den auszugebenden Wert erhält.
2. Bei der Definition einen geeigneten Initialwert angeben.
3. Die globale Variable dem Kanalwert Wert *[BOOL]* -> des Ausgangs zuweisen.
4. Im Anwenderprogramm eine sicherheitsgerichtete Fehlerreaktion unter Verwendung des Fehlercodes -> *Fehlercode [Byte]* programmieren.

Die globale Variable liefert Werte an den digitalen Ausgang.

Durch Zuweisen globaler Variable auf *DO.Fehlercode* und *ModulFehlercode* bestehen zusätzliche Möglichkeiten, Fehlerreaktionen im Anwenderprogramm zu programmieren.

9.2.5 Generierung der Ressourcenkonfiguration

Gehen Sie so vor:

1. Im Strukturbaum die Ressource auswählen.
2. In der Aktionsleiste auf die Schaltfläche [Codegenerierung] klicken oder im Kontextmenü den Eintrag [Codegenerierung] auswählen. Das Dialogfenster "Codegenerierung starten" öffnet sich.
3. Im Dialogfenster "Codegenerierung starten" auf [OK] klicken. Ein weiteres Dialogfenster "Codegenerierung starten" öffnet sich, zeigt den Ablauf der Codegenerierung an und schließt sich wieder. Im Logbuch erscheint eine Zeile, die das Ergebnis der Codegenerierung anzeigt.
4. Bei weiterhin ausgewählter Ressource aus dem Menü [Extras] den Eintrag [Versionsvergleich] auswählen. Das Dialogfenster "Versionsübersicht" öffnet sich. Es enthält den CRC des generierten Codes.
5. Auf [Export] klicken. Es erscheint ein Dialogfenster "Archivieren", das Eingabemöglichkeiten für einen Kommentar zum Projektstand und für den Namen der Archivdatei enthält.
6. Ein weiteres Mal Code generieren, wie in den Schritten 2 und 3 beschrieben.
7. Bei weiterhin ausgewählter Ressource aus dem Menü [Extras] den Eintrag [Versionsvergleich] auswählen. Das Dialogfenster "Versionsübersicht" öffnet sich.

8. Auf [Import] klicken und im Dialogfenster "Wiederherstellen" die in Schritt 5 exportierte Archivdatei importieren. Das Fenster "Versionsübersicht" enthält nun die Informationen zum letzten generierten und zum importierten Projektstand.
9. Auf [OK] klicken. Im Arbeitsbereich erscheint das Ergebnis des Versionsvergleichs. Erscheint "ok" in der Spalte "Vergleich der CRCs", sind die generierten Codes beider Projektstände gleich und geeignet für den sicherheitsgerichteten Betrieb. Abweichungen sind durch Hinterlegung mit roter Farbe gekennzeichnet.

Damit ist der Code der Ressourcenkonfiguration generiert.

ACHTUNG!

Fehler bei der Codegenerierung durch nicht sicheren PC möglich!

Für sicherheitsgerichtete Anwendungen muss der Codegenerator zweimal Code generieren und die Prüfsummen (CRCs) beider Generierungsdurchläufe müssen miteinander übereinstimmen. Nur dann ist ein fehlerfreier Code sichergestellt.

Weitere Informationen finden Sie im Sicherheitshandbuch "Dezentrale Sicherheitssteuerung PFF-HM31A für MOVIPRO®".

9.2.6 System-ID und Verbindungsparameter konfigurieren

Gehen Sie folgendermaßen vor:

1. Im Strukturbaum die Ressource auswählen
2. In der Aktionsleiste auf die Schaltfläche [Online] klicken oder im Kontextmenü den Eintrag "Online" auswählen.

   Das Dialogfenster System-Login öffnet sich.
3. Auf [Suchen] klicken

   Das Dialogfenster "Suchen per MAC" öffnet sich.
4. Die für die Steuerung gültige MAC-Adresse (siehe Aufkleber auf dem Gehäuse) eingeben und auf [Suchen] klicken.

   Das Dialogfenster zeigt die in der Steuerung eingestellten Werte für IP-Adresse, Subnet Mask und SRS an.
5. Zum Übernehmen der Werte die Schaltfläche [übernehmen] klicken
6. Mit dem Benutzer "Administrator" einloggen
7. Menü [Online] / [Inbetriebnahme] / [System-ID einstellen] wählen und gewünschte System-ID vergeben

   Die Änderung wird sofort wirksam, sodass die Verbindung abbricht.
8. Falls noch nicht geschehen: IP-Adresse COM&CPU über Hardware vergeben und Projekt übersetzen.
9. Zur Eingabe weiterer IP-Adressen/System-IDs die Schritte 1 bis 6 wiederholen
10. Programm in die Steuerung laden

    Die Änderung wird sofort wirksam, sodass die Verbindung abbricht.

Jetzt können Sie sich mit den im Projekt eingestellten IP-Adressen und System-ID einloggen.

Für einen Systemverbund mehrerer Sicherheitssteuerungen empfehlen wir Ihnen, die einzelnen Steuerungen nacheinander zu konfigurieren und danach diese in den Netzverbund aufzunehmen. In der Gerätegrundkonfiguration der Sicherheitssteuerung ist für

die IP-Adresse ein Standardwert eingetragen. Hierdurch ist die Zuordnung der Steuerung nur durch die MAC-Adresse der einzelnen Steuerung möglich.

⚠ WARNUNG!

Vertauschungsgefahr der angesprochenen Steuerung. Dadurch kann ein falsches Anwenderprogramm in die Sicherheitssteuerung geladen werden.

Tod oder schwere Körperverletzungen.

Bauen Sie bei der Konfiguration der Verbindungsparameter und der System-ID eine Punkt-zu-Punkt Verbindung mit der jeweiligen Steuerung auf.

9.2.7 Ressourcenkonfiguration vom Programmiergerät laden

Bevor ein Anwenderprogramm zusammen mit den Verbindungsparametern der Steuerung (IP-Adresse, Subnet Mask und System-ID) in die Steuerung geladen werden kann, muss der Code für die Ressource generiert worden sein und das Programmiergerät und die Ressource müssen gültige Verbindungsparameter haben (siehe Kapitel "System-ID und Verbindungsparameter konfigurieren").

Gehen Sie folgendermaßen vor, um die Ressourcenkonfiguration vom Programmiergerät zu laden:

1. Ressource im Strukturbaum wählen.
2. In der Aktionsleiste [Online] klicken oder aus dem Kontextmenü den Eintrag [Online] wählen.
3. In Fenster "System-Login" eine Benutzergruppe mit Administrator-Rechten oder Schreibzugang angeben. Das Controlpanel öffnet sich im Arbeitsbereich und zeigt den Zustand der Steuerung an.
4. Im Menü [Online] den Eintrag [Ressource Download] wählen. Das Dialogfenster "Ressource Download" öffnet sich.
5. Im Dialogfenster den Download mit "OK" bestätigen. SILworX lädt die Konfiguration in die Steuerung.
6. Nach dem Laden das Anwenderprogramm mit dem Eintrag [Ressource Kaltstart] des Menüs [Online] starten. Nach dem Kaltstart gehen "Systemzustand" und "Programm-Status" in den Modus RUN.

Die Ressourcekonfiguration ist vom Programmiergerät geladen. Die Funktionen "Starten", "Stoppen" und "Laden" sind auch als Symbole in der Symbolleiste verfügbar.

9.2.8 Ressourcenkonfiguration aus dem Flash-Speicher des Kommunikationssystems laden

Bei Datenfehler im NVRAM und damit verbundener Überschreitung der Watchdog-Zeit kann es sinnvoll sein, die Ressourcenkonfiguration aus dem Flash-Speicher des Kommunikationssystems, anstatt vom Programmiergerät zu laden.

Besteht kein Zugang mehr zum Control Panel (CP), müssen die Verbindungsparameter vom Anwenderprogramm in die Steuerung neu gesetzt werden, siehe Kapitel "System-ID und Verbindungsparameter konfigurieren").

Geht die Steuerung nach dem Neustart in den Zustand STOPP/GÜLTIGE KONFIGURATION, kann das Anwenderprogramm wieder gestartet werden.

Geht die Steuerung nach dem Neustart in den Zustand STOPP/UNGÜLTIGE KONFIGURATION, ist das Anwenderprogramm wieder ins NVRAM zu laden.

Mit dem Befehl [Konfiguration aus Flash] laden kann eine Sicherheitskopie der letzten, lauffähigen Konfiguration aus dem Flash-Speicher des Kommunikationssystems ausgelesen und in das NVRAM des Prozessors übertragen werden. Nun lässt sich das Anwenderprogramm mit [Online] / [Ressource Kaltstart] wieder starten, ohne dass ein Download des Projektes erforderlich wurde.

Gehen Sie folgendermaßen vor, um die Ressourcenkonfiguration aus dem Flash-Speicher des Kommunikationssystems zu laden:

1. Bei der gewünschten Ressource anmelden.
2. Im Menü [Online] das Untermenü [Wartung/Service] und dort den Eintrag [Konfiguration aus Flash laden] wählen.
3. Das Laden der Konfiguration im Dialogfenster bestätigen.

Die Steuerung lädt die Ressourcenkonfiguration aus dem Flash-Speicher des Kommunikationssystems ins NVRAM.

9.2.9 Ressourcenkonfiguration im Flash-Speicher des Kommunikationssystems bereinigen

Nach temporären Fehlern der Hardware ist es möglich, dass der Flash-Speicher des Kommunikationssystems Reste ungültiger Konfigurationen enthält.

Zur Beseitigung dieser Reste gibt es den Befehl [Konfiguration bereinigen].

Ressourcenkonfiguration bereinigen:

1. Ressource im Strukturbaum wählen.
2. In der Aktionsleiste [Online] klicken oder aus dem Kontextmenü den Eintrag [Online] wählen.
3. In Fenster "System-Login" eine Benutzergruppe mit Administrator-Rechten oder Schreibzugang angeben. Das Controlpanel öffnet sich im Arbeitsbereich und zeigt den Zustand der Steuerung an.
4. Aus dem Menü [Online] und dem Untermenü [Wartung/Service] den Eintrag [Konfiguration bereinigen] wählen.
5. Aktion im Dialogfenster "Konfiguration bereinigen" mit [OK] bestätigen.

Die Konfiguration im Flash-Speicher des Kommunikationssystems wurde bereinigt. Das Bereinigen der Konfiguration ist nur in seltenen Fällen notwendig. Eine gültige Konfiguration bleibt beim Bereinigen unangetastet.

9.2.10 Datum und Uhrzeit setzen

Gehen Sie so vor:

1. Ressource im Strukturbaum wählen.
2. In der Aktionsleiste [Online] klicken oder aus dem Kontextmenü den Eintrag [Online] wählen.
3. In Fenster "System-Login" eine Benutzergruppe mit Administrator-Rechten oder Schreibzugang angeben. Das Controlpanel öffnet sich im Arbeitsbereich und zeigt den Zustand der Steuerung an.
4. Aus dem Menü [Online] und dem Untermenü [Inbetriebnahme] den Eintrag [Datum/Uhrzeit einstellen] wählen. Das Dialogfenster "Datum/Uhrzeit einstellen" öffnet sich.
5. Eine der Optionen auswählen:
   – Datum und Uhrzeit des Programmiergeräts verwenden.

     Dadurch wird die angezeigte Uhrzeit mit Datum des Programmiergeräts in die Steuerung übertragen.

   – Benutzerdefiniert.

     Datum und Uhrzeit aus den beiden Eingabefeldern werden in die Steuerung übertragen. Beim Eingeben von Datum / Uhrzeit das angegebene Format beachten.
6. Klicken auf [OK] überträgt Datum und Uhrzeit auf die Steuerung. Datum und Uhrzeit auf der Steuerung sind gesetzt.

9.3 Benutzerverwaltung mit SILworX

SILworX kann eigene Benutzerverwaltungen für jedes Projekt und für jede Steuerung einrichten und pflegen.

9.3.1 Benutzerverwaltung für ein SILworX-Projekt

In jedes SILworX-Projekt lässt sich eine PADT-Benutzerverwaltung einfügen, die den Zugang zum Projekt in SILworX regelt.

Ohne PADT-Benutzerverwaltung kann jeder Benutzer ein Projekt öffnen und alle Bestandteile ändern. Hat ein Projekt eine Benutzerverwaltung, lässt es sich nur durch einen Benutzer öffnen, der sich authentifiziert hat. Der Benutzer kann nur dann Änderungen durchführen, wenn er dazu berechtigt ist. Es gibt folgende Stufen der Berechtigung.

Stufe	Bedeutung
Sicherheitsadministrator (Sec Adm)	Kann die Benutzerverwaltung ändern: Einrichten, Löschen, Ändern von Benutzerkonten und Benutzergruppen und der PADT-Benutzerverwaltung, Festlegen des Standard-Benutzerkontos. Außerdem sind alle sonstigen Funktionen von SILworX zulässig.
Lesen/Schreiben (R/W)	Alle Funktionen von SILworX, mit Ausnahme der Benutzerverwaltung.
Nur Lesen (RO)	Nur lesende Zugriffe, keine Änderungen, kein Archivieren.

Die Benutzerverwaltung vergibt die Berechtigung an Benutzergruppen. Die Benutzerkonten erhalten ihre Berechtigung von der Benutzergruppe, der sie zugeordnet sind.

Eigenschaften von Benutzergruppen:

- Der Name muss im Projekt eindeutig sein und 1 – 31 Zeichen enthalten.
- Einer Benutzergruppe ist eine Berechtigungsstufe zugeordnet.
- Einer Benutzergruppe können beliebig viele Benutzerkonten zugeordnet sein.

- Ein Projekt kann bis zu 100 Benutzergruppen enthalten.

Eigenschaften von Benutzerkonten:

- Der Name muss im Projekt eindeutig sein und 1 – 31 Zeichen enthalten.
- Ein Benutzerkonto ist einer Benutzergruppe zugeordnet.
- Ein Projekt kann bis zu 1000 Benutzerkonten enthalten.
- Ein Benutzerkonto kann Standardbenutzer des Projekts sein.

9.3.2 Benutzerverwaltung für die Steuerung

Die Benutzerverwaltung für eine Steuerung (PES-Benutzerverwaltung) dient dazu, eine Sicherheitssteuerung vor unberechtigten Eingriffen zu schützen. Die Benutzer und ihre Zugriffsrechte sind ein Teil des Projekts und werden mit SILworX definiert und auf das Prozessormodul geladen.

Die Benutzerverwaltung kann Zugriffsrechte für maximal zehn Anwender einer Steuerung verwalten. Die Zugriffsrechte sind in der Steuerung abgelegt und bleiben auch nach dem Ausschalten der Betriebsspannung erhalten.

Jedes Benutzerkonto besteht aus Name, Passwort und Zugriffsrecht. Sobald das Projekt per Download auf die Steuerung übertragen wurde, stehen diese Informationen für Logins zur Verfügung. Die Benutzer identifizieren sich beim Login auf die Steuerung mit ihrem Namen und Passwort.

Es ist nicht erforderlich, Benutzerkonten anzulegen, dieses trägt jedoch zum sicheren Betrieb bei. Ist für eine Ressource eine Benutzerverwaltung definiert, muss diese mindestens einen Benutzer mit Administratorrechten enthalten.

Standardbenutzer

Sind für eine Ressource keine anwenderspezifischen Benutzerkonten eingerichtet, gelten die werkseitigen Einstellungen.

Werkseinstellungen:

- Anzahl der Benutzer: 1
- Benutzerkennung: Administrator
- Passwort: ohne
- Zugriffsrecht: Administrator

HINWEIS

Beachten Sie, dass es beim Definieren eigener Benutzerkonten nicht möglich ist, die Standardeinstellung beizubehalten.

Parameter für Benutzerkonten

Beim Einrichten neuer Benutzerkonten sind die folgenden Parameter zu definieren.

Parameter	Beschreibung
Benutzername	Name oder Kennzeichen des Benutzers, unter dem er sich in der Steuerung einloggt. Der Benutzername darf nicht mehr als 32 Zeichen enthalten (empfohlen: max. 16 Zeichen) und darf nur aus Buchstaben (A bis Z, a bis z), Zahlen (0 bis 9) und den Sonderzeichen Unterstrich "_" und Bindestrich "-" bestehen. Groß-/Kleinschreibung beachten.
Passwort	Zum Benutzername gehörendes Kennwort, das zum Einloggen erforderlich ist. Das Passwort darf nicht mehr als 32 Zeichen enthalten und darf nur aus Buchstaben (A bis Z, a bis z), Zahlen (0 bis 9) und den Sonderzeichen Unterstrich "_" und Bindestrich "-" bestehen. Groß-/Kleinschreibung beachten.
Passwort bestätigen	Wiederholung des Kennwortes zur Bestätigung der Eingabe.

Parameter	Beschreibung
Zugriffsart	Die Zugriffsarten definieren die Privilegien, die ein Benutzer haben kann. Folgende Zugriffsarten sind möglich: • Lesen: Der Benutzer darf nur Informationen von der Steuerung lesen, aber keine Änderungen durchführen. • Lesen + Bediener: Wie Lesen, zusätzlich darf der Benutzer: – Anwenderprogramme per Download laden und starten – Prozessormodule in Redundanz setzen – Zykluszeit- und Fehlerstatistiken zurücksetzen – Systemzeit stellen – Forcen – Module neu starten und zurücksetzen – bei Prozessormodulen den Systembetrieb starten • Lesen + Schreiben: Wie Lesen + Bediener, zusätzlich darf der Benutzer Programme erstellen, übersetzen, in die Steuerung laden und testen. • Administrator: Wie Lesen + Schreiben, zusätzlich darf der Benutzer: – Betriebssysteme laden – Hauptfreigabeschalter ändern – SRS ändern – IP-Einstellungen ändern Wenigstens einer der Benutzer muss über Administratorrechte verfügen, andernfalls akzeptiert die Steuerung die Einstellungen nicht. Der Administrator kann einem Benutzer nachträglich den Zugriff auf eine Steuerung entziehen, indem er den Benutzer gänzlich aus der Liste entfernt.

Einrichten von Benutzerkonten

Ein Benutzer mit Administratorrechten hat Zugriff auf alle Benutzerkonten. Beim Einrichten von Benutzerkonten ist Folgendes zu beachten:

- Es ist sicherzustellen, dass wenigstens ein Benutzerkonto mit Administratorrechten eingerichtet ist. Für ein Benutzerkonto mit Administratorrechten ein Passwort definieren.
- Wenn der Administrator in der Benutzerverwaltung ein Benutzerkonto erstellt hat und dieses Benutzerkonto erneut bearbeiten möchte, muss er zur Legitimierung das Passwort des Benutzerkontos eingeben.
- Die Verifikation von SILworX verwenden, um die eingerichteten Benutzerkonten zu überprüfen.
- Nach der Codegenerierung und einem Download des Projekts auf die Steuerung werden die neuen Benutzerkonten gültig. Alle zuvor gespeicherten Benutzerkonten, z. B. die Standardeinstellung, werden ungültig!

9.4 Konfiguration der Kommunikation mit SILWorX

Dieses Kapitel beschreibt die Konfiguration der Kommunikation bei Einsatz des Programmierwerkzeugs SILworX..

Zu konfigurieren sind je nach Anwendung

- Ethernet/safeethernet
- Standardprotokolle

  Für die Konfiguration der Standardprotokolle siehe Kapitel "Modbus TCP/UDP".

9.4.1 Konfiguration der Ethernet-Schnittstellen

Die Konfiguration erfolgt in der Detailansicht des Kommunikationsmoduls (COM).

HINWEIS

SILworX stellt das Prozessorsystem und das Kommunikationssystem innerhalb eines Geräts oder einer Baugruppe als Prozessormodul und Kommunikationsmodul dar.

Für die Sicherheitssteuerung in den Ethernet-Switch-Einstellungen die Parameter *Speed [Mbit/s]* und *Flow-Control* auf "Autoneg" einstellen. Die Parameter *ARP Aging Time*, *MAC Learning*, *IP Forwarding*, *Speed [Mbit/s]* und *Flow-Control* sind ausführlich in der Online-Hilfe von SILworX erklärt.

HINWEIS

Austausch einer Steuerung mit gleicher IP-Adresse:

Beim Austausch einer Steuerung, für die *ARP Aging Time = 5 Minuten* und *MACLearning = Konservativ* eingestellt ist, übernimmt der Kommunikationspartner erst nach mindestens 5 Minuten bis höchstens 10 Minuten die neue MAC-Adresse. In dieser Zeit ist keine Kommunikation mit der ausgetauschten Steuerung möglich.

Die Port-Einstellungen des integrierten Ethernet-Switches der Sicherheitssteuerung lassen sich individuell parametrieren. Im Register "Ethernet-Switch" kann für jeden Switch-Port ein Tabelleneintrag angelegt werden.

Parameter der Port-Konfiguration	Erklärung
Port	Nummer des Ports wie Gehäuseaufdruck. Pro Port darf nur eine Konfiguration vorhanden sein. Wertebereich: 1 – n, je nach Ressource.
Speed [Mbit/s]	10 Mbit/s: Datenrate 10 Mbit/s 100 Mbit/s: Datenrate 100 Mbit/s Autoneg (10/100): Automatische Einstellung der Baudrate Standard: Autoneg
Flow-Control	Vollduplex: Kommunikation in beide Richtungen gleichzeitig Halbduplex: Kommunikation in eine Richtung zu einer Zeit Autoneg: Automatische Kommunikationssteuerung Standard: Autoneg
Autoneg auch bei festen Werten	Das Übermitteln der *Speed*- und *Flow-Control*-Eigenschaften (Advertising) wird auch bei fest eingestellten Werten von *Speed* und *Flow-Control* durchgeführt. Hierdurch können andere Geräte, deren Ports auf *Autoneg* eingestellt sind, erkennen, wie die Ports der Sicherheitssteuerung eingestellt sind.
Limit	Eingehende Multicast- und/oder Broadcast-Pakete limitieren. Aus: Keine Limitierung Broadcast: Broadcast limitieren (128 kbit/s) Multicast und Broadcast: Multicast und Broadcast limitieren (1024 kbit/s) Standard: Broadcast

Die Parameter lassen sich durch Doppelklicken auf jede Zelle der Tabelle ändern und in die Konfiguration des Kommunikationssystems eintragen. Die Einträge sind mit dem Anwenderprogramm neu zu kompilieren und in die Steuerung zu übertragen, bevor sie für die Kommunikation der Sicherheitssteuerung wirksam werden.

Die Eigenschaften des Kommunikationssystems und des Ethernet-Switches sind auch online über das Control Panel änderbar. Diese Einstellungen werden sofort wirksam, aber nicht in das Anwenderprogramm übernommen.

Einzelheiten zur Konfiguration der safeethernet-Kommunikation finden Sie im Kapitel "safeethernet".

9.5 Konfigurieren von Alarmen und Ereignissen

Definition von Ereignissen:

1. Für jedes Ereignis eine globale Variable definieren. In der Regel globale Variablen verwenden, die bereits für das Programm definiert sind.
2. Unter der Ressource einen neuen Unterzweig "Alarm & Events" erzeugen, falls dieser noch nicht existiert.
3. Im Alarm & Event-Editor Ereignisse definieren
   - Globale Variable ins Ereignisfenster für boolesche oder skalare Ereignisse ziehen.
   - Die Einzelheiten der Ereignisse festlegen, siehe die beiden nachfolgenden Tabellen.

Ereignisse sind definiert.

Die **Parameter der Booleschen Ereignisse** sind in eine Tabelle einzugeben, die folgende Spalten enthält.

Spalte	Beschreibung	Wertebereich
Name	Name der Ereignisdefinition, muss in der Ressource eindeutig sein.	Text, max. 32 Zeichen
Globale Variable	Name der zugewiesenen globalen Variable (Eingefügt z. B. durch Drag&Drop).	
Datentyp	Datentyp der globalen Variable, nicht änderbar.	BOOL
Event-Quelle	CPU Event: Das Prozessormodul bildet den Zeitstempel. Es führt die Ereignisbildung komplett in jedem seiner Zyklen durch. Auto Event: Wie CPU Event Standardwert: Auto Event	CPU, Auto
Alarm bei FALSE	Aktiviert: Die Wertänderung TRUE -> FALSE der globalen Variablen löst ein Ereignis aus. Deaktiviert: Die Wertänderung FALSE -> TRUE der globalen Variablen löst ein Ereignis aus. Standardwert: Deaktiviert	Kontrollkästchen aktiviert, deaktiviert
Alarm-Text	Text, der den Alarmzustand benennt.	Text
Alarm-Priorität	Priorität des Alarmzustands. Standardwert: 500	0 – 1000
Alarmbestätigung erfolgreich	Aktiviert: Bestätigung des Alarmzustandes durch den Bediener erforderlich (Quittierung). Deaktiviert: Bestätigung des Alarmzustandes durch den Bediener nicht erforderlich. Standardwert: Deaktiviert	Kontrollkästchen aktiviert, deaktiviert
Return to Normal Text	Text, der den Alarmzustand benennt.	Text
Return to Normal Severity	Priorität des Normalzustands. Standardwert: 500	0 – 1000
Return to Normal Ack Required	Bestätigung des Normalzustandes durch den Bediener erforderlich (Quittierung). Standardwert: Deaktiviert	Kontrollkästchen aktiviert, deaktiviert

Die **Parameter der skalaren Ereignisse** sind in eine Tabelle einzugeben, die folgende Spalten enthält.

Spalte	Beschreibung	Wertebereich
Name	Name der Ereignisdefinition, muss in der Ressource eindeutig sein.	Text, max. 32 Zeichen
Globale Variable	Name der zugewiesenen globalen Variable (Eingefügt z. B. durch Drag&Drop).	
Datentyp	Datentyp der globalen Variable, nicht änderbar.	Abhängig vom Typ der globalen Variablen.

Spalte	Beschreibung	Wertebereich
Event-Quelle	CPU Event: Das Prozessormodul bildet den Zeitstempel. Es führt die Ereignisbildung komplett in jedem seiner Zyklen durch. Auto Event: Wie CPU Event Standardwert: Auto Event	CPU, Auto
HH-Alarmtext	Text, der den Alarmzustand des obersten Grenzwerts benennt.	Text
HH-Alarmwert	Oberster Grenzwert, der ein Ereignis auslöst. Bedingung: (HH Alarm Value − Hysterese) > H Alarm Value oder HH Alarm Value = H Alarm Value	Abhängig vom Typ der globalen Variablen
HH-Alarmpriorität	Priorität des obersten Grenzwerts. Standardwert: 500	0 – 1000
HH-Alarmbestätigung erforderlich	Aktiviert: Bediener muss Überschreitung des obersten Grenzwerts bestätigen (Quittierung). Deaktiviert: Bediener muss Überschreitung des obersten Grenzwerts nicht bestätigen. Standardwert: Deaktiviert	Kontrollkästchen aktiviert, deaktiviert
H-Alarmtext	Text, der den Alarmzustand des oberen Grenzwerts benennt.	Text
H-Alarmwert	Oberer Grenzwert, der ein Ereignis auslöst. Bedingung: (H Alarm Value − Hysterese) > (L Alarm Value + Hysterese) oder H Alarm Value = L Alarm Value	Abhängig vom Typ der globalen Variablen
H-Alarmpriorität	Priorität des oberen Grenzwerts. Standardwert: 500	0 – 1000
H-Alarmbestätigung erforderlich	Aktiviert: Bediener muss Überschreitung des obersten Grenzwerts bestätigen (Quittierung). Deaktiviert: Bediener muss Überschreitung des obersten Grenzwerts nicht bestätigen. Standardwert: Deaktiviert	Kontrollkästchen aktiviert, deaktiviert
Return to Normal Text	Text, der den Alarmzustand benennt.	Text
Return to Normal Severity	Priorität des Normalzustands. Standardwert: 500	0 – 1000
Return to Normal Ack Required	Bestätigung des Normalzustandes durch den Bediener erforderlich (Quittierung) Standardwert: Deaktiviert	Kontrollkästchen aktiviert, deaktiviert
L-Alarmtext	Text, der den Alarmzustand des unteren Grenzwerts benennt.	Text
L-Alarmwert	Unterer Grenzwert, der ein Ereignis auslöst. Bedingung: (L Alarm Value + Hysterese) < (H Alarm Value − Hysterese) oder L Alarm Value = H Alarm Value	Abhängig vom Typ der globalen Variablen
L-Alarmpriorität	Priorität des unteren Grenzwerts. Standardwert: 500	0 – 1000
L-Alarmbestätigung erforderlich	Aktiviert: Bediener muss Unterschreitung des unteren Grenzwerts bestätigen (Quittierung). Deaktiviert: Bediener muss Unterschreitung des unteren Grenzwerts nicht bestätigen. Standardwert: Deaktiviert	Kontrollkästchen aktiviert, deaktiviert
LL-Alarmtext	Text, der den Alarmzustand des untersten Grenzwerts benennt.	Text
LL-Alarmwert	Unterster Grenzwert, der ein Ereignis auslöst. Bedingung: (LL Alarm Value + Hysterese) < (L Alarm Value) oder LL Alarm Value = L Alarm Value	Abhängig vom Typ der globalen Variablen
LL-Alarmpriorität	Priorität des untersten Grenzwerts. Standardwert: 500	0 – 1000

Spalte	Beschreibung	Wertebereich
LL-Alarmbestätigung erforderlich	Aktiviert: Bediener muss Unterschreitung des untersten Grenzwerts bestätigen (Quittierung). Deaktiviert: Bediener muss Unterschreitung des untersten Grenzwerts nicht bestätigen. Standardwert: Deaktiviert	Kontrollkästchen aktiviert, deaktiviert
Alarm-Hysterese	Die Hysterese verhindert ein ständiges Erzeugen von vielen Ereignissen, wenn der Prozesswert häufig um einen Grenzwert schwankt.	Abhängig vom Typ der globalen Variablen

ACHTUNG!

Fehlerhafte Ereignisbildung durch Parametrierungsfehler möglich!

Setzen der Parameter *L-Alarmwert* und *H-Alarmwert* auf denselben Wert kann zu unerwünschtem Verhalten der Ereignisbildung führen, da in diesem Fall kein Normalbereich existiert.

Deshalb sicherstellen, dass *L-Alarmwert* und *H-Alarmwert* unterschiedliche Werte haben.

9.6 Umgang mit dem Anwenderprogramm

Der Anwender hat über das Programmiergerät folgende Möglichkeiten, die Funktion seines Programms in der Steuerung zu beeinflussen.

9.6.1 Setzen der Parameter und Schalter

Während der Projektierung eines Anwenderprogramms werden die Parameter und Schalter offline gesetzt und mit dem codegenerierten Programm in die Steuerung geladen. Das Setzen der Parameter und Schalter kann aber auch in den Zuständen STOPP und RUN erfolgen, wenn der Schalter *Hauptfreigabe* gesetzt ist. Nur die Elemente im NVRAM können geändert werden, alle anderen werden beim Laden gesetzt.

9.6.2 Starten des Programms von STOPP/GÜLTIGE KONFIGURATION

Das Starten des Programms entspricht dem Überführen der Steuerung von der Betriebsart STOPP/GÜLTIGE KONFIGURATION in die Betriebsart RUN. Auch das Programm geht in den RUN-Modus. Das Programm geht in den Testmodus, wenn während des Startens der Testmodus aktiviert ist. Nach IEC 61131 ist zusätzlich zum Start im Testmodus auch der Kalt- oder Warmstart möglich.

HINWEIS

Das Starten des Programms ist nur möglich, wenn der Schalter *Start/Neustart* erlaubt gesetzt ist.

9.6.3 Neustart des Programms nach Fehler

Geht das Programm in STOPP/UNGÜLTIGE KONFIGURATION, z. B. durch unerlaubte Zugriffe auf Bereiche des Betriebssystems, startet es neu. Geht es innerhalb von ca. einer Minute nach dem Neustart erneut in den Zustand STOPP/UNGÜLTIGE KONFIGURATION, bleibt es in diesem Zustand. Dann kann es über die Start-Schaltfläche des Control Panel wieder gestartet werden. Nach dem Neustart prüft das Betriebssystem das gesamte Programm.

9.6.4 Stoppen des Programms

Wird das Anwenderprogramm gestoppt, geht die Steuerung von der Betriebsart RUN nach STOPP/GÜLTIGE KONFIGURATION.

9.6.5 Testmodus des Programms

Der Testmodus wird über das Control Panel im Menü [Testmodus] / [Testmodus mit Heissstart] (oder Kaltstart/Warmstart) gestartet. Mit dem Befehl *Zyklusschritt* wird jedes Mal ein Einzelschritt (einmaliger Logikdurchgang) aktiviert.

Verhalten von Variablen-/Signalwerten im Testmodus:

Die Wahl Kaltstart, Warmstart oder Heißstart legt fest, welche Variablenwerte für den ersten Durchgang im Testmodus verwendet werden.

- Kaltstart: Alle Variablen/Signale erhalten ihren Initialwert.
- Warmstart: Retain-Signale behalten ihren Wert, andere werden auf ihren Initialwert gesetzt
- Heißstart: Alle Variablen/Signale behalten ihren aktuellen Wert.

Anschließend kann mit dem Befehl *Zyklusschritt* das Anwenderprogramm im Einzelschrittmodus gestartet werden. Alle aktuellen Werte bleiben für den nächsten Zyklus erhalten (eingefrorener Zustand).

⚠ WARNUNG!

Aktoren im nicht sicheren Zustand.

Tod oder schwere Körperverletzungen.

Funktion Testmodus nicht im sicherheitsgerichteten Betrieb verwenden!

9.6.6 Online-Test

Die Funktion Online-Test erlaubt es, in die Programmlogik Online-Test-Felder (OLT-Felder) einzufügen und während des Betriebes der Steuerung zur Anzeige und zum Forcen von Signalen/Variablen zu verwenden.

Ist der Schalter *Online-Test erlaubt* eingeschaltet, ist es möglich, während des Programmlaufes Werte für Signale/Variablen manuell in die entsprechenden OLT-Felder einzugeben und damit zu Forcen. Der geforcte Wert hat allerdings nur solange Gültigkeit, bis ihn die Programmlogik überschreibt.

Wenn der Schalter *Online-Test erlaubt* ausgeschaltet ist, können Werte für Signale/ Variablen in OLT-Feldern nur angezeigt, aber nicht verändert werden.

Weitere Informationen zur Verwendung von OLT-Feldern sind unter dem Stichwort "OLT-Feld" in der Online-Hilfe des Programmiertools zu finden.

10 Betrieb

Dieses Kapitel beschreibt die Bedienung und Diagnose während des Betriebs der Steuerung.

10.1 Bedienung

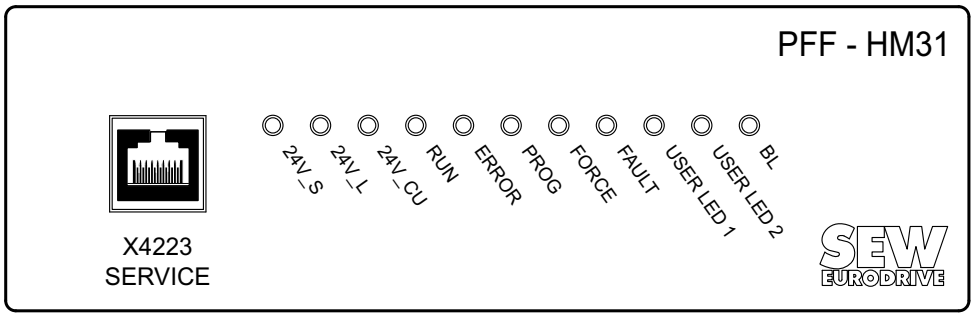
Eine Bedienung der Steuerung ist im normalen Betrieb nicht erforderlich. Nur beim Auftreten von Problemen kann ein Eingreifen mit dem Programmiergerät erforderlich sein.

10.2 Diagnose

Eine erste, grobe Diagnose kann mit Hilfe der Leuchtdiodenanzeigen erfolgen. Eine detailliertere Analyse des Betriebs- oder Fehlerzustands ist mit Hilfe der Diagnosehistorie möglich. Diese ist mit dem Programmiergerät anzeigbar.

10.2.1 LED-Anzeige

Die System-LEDs befinden sich auf der Service-Einheit des Geräts und zeigen die Feldbus- und Gerätestatus an. Zusätzlich exisitieren 2 vom Anwender frei konfigurierbare User-LEDs:



4867138571

Die folgende Tabelle zeigt den Status und die Bedeutung der LED an:

Bezeichnung	Status LED	Bedeutung
BL	Blinkt rot	• BL (Boot-Loader) defekt oder Hardware-Fehler. • Fehler der externen Prozessdaten-Kommunikation • Es wurde eine doppelte IP-Adresse entdeckt[1].
	Aus	Keines der beschriebenen Ereignisse ist eingetreten.
USER LED 2 USER LED 1	Leuchtet rot	Codierung: 1
	Blinkt rot	Codierung: 2
	Aus	Codierung: 0 oder 3...255
FAULT	Leuchtet gelb / Blinkt gelb[2]	• Das neue Betriebssystem ist verfälscht (nach dem Herunterladen) • Fehler beim Laden eines neuen Betriebssystems • Die geladene Konfiguration ist fehlerhaft. • Ein oder mehrere E/A-Fehler haben sich ereignet. • Es wurde eine doppelte IP-Adresse entdeckt[1].
	Aus	Keines der beschriebenen Ereignisse ist eingetreten.

Bezeichnung	Status LED	Bedeutung
FORCE	Leuchtet gelb	Forcen vorbereitet: • Force-Schalter einer Variablen ist gesetzt, • der Force-Hauptschalter ist noch deaktiviert. • Das Gerät ist im Zustand RUN oder STOPP.
	Blinkt gelb	• Forcen aktiv: Mindestens eine lokale oder globale Variable hat ihren Force-Wert angenommen. • Es wurde eine doppelte IP-Adresse entdeckt[1].
	Aus	Keines der beschriebenen Ereignisse ist eingetreten.
PROG	Leuchtet gelb	• Das Gerät wird mit einer neuen Konfiguration geladen. • Ein neues Betriebssystem wird geladen. • Änderung der WDZ oder FTZ. • Prüfung auf doppelte IP-Adresse. • Änderung der SRS.
	Blinkt gelb	• Reload-Funktion (Funktion ist als Geräteoption verfügbar) wird durchgeführt • Es wurde eine doppelte IP-Adresse entdeckt[1].
	Aus	Keines der beschriebenen Ereignisse ist eingetreten.
ERROR	Leuchtet rot / Blinkt rot[2]	• Das Gerät ist im Zustand FEHLERSTOPP: Durch Selbsttest festgestellter interner Fehler, z. B. Hardware-Fehler, Software-Fehler oder Fehler der Spannungsversorgung. Abhilfe: Das Prozessorsystem kann nur durch einen Befehl vom PADT wieder gestartet werden (Reboot). • Es werden nicht aktivierte Protokolle/Funktionen verwendet (Warnung). • Fehler beim Laden des Betriebssystems
	Aus	Keines der beschriebenen Ereignisse ist eingetreten.
RUN	Leuchtet grün	• Gerät im Zustand RUN, Normalbetrieb • Ein geladenes Anwenderprogramm wird ausgeführt
	Blinkt grün	• Gerät im Zustand STOPP • Ein neues Betriebssystem wird geladen
	Aus	Gerät ist nicht im Zustand RUN oder STOPP
24V_CU	Leuchtet grün	Zwischen X1541.1 und X1541.2 liegt 24 V an.
24V_L	Leuchtet grün	Zwischen X1541.3 und X1541.4 liegt 24 V an.
24V_S	Leuchtet grün	Zwischen X2312.1 und X2312.3 liegt 24 V an.

1) Bei gemeinsamem Blinken der LEDs: PROG, FORCE, FAULT und BL

2) Der Status "Leuchtet" signalisiert eine Warnung und "Blinken" signalisiert einen Alarm.

Beim Zuschalten der Versorgungsspannung erfolgt immer ein Test der Leuchtdioden, bei dem für kurze Zeit alle Leuchtdioden leuchten.

User-LEDs

Die beiden frei konfigurierbaren User-LEDs werden über Systemvariablen angesteuert. Dazu müssen den zugehörigen Systemvariablen globale Variablen vom Datentyp USINT zugewiesen werden.

10.2.2 Diagnosehistorie

Die Diagnosehistorie erfasst die verschiedenen Zustände des Prozessor- und des Kommunikationssystems und legt sie in einem nicht-flüchtigen Speicher ab. Dabei wird für beide zwischen Langzeit- und Kurzzeitdiagnose gemäß folgender Tabelle unterschieden.

	CPU	COM
Einträge in der Langzeitdiagnose	700	300
Einträge in der Kurzzeitdiagnose	700	700

Die Langzeitdiagnose des Prozessorsystems umfasst folgende Ereignisse:

- Reboot
- Wechsel der Betriebsart

(INIT, RUN, STOPP/GÜLTIGE KONFIGURATION, STOPP/UNGÜLTIGE KONFIGURATION)

- Wechsel der Programm-Betriebsart

  (START, RUN, FEHLER, TESTMODUS)
- Laden / Löschen einer Konfiguration
- Setzen und Rücksetzen von Schaltern
- Fehler im Prozessorsystem
- Laden eines Betriebssystems
- Forcen (Setzen und Rücksetzen des Schalters Forcen erlaubt)
- Diagnose der Spannungsversorgung und Temperatur

Die Langzeitdiagnose des Kommunikationssystems umfasst folgende Ereignisse:

- Reboot des Kommunikationssystems
- Wechsel der Betriebsart (INIT, RUN, STOPP/GÜLTIGE KONFIGURATION, STOPP/UNGÜLTIGE KONFIGURATION)
- Anmelden von Benutzern
- Laden eines Betriebssystems

Ist der Speicher der Langzeitdiagnose voll, werden alle Daten, die älter als drei Tage sind, gelöscht, und es können neue Einträge aufgenommen werden. Sind alle Daten weniger als drei Tage alt, können keine neuen Daten gespeichert werden und sind verloren. Ein Eintrag in der Langzeitdiagnose zeigt an, dass Daten nicht gespeichert werden konnten.

Die Kurzzeitdiagnose des Prozessorsystems umfasst folgende Ereignisse:

- Diagnose des Prozessorsystems (Setzen der Force-Schalter und Force-Werte)
- Diagnose des Anwenderprogramms (Zyklusbetrieb)
- Diagnose der Kommunikation
- Diagnose der Spannungsversorgung und der Temperatur

Die Kurzzeitdiagnose des Kommunikationssystems umfasst folgende Ereignisse:

- safeethernet-bezogene Ereignisse
- Start / Stopp beim Schreiben des Flash-Speichers
- Fehler, die beim Laden einer Konfiguration aus dem Flash-Speicher auftreten können
- Auseinandergelaufene Zeitsynchronisation zwischen Kommunikationssystem und Prozessorsystem

Parametrierungsfehler der Eingänge und Ausgänge werden bei der Codegenerierung u. U. nicht erkannt. Im Rückmeldefenster der Diagnose erscheint bei einem Parametrierungsfehler die Meldung INVALID CONFIG mit Angabe der Fehlerquelle und eines Fehlercodes. Diese Meldung hilft bei der Analyse von Fehlern bei der Parametrierung der Ein- und Ausgabe.

Ist der Speicher der Kurzzeitdiagnose voll, werden die jeweils ältesten Einträge entfernt, um Platz für neue Einträge zu schaffen. Es erfolgt keine Anzeige, wenn alte Einträge gelöscht werden.

Die Aufzeichnung der Diagnosedaten ist nicht sicherheitsgerichtet. Die in chronologischer Reihenfolge aufgezeichneten Daten können über das Programmierwerkzeug für eine Analyse ausgelesen werden. Das Auslesen löscht nicht die Daten in der Steuerung. Das Programmierwerkzeug kann den Inhalt des Diagnosefensters abspeichern.

10.2.3 Diagnose in SILworX

Der Zugang zur Diagnose erfolgt über die Online-Ansicht des Hardware-Editors in SILworX.

Gehen Sie folgendermaßen vor, um die Diagnose zu öffnen:

1. Unter der gewünschten Ressource den Zweig "Hardware" markieren.
2. Im Kontextmenü oder in der Aktionsleiste [Online] anklicken. Das Systemlogin-Fenster öffnet sich.
3. Ins Systemlogin-Fenster die folgenden Informationen auswählen oder eingeben:
   – IP-Adresse der Steuerung
   – Benutzer und Passwort

   Die Online-Ansicht des Hardware-Editors öffnet sich.
4. In der Online-Ansicht das gewünschte Modul auswählen, normalerweise das Prozessor- oder das Kommunikationsmodul.
5. Aus dem Kontextmenü oder dem Menü [Online] den Punkt [Diagnose] auswählen.

Die Diagnose für das betreffende Modul öffnet sich.

Bei laufender Steuerung erscheinen Meldungen über Zustände des Prozessorsystems, des Kommunikationssystems und der E/A-Baugruppen über bestimmte, einstellbare Zeiträume.

10.3 Parameter und Fehlercodes der Ein- und Ausgänge

In den folgenden Übersichten sind die lesbaren und einstellbaren Systemparameter der Ein-/Ausgänge einschließlich der Fehlercodes aufgeführt. Die Fehlercodes können innerhalb des Anwenderprogramms über die entsprechenden, in der Logik zugewiesenen Variablen ausgelesen werden. Die Anzeige der Fehlercodes kann auch in SILworX erfolgen.

10.3.1 Digitale Eingänge PFF-HM31A

Die nachfolgenden Tabellen enthalten die Status und Parameter des Eingangsmoduls (DI 26) in derselben Reihenfolge wie im Hardware-Editor.

Register-Modul

Das Register-Modul enthält die folgenden Systemparameter.

Systemparameter	Datentyp	R/W	Beschreibung	
DI AnzahlTaktspeisekanäle	USINT	W	Anzahl der Taktausgänge (Speiseausgänge)	
			Codierung	**Beschreibung**
			0	Kein Taktausgang für LS/LB[1)]-Erkennung vorgesehen
			1	Taktausgang 1 für LS/LB[1)]-Erkennung vorgesehen
			2	Taktausgänge 1 und 2 für LS/LB[1)]-Erkennung vorgesehen
			...	...
			6	Taktausgänge 1 bis 6 für LS/LB[1)]-Erkennung vorgesehen
			Taktausgänge dürfen nicht als sicherheitsgerichtete Ausgänge verwendet werden!	
DI Speisung [01]	BOOL	W	Ansteuerung des Versorgungsausgangs SS0. TRUE: Speisung ist eingeschaltet FALSE: Speisung ist nicht eingeschaltet	
DI Steckpl. Taktspeise-Bg	UDINT	W	Steckplatz der Taktspeisebaugruppe (LS/LB[1)]-Erkennung), Wert auf "2" einstellen.	
DI Taktverzögerung [µs]	UINT	W	Wartezeit für Line Control (Schluss- / Querschlusserkennung).	

Systemparameter	Datentyp	R/W	Beschreibung	
DI.Fehlercode	WORD	R	Fehlercodes aller digitalen Eingänge.	
			Codierung	**Beschreibung**
			0x0001	Fehler der Baugruppe
			0x0002	FTZ-Test des Testmusters fehlerhaft
			0x2000	Parametrierung der LS/LB[1)]-Erkennung fehlerhaft
DI.Fehlercode Speisung	WORD	R	Baugruppen-Fehlercodes des Versorgungsausgangs SS0	
			Codierung	**Beschreibung**
			0x0001	Fehler der Baugruppe
DI[01].Fehlercode Speisung	BYTE	R	Kanal-Fehlercodes des Versorgungsausgangs SS0.	
			Codierung	**Beschreibung**
			0x01	Fehler DI Speiseeinheit
			0x02	Speisung wegen Überstrom abgeschaltet
			0x04	Fehler beim Rücklesen der Speisung
DO.Fehlercode	WORD	R	Fehlercodes aller Taktausgänge	
			Codierung	**Beschreibung**
			0x0001	Fehler der Baugruppe
ModulFehlercode	WORD	R	Fehlercodes des Moduls	
			Codierung	**Beschreibung**
			0x0000	E/A-Verarbeitung, ggf. mit Fehlern, siehe weitere Fehlercodes
			0x0001	Keine E/A-Verarbeitung (CPU nicht in RUN)
			0x0002	Keine E/A-Verarbeitung während des Hochfahrtests
			0x0004	Hersteller-Interface in Betrieb
			0x0010	Keine E/A-Verarbeitung: falsche Parametrierung
			0x0020	Keine E/A-Verarbeitung: Fehlerrate überschritten
			0x0040/ 0x0080	Keine E/A-Verarbeitung: konfiguriertes Modul nicht gesteckt
ModulSRS	UDINT	R	Steckplatz-Nummer (System-Rack-Slot)	
ModulTyp	UINT	R	Typ des Moduls, Sollwert: 0x001A [26_{dez}]	

1) LS = Leitungsschluss / LB = Leitungsbruch (Line Control)

Register DI26: DI-Kanäle

Das Register DI 26: DI-Kanäle enthält die folgenden Systemparameter.

Systemparameter	Datentyp	R/W	Beschreibung	
Kanal-Nr.	-	R	Kanalnummer, fest vorgegeben	
-> Fehlercode [BYTE]	BYTE	R	Fehlercodes der digitalen Eingangskanäle	
			Codierung	**Beschreibung**
			0x01	Fehler im digitalen Eingangsmodul
			0x10	Leitungsschluss des Kanals
			0x80	Unterbrechung zwischen Taktausgang TO und digitalem Eingang DI, z. B. • Leitungsbruch • geöffneter Schalter • L+ Unterspannung (+24 V_S)
-> Wert [BOOL]	BOOL	R	Eingangswert der digitalen Eingänge. 0 = Eingang nicht angesteuert 1 = Eingang angesteuert	
Taktspeisekanal [USINT ->	USINT	W	Quellkanal der Taktspeisung	
			Codierung	**Beschreibung**
			0	Eingangskanal
			1	Takt vom 1. TO-Kanal
			2	Takt vom 2. TO-Kanal
			...	...
			6	Takt vom 6. TO-Kanal

Register DI26: DO-Kanäle

Das Register DI 26: DO-Kanäle enthält die folgenden Systemparameter.

Systemparameter	Datentyp	R/W	Beschreibung	
Kanal-Nr.	-	R	Kanalnummer, fest vorgegeben	
-> Fehlercode [BYTE]	BYTE	R	Fehlercodes der digitalen Ausgänge	
			Codierung	**Beschreibung**
			0x01	Fehler im digitalen Ausgangsmodul oder der Baugruppe
-> Wert [BOOL]	BOOL	W	Ausgabewert der DO-Kanäle	
			Codierung	**Beschreibung**
			0	Ausgang stromlos
			1	Ausgang angesteuert

10.3.2 Digitale Ausgänge PFF-HM31A

Die nachfolgenden Tabellen enthalten die Status und Parameter des Ausgangsmoduls (DO 8) in derselben Reihenfolge wie im Hardware-Editor.

Register Modul

Das Register Modul enthält die folgenden Systemparameter.

Systemparameter	Datentyp	R/W	Beschreibung	
DO. Fehlercode	WORD	R	Fehlercodes aller digitalen Ausgänge.	
			Codierung	**Beschreibung**
			0x0001	Fehler der Baugruppe
			0x0002	MEZ-Test der Sicherheitsabschaltung liefert einen Fehler
			0x0004	MEZ-Test Hilfsspannung liefert einen Fehler
			0x0008	FTZ-Test des Testmusters fehlerhaft
			0x0010	MEZ-Test des Testmusters der Ausgangsschalter fehlerhaft
			0x0020	MEZ-Test des Testmusters der Ausgangsschalter (Abschalttest der Ausgänge) fehlerhaft
			0x0040	MEZ-Test Aktive Abschaltung über WD fehlerhaft
			0x0400	FTZ-Test: 1. Temperaturschwelle überschritten
			0x0800	FTZ-Test: 2. Temperaturschwelle überschritten
			0x4000	Parametrierung der 2-poligen Überwachung fehlerhaft
Einschaltverzögerung	UINT	W	Einschaltverzögerung für 2-polige Tests, wegen Leitungskapazitäten, induktiver und kapazitiver Last. Wertebereich: 0 – 30 ms	
ModulFehlercode	WORD	R	Fehlercodes des Moduls	
			Codierung	**Beschreibung**
			0x0000	E/A-Verarbeitung, ggf.. mit Fehlern, siehe weitere Fehlercodes
			0x0001	Keine E/A-Verarbeitung (CPU nicht in RUN)
			0x0002	Keine E/A-Verarbeitung während des Hochfahrtests
			0x0004	Hersteller-Interface in Betrieb
			0x0010	Keine E/A-Verarbeitung: falsche Parametrierung
			0x0020	Keine E/A-Verarbeitung: Fehlerrate überschritten
			0x0040/ 0x0080	Keine E/A-Verarbeitung: konfiguriertes Modul nicht gesteckt
ModulSRS	UDINT	R	Steckplatz-Nummer (System-Rack-Slot)	
ModulTyp	UINT	R	Typ des Moduls, Sollwert: 0x0029 [41_{dez}]	

Register DO 8: Kanäle

Das Register DO 8: Kanäle enthält die folgenden Systemparameter.

Systemparameter	Datentyp	R/W	Beschreibung	
Kanal-Nr.	-	R	Kanalnummer, fest vorgegeben.	
-> + Fehlercode [BYTE]	WORD	R	Fehlercodes der digitalen Ausgänge.	
			Codierung	**Beschreibung**
			0x0001	Fehler im digitalen Ausgangsmodul.
			0x0002	Ausgang abgeschaltet wegen Überstrom.
			0x0004	Fehler beim Rücklesen der Ansteuerung der digitalen Ausgänge.
			0x0008	Fehler beim Rücklesen des Status der digitalen Ausgänge.
			0x0020	Externer Leitungsschluss oder Schluss des EMV-Schutzes liefert einen Fehler (L+ Schluss (24V_L)).
			0x0040	Externer Leitungsschluss oder Schluss des EMV-Schutzes liefert einen Fehler (L− Schluss (0V24)).
			0x0080	Kanal ist wegen Fehler des zugeordneten DO-Kanals abgeschaltet.
			0x0100	Test Schluss des Ausgangs gegen L+ (24V_L)aufgrund von Sollwertänderungen oder Unterspannung nicht durchgeführt.
			0x0200	Test Schluss des Ausgangs gegen L− (0V24) aufgrund von Sollwertänderungen oder Unterspannung nicht durchgeführt.
			0x0400	Alle Kanäle abgeschaltet, Gesamtstrom überschritten.
			0x0800	FTZ-Test: Überwachung der Hilfsspannung 1: Unterspannung.
-> − Fehlercode [BYTE]	WORD	R	Siehe -> + *Fehlercode [BYTE]*	
-> Wert [BOOL]	BOOL	W	Ausgangswert der DO-Kanäle. 0 = Ausgang stromlos 1 = Ausgang angesteuert	
2-polig abgeschaltet [BOOL] ->	BOOL	W	Parametrierung, ob der Kanal 2-polig verwendet wird. 0 = Kanal wird 2-polig verwendet 1 = Kanal wird 1-polig verwendet	

10.3.3 Zähler PFF-HM31A

Die nachfolgenden Tabellen enthalten die Status und Parameter des Zählermoduls (HSC 2) in derselben Reihenfolge wie im Hardware-Editor.

Register Modul

Das Register Modul enthält die folgenden Systemparameter.

Systemparameter	Datentyp	R/W	Beschreibung	
ModulFehlercode	WORD	R	Fehlercodes des Moduls.	
			Codierung	**Beschreibung**
			0x0000	E/A-Verarbeitung, ggf.. mit Fehlern, siehe weitere Fehlercodes.
			0x0001	Keine E/A-Verarbeitung (CPU nicht in RUN).
			0x0002	Keine E/A-Verarbeitung während des Hochfahrtests.
			0x0004	Hersteller-Interface in Betrieb.
			0x0010	Keine E/A-Verarbeitung: falsche Parametrierung.
			0x0020	Keine E/A-Verarbeitung: Fehlerrate überschritten.
			0x0040/ 0x0080	Keine E/A-Verarbeitung: konfiguriertes Modul nicht gesteckt.
ModulSRS	UDINT	R	Steckplatz-Nummer (System-Rack-Slot)	
ModulTyp	UINT	R	Typ des Moduls, Sollwert: 0x0003 [3_{dez}]	

Systemparameter	Datentyp	R/W	Beschreibung	
Zähler.Fehlercode	WORD	R	Fehlercodes des Zählermoduls.	
			Codierung	**Beschreibung**
			0x0001	Fehler der Baugruppe.
			0x0002	Fehler beim Vergleich der Zeitbasis.
			0x0004	Adressfehler beim Lesen der Zeitbasis.
			0x0008	Parameter für die Zeitbasis fehlerhaft.
			0x0010	Adressfehler beim Lesen des Zählerstands.
			0x0020	Parametrierung des Zählers wurde verfälscht.
			0x0040	Adressfehler beim Lesen des Gray-Codes.
			0x0080	FTZ-Test des Testmusters fehlerhaft.
			0x0100	FTZ-Test Fehler bei Überprüfung der Koeffizienten
			0x0200	Fehler bei der initialen Parametrierung der Baugruppe.

Register HSC 2: Kanäle

Das Register HSC 2: Kanäle enthält die folgenden Systemparameter.

Systemparameter	Datentyp	R/W	Beschreibung	
Zähler[0x].5/24V Modus	BOOL	R/W	Zählereingang 5 V oder 24 V. TRUE: 24 V FALSE: 5 V	
Zähler [0x]Autom.Drehrichtungserkennung	BOOL	R/W	Automatische Drehrichtungserkennung. TRUE: Automatische Drehrichtungserkennung EIN FALSE: Manuelles Setzen der Drehrichtung	
Zähler[0x].Fehlercode	BYTE	R	Fehlercodes der Zählerkanäle.	
			Codierung	**Beschreibung**
			0x01	Fehler im Zählermodul
			0x02	Fehler beim Vergleich der Zählerstände
			0x08	Fehler beim Einstellen der Parametrierung (Reset).
Zähler[0x].Gray-Code	BOOL	R/W	Decoder/Impulsbetrieb. TRUE: Gray-Code Decoder FALSE: Impulsbetrieb **Decoder-Betrieb nicht zulässig!**	
Zähler[0x].Leer1	BOOL	R/W	Keine Funktion	
Zähler[0x].Leer2	BOOL	R/W		
Zähler[0x].Leer3	BOOL	R/W		
Zähler[0x].Reset	BOOL	R/W	Reset des Zählkanals (nur wenn *Zähler[0x].Autom. Drehrichtungserkennung = FALSE*) TRUE: kein Reset FALSE: Reset	
Zähler[0x].Richtung	BOOL	R/W	Zählrichtung des Zählers (nur wenn *Zähler[0x].Autom. Drehrichtungserkennung = FALSE*) TRUE: Abwärts (Dekrementieren) FALSE: Aufwärts (Inkrementieren)	
Zähler[0x].Wert	UDINT	R	Zählerstand der Zähler: 24 Bit für Impulszähler.	
Zähler[0x].Wert-Überlauf	BOOL	R	Zähler-Überlaufanzeige TRUE: Überlauf seit letztem Zyklus (nur wenn *Zähler[0x].Autom. Drehrichtungserkennung = FALSE*) FALSE: Kein Überlauf seit letztem Zyklus	
Zähler[0x].Zeitstempel	UDINT	R	Zeitstempel für *Zähler[0x].Wert*, 24 Bit, Zeitauflösung 1 µs.	
Zähler[0x].Zeit-Überlauf	BOOL	R	Überlaufanzeige für den Zeitstempel der Zähler TRUE: 24-Bit-Überlauf seit letztem Zyklus FALSE: Kein Überlauf seit letztem Zyklus	

11 Instandhaltung

Die Instandhaltung der Sicherheitssteuerung beschränkt sich auf Folgendes:

- Beseitigung von Störungen
- Laden von Betriebssystemen

11.1 Störungsinformation

Störungen im Prozessorsystem (CPU) haben meist das Abschalten der gesamten Steuerung zur Folge und werden durch die Status-LED "ERROR" angezeigt.

Die Anzeige kann durch Ausführen des Befehls "Ressource Rebooten" im Menü [Extra] des Control Panels von SILWorX gelöscht werden. Die Steuerung wird gebootet und erneut gestartet. Störungen in Eingangs- und Ausgangskanälen erkennt das System während des Betriebs automatisch und zeigt sie auf der Oberseite des Geräts durch die Status-LED "FAULT" an.

Das PADT (SILWorX) bietet auch bei einem Stopp der Steuerung die Möglichkeit, festgestellte Fehler über die Diagnose auszulesen, so weit die Kommunikation nicht ebenfalls gestört ist.

- Prüfen Sie vor dem Wechsel einer Steuerung, ob eine externe Leitungsstörung vorliegt und der entsprechende Sensor/Aktor in Ordnung ist.

11.2 Laden von Betriebssystemen

Prozessorsystem und Kommunikationssystem haben unterschiedliche Betriebssysteme, die in wieder beschreibbaren Flash-Speichern gespeichert sind und bei Bedarf ersetzt werden können.

⚠ WARNUNG!

Unterbrechung des sicherheitsgerichteten Betriebs durch Laden neuer Betriebssysteme vom Programmierwerkzeug.

Tod oder schwere Körperverletzungen!

- Zum Laden neuer Betriebssysteme vom Programmierwerkzeug muss die Steuerung im STOPP sein.
- Der Betreiber muss sicherstellen, dass während dieser Zeit die Sicherheit der Anlage gewährleistet bleibt, z. B. durch organisatorische Maßnahmen.

HINWEISE

- Das Programmierwerkzeug verhindert das Laden von Betriebssystemen im Zustand RUN und meldet dies.
- Eine Unterbrechung oder inkorrekte Beendung des Ladens führt dazu, dass die Steuerung nicht mehr funktionsfähig ist. Es ist jedoch möglich, erneut ein Betriebssystem zu laden.

Das Betriebssystem für das Prozessorsystem (CPU-Betriebssystem) ist vor dem für das Kommunikationssystem (COM-Betriebssystem) zu laden. Voraussetzung zum Laden von Betriebssystemen ist, dass das neue Betriebssystem in einem Verzeichnis abgelegt ist, das mit dem Programmierwerkzeug zu erreichen ist.

11.2.1 Laden von Betriebssystemen mit SILworX

Gehen Sie so vor, um ein neues Betriebssystem zu laden:

1. Steuerung in den Zustand STOPP bringen, falls nicht bereits geschehen.
2. Online-Ansicht der Hardware öffnen, dabei auf der Steuerung mit Administratorrechten anmelden.
3. Zu ladendes Modul (Prozessormodul oder Kommunikationsmodul) mit rechter Maustaste klicken.
4. Im geöffneten Kontextmenü [Wartung/Service] / [Modul Betriebssystem laden] klicken.
5. Im Dialogfenster "Modul Betriebssystem laden" die Art des zu ladenden Betriebssystems auswählen.
6. Im geöffneten Dateiauswahlfenster die Datei mit dem zu ladenden Betriebssystem auswählen und [Öffnen] klicken.

SILworX lädt das neue Betriebssystem in die Steuerung.

12 Anhang

12.1 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
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/signal 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/signal)
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)

Begriff	Beschreibung
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/signal 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

Stichwortverzeichnis




SEW-EURODRIVE
Driving the world

SEW-EURODRIVE GmbH & Co KG
P.O. Box 3023
D-76642 Bruchsal/Germany
Phone +49 7251 75-0
Fax +49 7251 75-1970
sew@sew-eurodrive.com

➞ **www.sew-eurodrive.com**