X20SL80xx

1 Gestaltung von Sicherheitshinweisen

Die Sicherheitshinweise werden im vorliegenden Handbuch wie folgt gestaltet:

Sicherheitshinweis	Beschreibung
Gefahr!	Bei Missachtung der Sicherheitsvorschriften und -hinweise besteht die Gefahr schwerer Verletzungen, Todesgefahr oder großer Sachschäden.
Information:	Wichtige Angaben zur Vermeidung von Fehlfunktionen.

Tabelle 1: Gestaltung von Sicherheitshinweisen

2 Bestelldaten

Bestellnummer	Kurzbeschreibung
	Zentraleinheiten
X20SL8000	X20 SafeLOGIC, Sicherheits-CPU standard, für bis zu 20 Safety Nodes, tauschbarer Anwenderspeicher: Memory Key, 1 POWERLINK V2 Schnittstelle, Controlled Node, integrierter 2fach Hub, inkl. Einspeisemodul, Feldklemme X20TB52, X20 Abschlussplatte rechts X20AC0SR1 beiliegend, Memory Key gesondert bestellen!
X20SL8001	X20 SafeLOGIC, Sicherheits-CPU plus, für bis zu 100 Safety Nodes, 32 Maschinenoptionen, POWERLINK Safety Gateway, tauschbarer Anwenderspeicher: Memory Key, 1 POWERLINK V2 Schnittstelle, Controlled Node, integrierter 2fach Hub, inkl. Einspeisemodul, Feldklemme X20TB52, X20 Abschlussplatte rechts X20AC0SR1 beiliegend, Memory Key gesondert bestellen!
X20SL8010	X20 SafeLOGIC, Sicherheits-CPU standard, SafeMC für bis zu 20 Safety Nodes inkl. SafeMC Nodes, tauschbarer Anwenderspeicher: Memory Key, 1 POWERLINK V2 Schnittstelle, Controlled Node, integrierter 2fach Hub, inkl. Einspeisemodul, Feldklemme X20TB52, X20 Abschlussplatte rechts X20AC0SR1 beiliegend, Memory Key gesondert bestellen!
X20SL8011	X20 SafeLOGIC, Sicherheits-CPU plus, SafeMC für bis zu 100 Safety Nodes inkl. SafeMC Nodes, 32 Maschinenoptionen, POWERLINK Safety Gateway, tauschbarer Anwenderspeicher: Memory Key, 1 POWERLINK V2 Schnittstelle, Controlled Node, integrierter 2fach Hub, inkl. Einspeisemodul, Feldklemme X20TB52, X20 Abschlussplatte rechts X20AC0SR1 beiliegend, Memory Key gesondert bestellen!
	Erforderliches Zubehör
	Zubehör
X20MK0201	X20 Memory Key, 2 MByte
X20MK0203	X20 Memory Key, 8 MByte

Tabelle 2: X20SL8000, X20SL8001, X20SL8010, X20SL8011 - Bestelldaten

3 Technische Daten

Produktbezeichnung	X20SL8000	X20SL8001	X20SL8010	X20SL8011
Kurzbeschreibung				
Schnittstellen	POWERLINK V2			
Systemmodul	Zentraleinheit			
Allgemeines				
Kühlung	lüfterlos			
Statusanzeigen	CPU Funktion, POWERLINK, SafeKEY			
Diagnose				
CPU Funktion	Ja, per Status LED			
POWERLINK	Ja, per Status LED			
SafeKEY	Ja, per Status LED			
Leistungsaufnahme	5,1 W			
Zertifizierungen				
CE	Ja			
c-UL-us	Ja			
GOST-R	Ja			
IEC 61508	Ja			
IEC 62061	Ja			
EN 13849	Ja			
Funktionalität				
Anzahl der unterstützten Sicherheitsknoten	max. 20	max. 100	max. 20	max. 100
Kommunikation untereinander	Kommunikation nur zu einer SafeLOGIC SL8001 oder SL8011 möglich	Freie Kommunikation zu max. 10 anderen SafeLOGIC möglich	Kommunikation nur zu einer SafeLOGIC SL8001 oder SL8011 möglich	Freie Kommunikation zu max. 10 anderen SafeLOGIC möglich
Unterstützung von Maschinenoptionen	Nein	Ja	Nein	Ja
Unterstützung von SafeMC (Safe Motion Control)	Nein		Ja	
Controller				
Echtzeituhr	Nullspannungssicher, Auflösung 1 s			
Modulare Schnittstellensteckplätze	keine			
Prozessor	Intel XSCALE 266 MHz			
SafeKEY Slot	1x			
Schnellste Taskklassen Zykluszeit	1 ms			
Feldbus				
Typ	POWERLINK V2			
Ausführung	Interner 2fach Hub, 2x geschirmter RJ45 Port			
Leitungslänge	max. 100 m zwischen zwei Stationen (Segmentlänge)			
Übertragungsrate	100 MBit/s			
Zykluszeit	max. 20 ms			
Versorgung				
Nennspannung	+24 V (-15% / +20%)			
Sicherung	Integriert, nicht tauschbar			
Verpolungsschutz	Ja			
Einsatzbedingungen				
Einbaulage				
waagrecht	Ja			
senkrecht	Ja			
Aufstellungshöhe über NN (Meeresspiegel)				
0 bis 2000 m	Ohne Derating			
> 2000 m	Reduktion der Umgebungstemperatur um 0,5°C pro 100 m			
Schutzart nach EN 60529	IP20			
Umgebungsbedingungen				
Temperatur				
Betrieb				
waagrechte Einbaulage	0 bis 55°C			
senkrechte Einbaulage	0 bis 45°C			
Lagerung	-25 bis 70°C			
Transport	-25 bis 70°C			
Luftfeuchtigkeit				
Betrieb	5 bis 95%			
Lagerung	5 bis 95%			
Transport	5 bis 95%			
Mechanische Eigenschaften				
Anmerkung	Programmspeicher (SafeKEY) gesondert bestellen X20 Abschlussplatte rechts ist im Lieferumfang enthalten X20 Feldklemme 12fach, Safety kodiert, ist im Lieferumfang enthalten SafeKEY Abdeckung ist im Lieferumfang enthalten			
Abmessungen				
Breite	87,5 mm			
Höhe	99 mm			
Tiefe	75 mm			

Tabelle 3: X20SL8000, X20SL8001, X20SL8010, X20SL8011 - Technische Daten

4 Sicherheitstechnische Kennwerte

Kriterium	Kennwert
Kategorie gem. EN ISO 13849	KAT 4
Maximaler Performance Level gem. EN ISO 13849	PL e
Maximaler Safety integrity Level gem. IEC 62061	SIL 3
Maximaler Safety integrity Level gem. IEC 61508	SIL 3
PFH (Probability of dangerous Failure per Hour)	< $1*10^{-10}$
PFD (Probability of dangerous Failure on demand)	< $1* 10^{-5}$ bei einem Proof Test Intervall von 10 Jahren < $2* 10^{-5}$ bei einem Proof Test Intervall von 20 Jahren
PT (Proof Test Intervall)	max. 20 Jahre
DC (Diagnostic Coverage)	> 90 %
MTTFd (Mean Time To Failure dangerous)	2500 Jahre

Tabelle 4: X20SL80xx Sicherheitstechnische Kennwerte

5 Bedien- und Anschlusselemente

Für die Bedienung der SafeLOGIC sind LEDs und Taster/Schalter vorgesehen. Mit diesen Elementen kann das

- Tauschen eines Moduls inkl. Überprüfen der gesamten Modulkonfiguration (Kapitel 7.1 "Tauschen von Modulen" auf Seite 17)
- Tauschen der Firmware (Kapitel 7.3 "Bestätigung eines Firmwaretauschs" auf Seite 19)
- Tauschen des SafeKEY, evt. inklusive Übernahme der Modulkonfiguration vom alten SafeKEY (Kapitel 7.5 "SafeKEY" auf Seite 19)
- Tauschen der SafeLOGIC (Kapitel 7.6 "Tauschen einer SafeLOGIC" auf Seite 21)

bedient werden.

Eine SafeLOGIC verfügt über folgende Bedien- und Anschlusselemente:

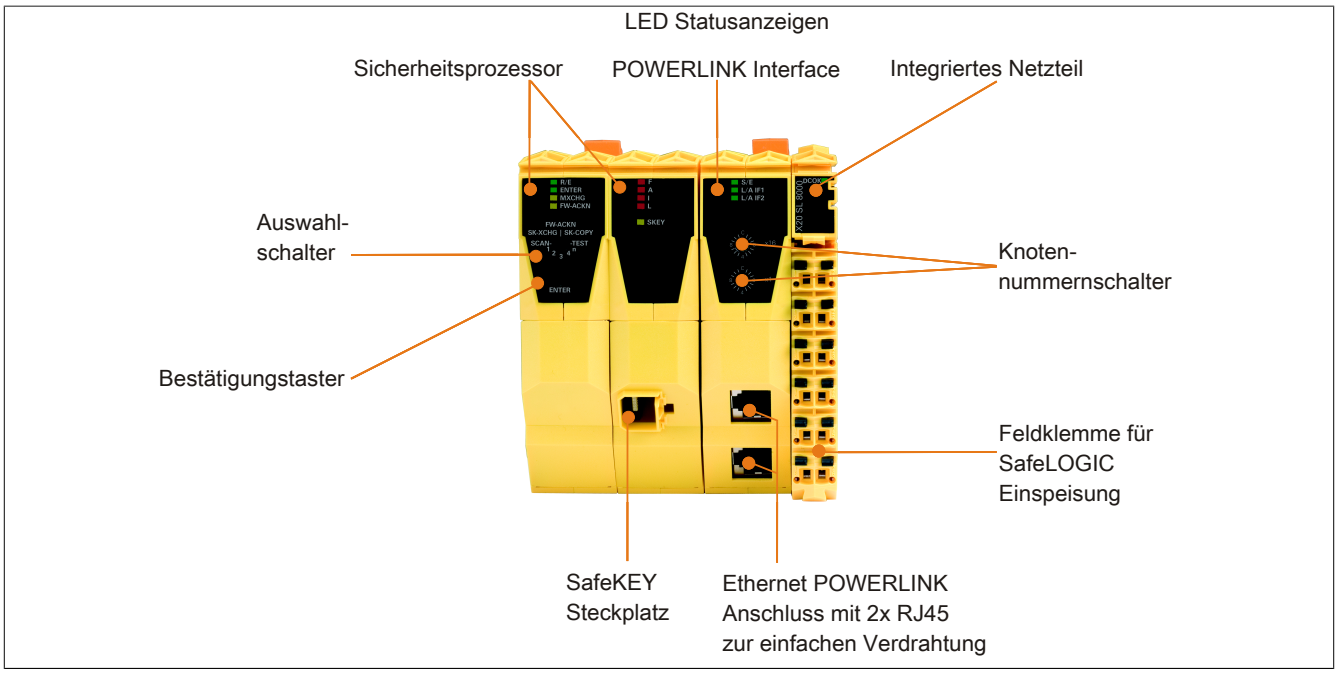
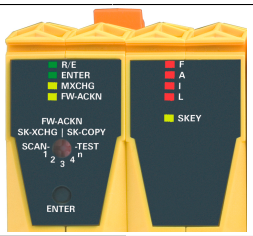


Abbildung 1: X20SL80xx Bedienelemente

Mit Hilfe des im Kapitel 8.1 "Fernbedienung" auf Seite 22 beschrieben Interface kann auch eine Bedienung der SafeLOGIC über ein Operator Panel realisiert werden.

5.1 Sicherheitsprozessor

5.1.1 Status LEDs des Sicherheitsprozessors



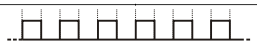
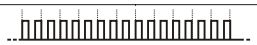
LED	Farbe	Status	Beschreibung
R/E		Aus	Hochlaufphase
	Grün	Ein	Applikation ist vorhanden und wird exekutiert
		Blinkend	Applikation vorhanden, wird jedoch nicht abgearbeitet (im Download Dialog des SafeDESIGNERS wurde "Automatischer Start" nicht angewählt ODER Hochlaufphase d.h. noch nicht alle notwendigen sicheren Module am Netzwerk wurden korrekt konfiguriert.)
	Orange	Ein	SafeDESIGNER ist im Debug Mode
		Blinkend	SafeDESIGNER ist im Debug Mode, Applikation im Stop
		Schnell blinkend	Am SafeKEY ist keine Applikation vorhanden
ENTER	Grün	Ein	Fehlende Autorisierung
		1x Blinken für 0,8 s	Bestätigung einer korrekten Eingabe
		Blinkend (1 Hz) für 5 sec.	Fehlbedienung
MXCHG	Orange	AUS	Modulkonfiguration in Ordnung
			Tauschen 1 Modul erkannt
			Tauschen 2 Module erkannt
			Tauschen 3 Module erkannt
			Tauschen 4 Module erkannt
			Tauschen mehr als 4 Module erkannt
			Fehlendes Modul erkannt
FW-ACKN	Orange	Aus	Firmware Konfiguration ok
		Blinkend	Firmware Update wurde durchgeführt
		Ein	SafeKEY wurde getauscht
ENTER MXCHG FW-ACKN	Grün Orange Orange	Durchlaufende Sequenz	Modul-Scan wird ausgeführt oder Hochlaufphase (ab Release 1.5 - Hinweis: LED "STATUS" Status LEDs für das POWERLINK Interface kontrollieren!).
FAIL	Rot		Die vier LEDs "FAIL" signalisieren das Hochlaufverhalten bzw. nach dem Hochlauf den gesamtmodulbetreffenden Fail Safe Zustand.
		F **A** **I** **L** x x x x x x x x x **X** x **X** **X** x x x x x = leuchtend **X** = stark leuchtend	**Bedeutung** Bootphase, Laden der Firmware, Zustand bei Fehlen des SafeKEY Vollständiger HW Test (max. Dauer ca. 5 Sek.) Initialisierung und Startup der Firmware Preoperational State Operational State Gesamtmodulbetreffender Fail Safe Zustand
		abwechselndes Blinken von "FI" und "AL"	SafeDESIGNER ist im Run - Debug Mode
SKEY	Orange	Aus	Kein Zugriff auf den SafeKEY
		Blinkend	Zugriff auf den SafeKEY

Tabelle 5: X20SL80xx Statusanzeige Sicherheitsprozessor

Gefahr!

Statisch leuchtende LEDs "FAIL" signalisieren ein defektes Modul, welches sofort auszutauschen ist. Sorgen Sie eigenverantwortlich dafür, dass nach dem Auftreten eines Fehlers alle notwendigen Reparaturmaßnahmen eingeleitet werden, da nachfolgende Fehler eine Gefährdung auslösen können!

5.1.2 LED Test

Mit Hilfe des folgenden Ablaufes kann die Funktion der LEDs getestet werden:

- Auswahlschalter auf TEST stellen
- Bestätigungstaste drücken
- Exakt für die Dauer der Betätigung des Bestätigungstasters werden alle LEDs des Sicherheitsprozessors (linkes und mittleres Modul der SafeLOGIC) eingeschaltet
  Bei Releases < 1.4 wird bei diesem Test die "SKEY" LED nicht eingeschaltet

5.1.3 Auswahlschalter und Bestätigungstaster

Sind Konfigurationsbestätigungen durch den Anwender notwendig, werden diese durch Vorwahl der gewünschten Funktion mittels Auswahlschalter und anschließendem Drücken des Bestätigungstasters "ENTER" durchgeführt.

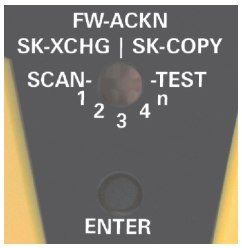


Abbildung 2: X20SL80xx Auswahlschalter und Betätigungstaster

Schalterstellung	Funktionalität	Beschreibung
FW-ACKN	Firmware Acknowledge	Bestätigung Firmwaretausch bei einem oder mehreren Modulen[1)]
unbeschriftete Position zwischen FW-ACKN und SK-XCHG	SafeKEY Format	SafeKEY formatieren (ab Release 1.4)[1)]
SK-XCHG	SafeKEY Exchange	Bestätigen des Austauschs des SafeKEYs[1)]
SK-COPY	SafeKEY Copy	Kopieren der Konfigurationsdaten vom SafeKEY[1)]
SCAN	Scannen	Auslösen eines Modul-Scans
TEST	Test	Durchführung eines LED Tests
1,2,3,4,n	Modultausch	Tausch von 1, 2, 3, 4 oder mehr als 4 Modulen bestätigen

Tabelle 6: X20SL80xx Bestätigungsmodi

1) löst einen automatischen Neustart aus

Bestätigung (alle Funktionen außer "SafeKEY Format")

Für eine Bestätigung muss der Bestätigungstaster für eine Dauer von 0,5 - 5 s gedrückt werden. Nach 0,5 s beginnt die LED "ENTER" (siehe Kapitel 5.1.1 "Status LEDs des Sicherheitsprozessors" auf Seite 4) zu leuchten. Nach Loslassen des Bestätigungstasters leuchtet die LED "ENTER" noch weitere 0,8 s nach. Mit dieser Sequenz wird eine korrekte Eingabe signalisiert.

- Wird der Bestätigungstaster vor 0,5 s losgelassen, so hat dies keinerlei Auswirkung.
- Wird der Bestätigungstaster länger als 5 s gedrückt, dann blinkt die LED "ENTER" für 5 s und zeigt damit eine Fehlbedienung an.

Ein weiterer möglicher Grund für eine Fehlbedienung ist eine unpassende Stellung des Auswahlschalters. Wenn man z. B. den Modultausch von genau einem Modul bestätigen möchte, dann muss der Auswahlschalter auf der Stellung "1" stehen (siehe Kapitel 7.1.4 "Tauschen eines einzelnen Moduls" auf Seite 18). Wird in diesen Fällen mittels des Bestätigungstasters eine andere Stellung als "1" bestätigt, so gilt das als Fehlbedienung und die LED "ENTER" blinkt ebenfalls 5 s.

Bestätigung "SafeKEY Format"

Für eine Bestätigung des "SafeKEY Format" muss der Bestätigungstaster für eine Dauer von 20 - 30 s gedrückt werden. Nach 20 s beginnt die LED "ENTER" zu leuchten. Nach Loslassen des Bestätigungstasters leuchtet die LED "ENTER" noch weitere 0,8 s nach. Mit dieser Sequenz wird eine korrekte Eingabe signalisiert.

- Wird der Bestätigungstaster vor 20 s losgelassen, so hat dies keinerlei Auswirkung.
- Wird der Bestätigungstaster länger als 30 s gedrückt, dann blinkt die LED "ENTER" für 5 s und zeigt damit eine Fehlbedienung an.

Es werden alle Daten (inkl. Passwort) gelöscht - deshalb wird empfohlen, anschließend mit dem SafeDESIGNER online zu gehen und ein neues Passwort zu vergeben.

5.2 Steckplatz für Programmspeicher (SafeKEY)

Zum Betrieb der SafeLOGIC ist ein Programmspeicher (SafeKEY) zum Speichern des Programms, der Parameter und der Systemkonfiguration erforderlich. Als SafeKEY stehen aus dem X20 System Zubehör die Memory Key Varianten X20MK0201 (2 MB) sowie X20MK0203 (8 MB) zur Verfügung. Der Memory Key ist nicht im Lieferumfang der SafeLOGIC enthalten, sondern muss als Zubehör extra bestellt werden!

Der SafeKEY ist mit einer mechanischen Verriegelung ausgestattet, um das unbeabsichtigte Ziehen während des Betriebes zu erschweren.

Abbildung 3: SafeKEY entriegelt

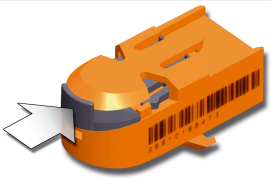


Abbildung 4: SafeKEY verriegelt

Information:

Das Ziehen des SafeKEYs während des Betriebs führt zum Neustart der SafeLOGIC und damit zur Abschaltung aller sicherheitstechnischer Aktoren.

Das Ziehen des SafeKEYs während des Betriebs kann zu einer Zerstörung der Daten am SafeKEY führen.

Das Ziehen des SafeKEYs während des Betriebs ist deshalb unbedingt zu vermeiden.

5.3 POWERLINK Interface

5.3.1 Status LEDs für das POWERLINK Interface

Abbildung	LED	Farbe	Status	Beschreibung
	STATUS[1)]	Grün/rot		Status/Error LED. Die LED Stati sind im nachfolgenden Abschnitt beschrieben.
	L/A IFx	Grün	Ein	Der Link zur Gegenstelle ist aufgebaut.
			Blinkend	Der Link zur Gegenstelle ist aufgebaut. Die LED blinkt, wenn am Bus eine Ethernet Aktivität vorhanden ist.

Tabelle 7: X20SL80xx POWERLINK Interface Statusanzeige

1) Die Status/Error LED ist eine grün/rote Dual LED.

5.3.2 LED STATUS

Die LED STATUS ist als Dual LED in den Farben grün und rot ausgeführt. Die Farbe rot (Error) wird von der Farbe grün (Status) überlagert.

Farbe rot - Error	Beschreibung
Ein	Das POWERLINK Interface befindet sich in einem Fehlerzustand (Ausfall von Ethernet Frames, Häufung von Kollisionen am Netzwerk usw.). Anmerkung: Direkt nach dem Einschalten werden einige rote Blinksignale angezeigt. Dabei handelt es sich aber um keine Fehler.

Tabelle 8: X20SL80xx POWERLINK Schnittstelle Status/Error leuchtet rot

Farbe grün - Status	Beschreibung
Aus	Das POWERLINK Interface ist entweder nicht versorgt oder befindet sich im Zustand NOT_ACTIVE. In diesem Zustand wartet das POWERLINK Interface nach einem Neustart ungefähr 5 Sekunden. Es ist keine Kommunikation mit dem POWERLINK Interface möglich. Wird in diesen 5 s keine POWERLINK Kommunikation erkannt, geht das POWERLINK Interface in den Zustand BASIC_ETHERNET über (flackernd). Wenn jedoch vor Ablauf der Zeit eine POWERLINK Kommunikation erkannt wird, geht das POWERLINK Interface direkt in den Zustand PRE_OPERATIONAL_1 über (Single Flash).
Grün flackernd (ca. 10 Hz)	Das POWERLINK Interface hat keine POWERLINK Kommunikation erkannt. In diesem Zustand ist es möglich, mit dem POWERLINK Interface direkt per UDP zu kommunizieren. Wird während dieses Zustandes eine POWERLINK Kommunikation erkannt, geht das POWERLINK Interface in den Zustand PRE_OPERATIONAL_1 über (Single Flash).
Single Flash (ca. 1 Hz)	Das POWERLINK Interface befindet sich im Zustand PRE_OPERATIONAL_1. Der CN (Controlled Node) wartet auf den Empfang eines SoC Frames und wechselt dann in den Zustand PRE_OPERATIONAL_2 (Double Flash).
Double Flash (ca. 1 Hz)	Das POWERLINK Interface befindet sich im Zustand PRE_OPERATIONAL_2. In diesem Zustand wird das POWERLINK Interface üblicherweise vom Manager konfiguriert. Danach wird per Kommando in den Zustand READY_TO_OPERATE weitergeschaltet (Tripple Flash). Hinweis: Es wird nicht in den nächsten Status geschalten, wenn z.B.: eine falsche Knotennummer eingestellt ist, oder das Modul im AS deaktiviert ist.
Tripple Flash (ca. 1 Hz)	Das POWERLINK Interface befindet sich im Zustand READY_TO_OPERATE. Der Manager schaltet per Kommando in den Zustand OPERATIONAL weiter.
Ein	Das POWERLINK Interface befindet sich im Zustand OPERATIONAL.
Blinkend (ca. 2,5 Hz)	Das POWERLINK Interface befindet sich im Zustand STOPPED. Output Daten werden nicht ausgegeben und es werden keine Input Daten geliefert. Dieser Zustand kann nur durch ein entsprechendes Kommando vom Manager erreicht und wieder verlassen werden.

Tabelle 9: X20SL80xx POWERLINK Schnittstelle Status/Error LED leuchtet grün

5.3.3 POWERLINK Stationsnummer

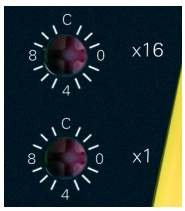


Abbildung 5: X20SL80xx POWERLINK Stationsnummernschalter

Mittels der beiden Nummernschalter wird die Stationsnummer der POWERLINK Station eingestellt. Stationsnummern im Bereich $01 bis $EF sind erlaubt.

Schalterstellung	Beschreibung
$00	Reserviert, Schalterstellung ist nicht erlaubt.
$01 - $EF	Stationsnummer der POWERLINK Station. Betrieb als Controlled Node (CN).
$F0 - $FF	Reserviert, Schalterstellung ist nicht erlaubt.

Tabelle 10: X20SL80xx Stationsnummer POWERLINK V2

5.3.4 RJ45 Ports

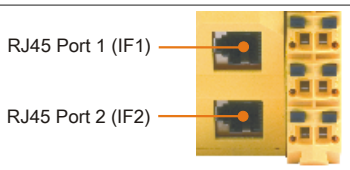


Abbildung 6: X20SL80xx RJ45 Ports

Pin	Belegung
1	RXD
2	RXD\
3	TXD
4	Termination
5	Termination
6	TXD\
7	Termination
8	Termination

Tabelle 11: X20SL80xx Pinbelegung für RJ45 Port

RXD ... Receive Data TXD ... Transmit Data

5.4 SG Unterstützung

SG3 / SGC

Die SafeLOGIC wird zur Zeit auf SG3 und SGC Targets nicht unterstützt.

SG4

Die SafeLOGIC wird mit installierter Firmware ausgeliefert. Weiters wird mit dem Download des Automation Studio Projektes die zum eingestellten Safety Release passende Firmwareversion auf der funktionalen CPU hinterlegt.

Bei unterschiedlicher Version wird automatisch die auf der funktionalen CPU hinterlegte Firmware auf das Modul geladen.

Bei einer Änderung der sicherheitsrelevanten Firmware auf der SafeLOGIC sind die in Kapitel "Bestätigung eines Firmwaretauschs" auf Seite 19 angeführten Maßnahmen durchzuführen.

5.5 Integriertes Netzteil

Für die Versorgung der SafeLOGIC ist ein Netzteil integriert.

5.5.1 Status LEDs für integriertes Netzteil

Abbildung	LED	Farbe	Status	Beschreibung
	DCOK	Grün	Ein	Modul mit Spannung versorgt
			Aus	Modul nicht mit Spannung versorgt

Tabelle 12: X20SL80xx Statusanzeige für integriertes Netzteil

5.5.2 Anschlussbelegung für das integrierte Netzteil

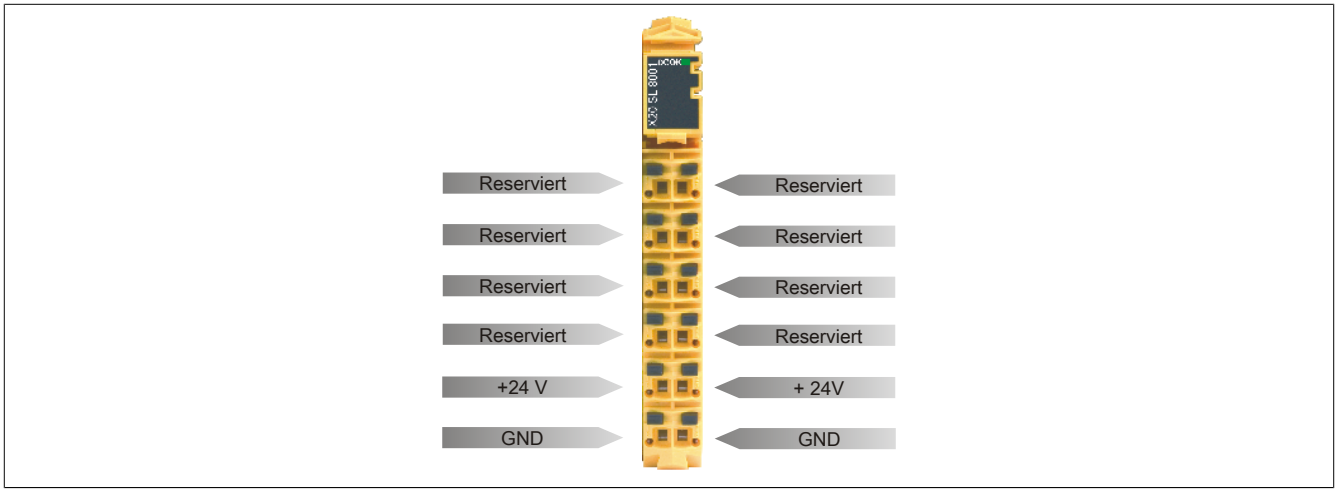


Abbildung 7: SafeLOGIC Anschlussbelegung des integrierten Netzteils

5.5.3 Anschlussbeispiel

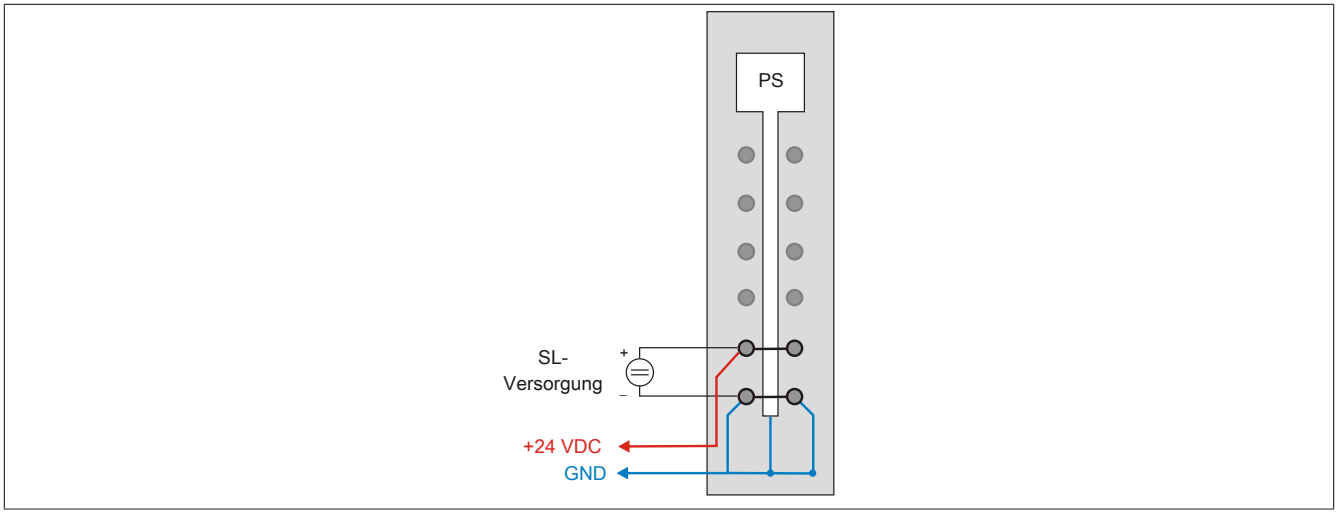


Abbildung 8: SafeLOGIC Anschlussbeispiel

6 Registerbeschreibung X20SL80xx

6.1 Parameter in der I/O Konfiguration

Gruppe: POWERLINK parameters

Parameter	Beschreibung	Default Wert	Einheit
Mode	SafeLOGIC kann nur als "controlled node" betrieben werden. Der "Management node (MN)" wird nicht unterstützt.	controlled node	-
Response timeout [us]	Response timeout für POWERLINK. • Erlaubte Werte: 1 - 30000	25	µs
Multiplexed station	Festlegen der Multiplexed Station Betriebsart.	off	-

Parameter Wert	Beschreibung
on	SafeLOGIC wird als Multiplexed Station betrieben.
off	SafeLOGIC wird nicht als Multiplexed Station betrieben.

Tabelle 13: Parameter I/O Konfiguration: POWERLINK parameters

Gruppe: Function model

Parameter	Beschreibung	Default Wert	Einheit
Function model	Dieser Parameter ist für zukünftige Funktionserweiterungen reserviert.	default	-

Tabelle 14: Parameter I/O Konfiguration: Function model

Gruppe: General

Parameter	Beschreibung	Default Wert	Einheit
Modul supervised	Systemverhalten bei fehlendem Modul	on	-

Parameter Wert	Beschreibung
on	Fehlendes Modul löst Service Mode aus.
off	Fehlendes Modul wird ignoriert.

Node used as IP gateway	Dieser Parameter ist für zukünftige Funktionserweiterungen reserviert.	240	-
SafeLOGIC ID	Bei Applikationen mit mehreren SafeLOGICen legt dieser Parameter die eindeutige SafeLOGIC Adresse fest. • Erlaubte Werte: 1 - 1024	wird automatisch vergeben	-
SafeMODULE ID	Eindeutige Safety Adresse des Moduls • Erlaubte Werte: 1	1	-
SafeDESIGNER project	Name des Sicherheitsprojekts	wird automatisch vergeben	-
Safe Runtime version (bis Release 1.3)	reserviert	-	-
SafeDESIGNER version	SafeDESIGNER Version für das Sicherheitsprojekt dieser SafeLOGIC	wird automatisch vergeben	-
Authorization	Aktivierung der Funktion "Autorisierung" - siehe Autorisierung.	disabled	-

Parameter Wert	Beschreibung
enabled	Funktion "Autorisierung" ist aktiviert - funktionale CPU kann Quittieraktionen der SL blockieren.
disabled	Funktion "Autorisierung" ist deaktiviert - kein Einfluss der funktionalen CPU auf die Quittierfunktionen.

Tabelle 15: Parameter I/O Konfiguration: General

Gruppe: SafeDESIGNER to SafeLOGIC communication

Ab SafeLOGIC V1.4.0.0 und Automation Runtime V3.04:

Mit aktiviertem SPROXY kann die SafeLOGIC über einen TCP/IP-Port der funktionalen CPU erreicht werden.

Dies nutzt die SafeDESIGNER-Einstellung "SL- Kommunikation über die CPU" (ab SafeDESIGNER V2.80).

Parameter	Beschreibung	Default Wert	Einheit
Activate SPROXY	Aktiviert die SafeDESIGNER Onlineverbindung	off	-
Server Communication Port	TCP/IP Portnummer, über den die SafeLOGIC erreichbar ist. **Hinweis:** wenn mehrere SafeLOGICen im Projekt vorhanden sind, muss für jede eine andere Portnummer eingestellt werden!	50000	-

Tabelle 16: Parameter I/O Konfiguration: SafeDESIGNER to SafeLOGIC communication

Gruppe: CPU to SafeLOGIC communication

Parameter	Beschreibung	Default Wert	Einheit
Number of BOOL channels	Anzahl der BOOL Kanäle von der CPU zur SafeLOGIC. • Erlaubte Werte: 0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96;	8	-
Number of extended BOOL channels	Anzahl der BOOL Kanäle von der CPU zur SafeLOGIC. • Erlaubte Werte: 0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256;	0	-
Number of INT channels	Anzahl der INT Kanäle von der CPU zur SafeLOGIC. • Erlaubte Werte: 0 - 30;	0	-
Number of UINT channels	Anzahl der UINT Kanäle von der CPU zur SafeLOGIC. • Erlaubte Werte: 0 - 30;	0	-
Number of DINT channels (Safety Release 1.4 und AR V3.08 erforderlich)	Anzahl der DINT Kanäle von der CPU zur SafeLOGIC • Erlaubte Werte: 0-15;	0	-
Number of UDINT channels	Anzahl der UDINT Kanäle von der CPU zur SafeLOGIC. • Erlaubte Werte: 0 - 15;	0	-

Tabelle 17: Parameter I/O Konfiguration: CPU to SafeLOGIC communication

Gruppe: SafeLOGIC to CPU communication

Parameter	Beschreibung	Default Wert	Einheit
Number of BOOL channels	Anzahl der BOOL Kanäle von der SafeLOGIC zur CPU. • Erlaubte Werte: 0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96;	8	-
Number of extended BOOL channels	Anzahl der BOOL Kanäle von der SafeLOGIC zur CPU. • Erlaubte Werte: 0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256;	0	-
Number of INT channels	Anzahl der INT Kanäle von der SafeLOGIC zur CPU. • Erlaubte Werte: 0 - 30;	0	-
Number of UINT channels	Anzahl der UINT Kanäle von der SafeLOGIC zur CPU. • Erlaubte Werte: 0 - 30;	0	-
Number of DINT channels (Safety Release 1.4 und AR V3.08 erforderlich)	Anzahl der DINT Kanäle von der SafeLOGIC zur CPU. • Erlaubte Werte: 0-15;	0	-
Number of UDINT channels	Anzahl der UDINT Kanäle von der SafeLOGIC zur CPU. • Erlaubte Werte: 0 - 15;	0	-

Tabelle 18: Parameter I/O Konfiguration: SafeLOGIC to CPU communication

Gruppe: SafeLOGIC to SafeLOGIC communication

Parameter	Beschreibung	Default Wert	Einheit
Use as source SafeLOGIC	Dieser Parameter konfiguriert diese SafeLOGIC als Datenquelle zu einer weiteren SafeLOGIC.		

Parameter Wert	Beschreibung
Ein	Diese SafeLOGIC steht als Datenquelle für eine weitere SafeLOGIC zur Verfügung.
Aus	Diese SafeLOGIC steht nicht als Datenquelle für weitere SafeLOGICen zur Verfügung.

Extended source SafeLOGIC communication (Safety Release 1.4 und AR V3.08 erforderlich)	Aktiviert die Möglichkeit, die Anzahl der Datenpunkte der SafeLOGIC-zu-SafeLOGIC-Kommunikation zu parametrieren für Verbindungen bei denen diese SafeLOGIC als Datenquelle für eine weitere SafeLOGIC dient.	off	-
Connected SafeLOGIC modules[1)] SafeLOGIC ID of connection *1-10* (bis Safety Release 1.3)	Dieser Parameter konfiguriert eine SafeLOGIC zu SafeLOGIC Kommunikation. Eine X20SL8001 ist in der Lage mit 10 weiteren SafeLOGICen zu kommunizieren, so dass an dieser Stelle 10 Kommunikationsverbindungen zur Verfügung stehen. Als Parameterwert ist an dieser Stelle die SafeLOGIC ID der für die jeweilige Kommunikationsverbindung relevanten SafeLOGIC einzutragen.	0	-
Gruppe: Connected SafeLOGIC modules[1)] (ab Safety Release 1.4)			
Gruppe: Connection *1-10*	Parametrierung der maximal 10 SafeLOGICen zu denen diese SafeLOGIC eine Verbindung aufbaut.		
SafeLOGIC ID of connection *1-10*	SafeLOGIC ID zu der eine Verbindung aufgebaut werden soll	0	-
Gruppe: Output channels (Safety Release 1.4 und AR V3.08 erforderlich)			
Number of BOOL channels	Anzahl der Kanäle mit dem jeweiligen Datentyp	8	-
Number of INT channels		0	-
Number of UINT channels		0	-
Number of DINT channels		0	-
Number of UDINT channels		0	-
Gruppe: Input channels (Safety Release 1.4 und AR V3.08 erforderlich)			
Number of BOOL channels	Anzahl der Kanäle mit dem jeweiligen Datentyp	8	-
Number of INT channels		0	-
Number of UINT channels		0	-
Number of DINT channels		0	-
Number of UDINT channels		0	-

Tabelle 19: Parameter I/O Konfiguration: SafeLOGIC to SafeLOGIC communication

1) nur X20SL8001 und X20SL8011

6.2 Parameter im SafeDESIGNER

Gruppe: Basic

Parameter	Beschreibung	Default Wert	Einheit
Min_required_FW_Rev	Dieser Parameter ist für zukünftige Funktionserweiterungen reserviert.	Basic Release	-
Cycle_Time_us	Mit diesem Parameter wird die Zykluszeit der SafeLOGIC festgelegt. • Erlaubte Werte: 800 - 20000 µs Der eingestellte Wert wird intern auf das nächste ganzzahlige Vielfache der POWERLINK Zykluszeit aufgerundet.	2000	µs
Cycle_Time_max_us (ab Release 1.5)	Parameter zur Kontrolle auf Überschreitung einer maximalen Zeit zwischen 2 Zyklen. • Erlaubte Werte: 800 - 21000µs ACHTUNG: Der Wert sollte nicht genau gleich der tatsächlichen Zykluszeit sein, sondern eventuelle Netzwerkjitter müssen berücksichtigt werden.	21000	µs
SSDO_Creation	Dieser Parameter definiert die Anzahl der azyklischen Bearbeitung pro SafeLOGIC Zyklus. Mit diesem Parameter lässt sich das Hochlaufverhalten des Systems optimieren, wobei der Defaultwert "Zeitabhängig" die Kompatibilität zum Release 1.1 sicherstellt.	Zeitabhängig	-

Parameter Wert	Beschreibung
Zeitabhängig	Abhängig von der SafeLOGIC Zykluszeit (kompatibel zu Release 1.1): • bei Zykluszeiten <= 3 ms = 1_per_5_cyle • bei Zykluszeiten > 3 ms = 1_per_cycle
1 je 5 Zyklen	Eine azyklische Bearbeitung wird auf 5 SafeLOGIC Zyklen verteilt • kann zu langen Hochlaufzeiten führen • geringster Kommunikationsoverhead im Zyklus
1 je Zyklus	Eine azyklische Bearbeitung pro SafeLOGIC Zyklus • neutrale Hochlaufzeiten • neutraler Kommunikationsoverhead im Zyklus
5 je Zyklus	5 azyklische Bearbeitungen je SafeLOGIC Zyklus • minimale Hochlaufzeiten • maximaler Kommunikationsoverhead im Zyklus

Node_Guarding_Timeout_s	Timeout für den Wechsel der Safety Module in den Pre Operational State nach dem Ausfall der SafeLOGIC bzw. bei einem Kommunikationsproblem zwischen Safety Modul und SafeLOGIC. Dieser Parameter bestimmt auch, wie lange es dauert, bis die SafeLOGIC es erkennt, wenn ein Modul fehlt. **Hinweise** • Je kürzer die Zeit, desto höher das asynchrone Datenaufkommen. • Diese Einstellung ist nicht sicherheitskritisch - die Zeit für die sichere Abschaltung der Aktoren wird unabhängig davon mit dem Parameter Worst_Case_Response_Time bestimmt.	60	s
ExternalMachineOptions (ab Release 1.4)	Aktivierung der externen Maschinenoptionen	Nein	-

Parameter Wert	Beschreibung
Ja-ACHTUNG	externe Maschinenoptionen sind aktiviert
Nein	externe Maschinenoptionen sind deaktiviert

ExternalStartupFlags (ab Release 1.4)	Aktivierung der externen Startup-Flags	Nein	-

Parameter Wert	Beschreibung
Ja-ACHTUNG	externe Startup-Flags sind aktiviert
Nein	externe Startup-Flags sind deaktiviert

RemoteControlAllowed (ab Release 1.4)	Aktivierung der Fernsteuerung der SafeLOGIC	Nein	-

Parameter Wert	Beschreibung
Ja-ACHTUNG	Fernsteuerung der SafeLOGIC freigeschalten
Nein	Fernsteuerung der SafeLOGIC gesperrt

Tabelle 20: Parameter SafeDESIGNER: Basic

Information:

Der Parameter "Cycle_Time_us" muss größer sein als die Bearbeitungszeit für die Sicherheitsapplikation. Die Bearbeitungszeit kann im Online Dialog Fenster mit der Funktion "Info" bestimmt werden. Ist der Parameter "Cycle_Time_us" kleiner bzw. zu nahe an der notwendigen Bearbeitungszeit, so kann es zu einer Zykluszeitverletzung kommen.

Weitere Informationen hierzu finden sie auch unter Abschnitt 6.4 "SafeLOGIC Info Dialog im SafeDESIGNER" auf Seite 16.

Gefahr!

Sofern einer der Parameter "ExternalMachineOptions", "ExternalStartupFlags" bzw. "RemoteControlAllowed" auf "JA - Achtung" gesetzt wird und damit das Nutzen einer dieser Funktionen im SafeDESIGNER freigeschaltet wird, müssen unbedingt die damit verbundenen Hinweise im Kapitel 8 "POWERLINK Dateninterface" auf Seite 22 beachtet werden. Andernfalls kann es durch Fehlfunktionen zu gefahrbringenden Zuständen kommen.

Gruppe: Safety_Response_Time_Defaults

Üblicherweise werden die Parameter zur sicheren Reaktionszeit für alle an der Applikation beteiligten Knoten gleich eingestellt. Aus diesem Grund werden diese Parameter im SafeDESIGNER bei der SafeLOGIC in der Gruppe Safety_Response_Time_Defaults konfiguriert.

Wird bei den einzelnen Modulen der Parameter "Manual_Configuration = Nein" gesetzt, so werden diese Default Werte verwendet.

Parameter	Beschreibung	Default Wert	Einheit
Synchronous_Network_Only	Dieser Parameter legt die Synchronisationseigenschaften des Zugrunde liegenden Netzwerks fest. **Parameter Wert** / **Beschreibung** Ja: Für die Berechnung der sicheren Reaktionszeit werden ausschließlich synchrone Netzwerke mit gleichen Zykluszeiten oder ganzzahligen Verhältnissen der Zykluszeiten vorausgesetzt. Nein: Keine Anforderung an die Synchronität der Netzwerke.	Ja	-
Max_X2X_CycleTime_us	Dieser Parameter gibt die max. X2X Zykluszeit für die Berechnung der sicheren Reaktionszeit an. • Erlaubte Werte: 200 - 30000 µs	5000	µs
Max_Powerlink_CycleTime_us	Dieser Parameter gibt die max. POWERLINK Zykluszeit für die Berechnung der sicheren Reaktionszeit an. • Erlaubte Werte: 200 - 30000 µs	5000	µs
Max_CPU_CrossLinkTask_CycleTime_us	Dieser Parameter gibt die max. Zykluszeit für den Kopiertask in der CPU für die Berechnung der sicheren Reaktionszeit an. Ein Wert von "0" signalisiert, dass für die Reaktionszeit kein Kopiertask berücksichtigt wird. • Erlaubte Werte: 0 - 30000 µs	5000	µs
Min_X2X_CycleTime_us	Dieser Parameter gibt die min. X2X Zykluszeit für die Berechnung der sicheren Reaktionszeit an. • Erlaubte Werte: 200 - 30000 µs	200	µs
Min_Powerlink_CycleTime_us	Dieser Parameter gibt die min. POWERLINK Zykluszeit für die Berechnung der sicheren Reaktionszeit an. • Erlaubte Werte: 200 - 30000 µs	200	µs
Min_CPU_CrossLinkTask_CycleTime_us	Dieser Parameter gibt die min. Zykluszeit für den Kopiertask in der CPU für die Berechnung der sicheren Reaktionszeit an. Ein Wert von "0" signalisiert, dass für die Reaktionszeit auch Konfigurationen ohne Kopiertasks berücksichtigt werden. • Erlaubte Werte: 0 - 30000 µs	0	µs
Worst_Case_Response_Time_us	Dieser Parameter gibt den Grenzwert für die Überwachung der sicheren Reaktionszeit an. Der Wert des Parameters kann auch aus dem Berechnungstool für die sichere Reaktionszeit entnommen werden. • Erlaubte Werte: 3000 - 500000 µs	50000	µs

Tabelle 21: Parameter SafeDESIGNER: Safety_Response_Time_Defaults

Gruppe: Commissioning (nur X20SL8001 und X20SL8011)

Die Parameter SafeMachineOption00 - SafeMachineOption31 ermöglichen das Aktivieren bzw. Deaktivieren dedizierter Maschinenoptionen während der Inbetriebnahme.

Parameter	Beschreibung	Default Wert	Einheit
SafeMachineOptionXX	Mit diesem Parameter können bei der Inbetriebnahme einzelne Maschinenoptionen aktiviert oder deaktiviert werden.	AUS	-

Parameter Wert	Beschreibung
EIN	MaschinenoptionXX ist aktiviert, Kanal SafeMaschineOptionXX wird konstant auf SAFETRUE gesetzt.
AUS	MaschinenoptionXX ist deaktiviert, Kanal SafeMaschineOptionXX wird konstant auf SAFEFALSE gesetzt.

Tabelle 22: Parameter SafeDESIGNER: Commissioning (nur X20SL8001 und X20SL8011)

6.3 Kanalliste

Kanalname	Zugriff über Automation Studio	Zugriff über SafeDESIGNER	Datentyp	Beschreibung
ModuleOk	Read	-	BOOL	Kennung ob Modul OK
SerialNumber	Read	-	UDINT	Serialnummer des Moduls
ModuleID	Read	-	UINT	Modulkennung
HardwareVariant	Read	-	UINT	HW Variante
FirmwareVersion	Read	-	UINT	Firmwareversion des Moduls
UDID_low	Read	-	UDINT	UDID, unteren 4 Bytes
UDID_high	Read	-	UINT	UDID, oberen 2 Bytes
SafeModuleOK	-	Read	SAFEBOOL	Kennung ob sicherer Kommunikationskanal OK
BOOL1xx	Write	Read	BOOL	Kommunikationskanal CPU zur SafeLOGIC
BOOLext1xxx	Write	Read	BOOL	Kommunikationskanal CPU zur SafeLOGIC
INT1xx	Write	Read	INT	Kommunikationskanal CPU zur SafeLOGIC
UINT1xx	Write	Read	UINT	Kommunikationskanal CPU zur SafeLOGIC
UDINT1xx	Write	Read	UDINT	Kommunikationskanal CPU zur SafeLOGIC
BOOL0xx	Read	Write	BOOL	Kommunikationskanal SafeLOGIC zur CPU
BOOLext0xxx	Read	Write	BOOL	Kommunikationskanal SafeLOGIC zur CPU
INT0xx	Read	Write	INT	Kommunikationskanal SafeLOGIC zur CPU
UINT0xx	Read	Write	UINT	Kommunikationskanal SafeLOGIC zur CPU
UDINT0xx	Read	Write	UDINT	Kommunikationskanal SafeLOGIC zur CPU
SafeBOOLx	-	Write	SAFEBOOL	Kommunikationskanal SafeLOGIC zur SafeLOGIC
SafeMachineOptionxx[1)]	-	Read	SAFEBOOL	Interner Kanal für Maschinenoptionen

Tabelle 23: Kanalliste

1) Nur X20SL8001 und X20SL8011

Information:

Kanäle für SafeLOGIC to SafeLOGIC Communication: siehe Darstellung im SafeDESIGNER

6.4 SafeLOGIC Info Dialog im SafeDESIGNER

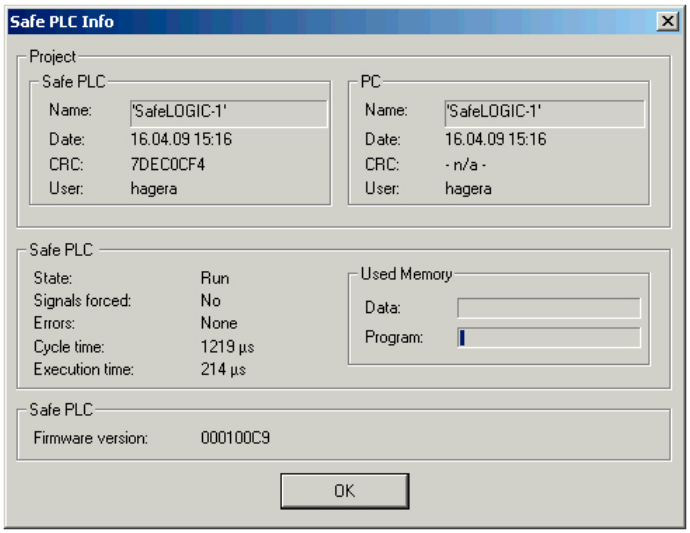


Abbildung 9: SafeLOGIC Info Dialog

Project	Projektbeschreibende Daten	
Safe PLC	Daten zum Projekt, welches am SafeKEY der SafeLOGIC gespeichert ist.	
	Name	Name des Projekts
	Date	Letztes Änderungsdatum
	CRC	CRC
	User	Anwender der letzten Änderung
PC	Daten zum SafeDESIGNER Projekt am PC	
	Name	Name des Projekts
	Date	Letztes Änderungsdatum
	CRC	CRC „- n/a -“, falls das Projekt nicht compiliert ist
	User	Anwender der letzten Änderung
Safe PLC	Status und Informationen zur SafeLOGIC	
State	Run	Die sicherheitstechnische Applikation wird ausgeführt.
	On	An der SafeLOGIC ist kein gültiges Programm am SafeKEY verfügbar.
	Stop [Safe]	Die SafeLOGIC ist im sicheren Modus. Ein Programm ist geladen, wird jedoch nicht ausgeführt.
	Run [Safe]	Die SafeLOGIC ist im sicheren Modus. Das Programm wird ausgeführt.
	Stop [Debug]	Die SafeLOGIC ist im Debug Modus. Das Programm wird nicht ausgeführt.
	Run [Debug]	Die SafeLOGIC ist im Debug Modus. Das Programm wird ausgeführt.
	Halt [Debug]	Die SafeLOGIC ist im Debug Modus. Das Programm wurde angehalten (Einzelzyklus).
	No Execution	Die SafeLOGIC befindet sich im Hochlauf: bereit für "Run", wartet aber noch auf Module.
	TIMEOUT	Kommunikationsproblem zwischen SafeDESIGNER und SafeLOGIC.
	Failure	Die SafeLOGIC ist im Zustand Fail SAFE.
Signals forced	No	Es sind keine Variablen geforced
	Yes	Es sind Variablen geforced
Errors	Information bezüglich verfügbarer Fehlermeldungen im SafeDESIGNER Meldungsfenster.	
Cycle time	Tatsächliche notwendige Zykluszeit, maximaler Wert seit letztem Power Up; dieser Wert ist nur aussagekräftig bei Safe PLC state = Run	
Execution time	Tatsächliche Applikations-Abarbeitungszeit; dieser Wert entspricht der Safe PLC Cycle time abzüglich System- und Kommunikationsoverhead	
Used Memory	Balken zur Darstellung der benutzten Systemresourcen	
	Data	Datenspeicher der sicheren Applikation
	Program	Programmspeicher der sicheren Applikation
Firmware version	Firmware Version	

Detaillierte Informationen zum SafeLOGIC Info Dialog im SafeDESIGNER siehe Online Hilfe SafeDESIGNER.

7 Wartungsszenarien

Die Beschreibung der Bedienelemente ist in Kapitel 5 "Bedien- und Anschlusselemente" auf Seite 3 zu finden.

7.1 Tauschen von Modulen

Die SafeLOGIC erkennt selbständig das Tauschen von sicheren Modulen. Das Gesamtsystem (SafeLOGIC, openSAFETY) sorgt nach dem Modultausch automatisch dafür, dass das Modul wieder mit den korrekten Parametern betrieben wird und inkompatible Modultypen abgewiesen werden. Somit verbleiben nach dem Modultausch folgende Fehlermöglichkeiten:

- Vertauschen der Klemmen zwischen mehreren Modulen
- Verdrahtungsfehler
- Vertauschungen von SafeIO Modulen untereinander

7.1.1 Vertauschen der Klemmen zwischen mehreren Modulen

Um das Vertauschen von Klemmen zwischen mehreren Modulen zu erkennen, muss der Anwender mittels eines Verdrahtungstests die Sicherheitsfunktion prüfen.

> **Gefahr!**
>
> **Der Verdrahtungstest muss vom Anwender so gestaltet sein, dass Vertauschungen von Klemmen erkannt werden.**
>
> **Führen Sie in jedem Fall eine Validierung der gesamten Sicherheitsfunktion durch!**

7.1.2 Verdrahtungsfehler

Falls die Verdrahtung zwischen Sensor bzw. Aktor und der X20 Klemme gelöst wird, kann es zu Verdrahtungsfehlern kommen. Um solche Fehler in der Verdrahtung zu erkennen, muss der Anwender mittels eines Verdrahtungstests die Sicherheitsfunktion prüfen.

> **Gefahr!**
>
> **Der Verdrahtungstest muss vom Anwender so gestaltet sein, dass Verdrahtungsfehler erkannt werden.**
>
> **Führen Sie in jedem Fall eine Validierung der gesamten Sicherheitsfunktion durch!**

7.1.3 Vertauschungen von SafeIO Modulen untereinander

Durch Fehler in der funktionalen Applikation können SafeIO Module vertauscht werden, was sich in der SafeLOGIC identisch zu einem Modultausch darstellt. Um diese Fehler aufzudecken, muss der Anwender die Anzahl der getauschten Module an der SafeLOGIC bestätigen. Damit ist die Anzahl der vom Anwender getauschten Module und der vom System erkannten Vertauschungen verknüpft und zusätzliche Vertauschungen können erkannt werden.

Die SafeLOGIC informiert den Anwender mittels Blinkcode an der LED MXCHG über die Anzahl der ermittelten Modul-Vertauschungen. Bis zu 4 unterschiedliche Module werden mit einem Blinkcode dargestellt. Der Blinkcode dauert jeweils 4 s, wobei die LED so oft eingeschaltet wird, wie es unterschiedliche Module gibt. Ab 5 unterschiedlichen Modulen blinkt die LED MXCHG durchgehend.

Der Anwender muss prüfen, ob die von der SafeLOGIC erkannte Anzahl und die tatsächliche Anzahl an getauschten Modulen übereinstimmen. Falls die Werte gleich sind, muss der Anwender die Anzahl bestätigen und anschließend einen Verdrahtungstest durchführen. Der Verdrahtungstest kann sich hier auf die getauschten Module konzentrieren.

Falls ein Unterschied vorliegen sollte, muss der Anwender die Anzahl der von der SafeLOGIC ermittelten Vertauschungen bestätigen und einen vollständigen Verdrahtungstest über alle Module durchführen.

> **Gefahr!**
>
> **Führen Sie in jedem Fall eine Validierung der gesamten Sicherheitsfunktion durch!**

7.1.4 Tauschen eines einzelnen Moduls

In Situationen, in denen nur ein Modul getauscht (LED MXCHG signalisiert einen Blinkcode für ein getauschtes Modul) und an der Verdrahtung nichts geändert wurde, kann der Anwender entscheiden, den Verdrahtungstest entfallen zu lassen, da in diesem Fall

- Vertauschen der Klemmen zwischen mehreren Modulen
- Verdrahtungsfehler
- Vertauschungen von SafeIO Modulen untereinander

ausgeschlossen werden können.

Gefahr!

Der Verdrahtungstest darf nur entfallen, wenn im Zuge des Tauschens eines einzelnen Moduls keine weiteren Veränderungen, wie z. B. Lösen weiterer Klemmen, Lösen der Verdrahtung, etc. vorgenommen wurden.

7.1.5 Modultausch bestätigen

Zur Bestätigung der Anzahl der getauschten Module muss der Auswahlschalter in eine der folgenden Stellungen gebracht werden:

- 1 - ein Modul getauscht
- 2 - zwei Module getauscht
- 3 - drei Module getauscht
- 4 - vier Module getauscht
- n - fünf oder mehrere Module getauscht

Bei bis zu vier getauschten Modulen kann der Tausch bestätigt und der anschließende Verdrahtungstest auf diese getauschten Module konzentriert werden. Bei mehr als vier getauschten Modulen muss ein vollständiger Verdrahtungstest über alle Module durchgeführt werden.

Nach dem Bestätigen des Modultausches beginnt die SafeLOGIC sofort mit einem Modul Scan.

Gefahr!

Der Verdrahtungstest muss vom Anwender so gestaltet sein, dass Verdrahtungsfehler oder Vertauschungen von Klemmen erkannt werden.

Führen Sie in jedem Fall eine Validierung der gesamten Sicherheitsfunktion durch!

7.2 Sonstige Fehler in der Modulkonfiguration

Die bisher betrachteten Unterschiede beziehen sich ausschließlich auf den Modultausch. Falls ein Gerät nicht vorhanden ist (Ausnahme nur wenn das Gerät als optional definiert wurde), eine falsche HW-Kennung hat oder sonstige Probleme am Modul vorliegen (z. B. falsche Parameter, aber die Parameter am Modul können von der SafeLOGIC nicht verändert werden), dann wird ein Fehler signalisiert. Dabei blinkt die LED "MXCHG" dauernd. Dieser Zustand wird nur signalisiert, wenn es keinen Zustand "Modultausch" und keinen Firmwaretausch gibt. Der Zustand kann nicht quittiert werden.

Gefahr!

Sorgen Sie eigenverantwortlich dafür, dass nach dem Auftreten eines Fehlers alle notwendigen Reparaturmaßnahmen eingeleitet werden, da nachfolgende Fehler eine Gefährdung auslösen können!

7.3 Bestätigung eines Firmwaretauschs

Eine Änderung an der FW wird durch Blinken der LED "FW-ACKN" angezeigt. Bestätigt wird dieser Zustand durch Wahl der Stellung "FW-ACKN". Ein Firmwaretausch muss immer mit einem vollständigen Funktionstest abgeschlossen werden.

Gefahr!

Der Funktionstest darf nur von Personen durchgeführt werden, welche mit der Sicherheitsapplikation und deren Funktionen vertraut sind und auf den Vorgang des Firmwaretauschs geschult sind.

Führen Sie in jedem Fall eine Validierung der gesamten Sicherheitsfunktion durch!

Gefahr!

Verwenden Sie ausschließlich Firmwareversionen, die in der zum TÜV-Zertifikat der B&R-Sicherheitstechnik gehörenden "Liste der Modulversionen" aufscheinen (siehe B&R Homepage unter Service > Allgemeine Downloads).

7.4 Auslösen eines Modul Scan

Bei einem Modul Scan wird untersucht, ob alle in der Applikation projektierten Module vorhanden sind und ob sie der Projekt-Konfiguration entsprechen. Der Modul Scan läuft üblicherweise automatisch, jedoch in großen Zeitintervallen ab. Um im Falle eines Modultausches die Wartezeit, bis die SafeLOGIC das getauschte Modul erkennt, zu minimieren, kann man diese Funktion auch manuell auslösen. Das Resultat des Scans wird unter folgenden Abschnitten beschrieben:

- "Tauschen von Modulen" auf Seite 17
- "Sonstige Fehler in der Modulkonfiguration" auf Seite 18
- "Bestätigung eines Firmwaretauschs" auf Seite 19

Der Vorgang selbst wird mit der Stellung "SCAN" des Auswahlschalters gestartet und mit einem Lauflicht mit den LEDs "ENTER", "MXCHG" und "FW-ACKN" signalisiert. Als Abschluss des Scans leuchtet die LED "ENTER" wieder für 0,8 s auf. Erst danach werden die Resultate signalisiert (z. B. drei Module getauscht).

7.5 SafeKEY

7.5.1 Ziehen eines SafeKEYs

Das Ziehen eines SafeKEYs führt immer zu einem Wechsel in den BOOT Zustand (es leuchten die Buchstaben LEDs "F", "I" und "L") und somit zu einer kompletten Abschaltung der sicheren Applikation.

Information:

Das Ziehen des SafeKEYs während des Betriebs führt zum Neustart der SafeLOGIC und damit zur Abschaltung aller sicherheitstechnischer Aktoren.

Das Ziehen des SafeKEYs während des Betriebs kann zu einer Zerstörung der Daten am SafeKEY führen.

Das Ziehen des SafeKEYs während des Betriebs ist deshalb unbedingt zu vermeiden.

Die Sequenz "Sicherung des SafeKEYs" ist von dieser Regelung ausgeschlossen.

7.5.2 Bestätigen eines SafeKEY Tauschs

Der Tausch eines SafeKEYs wird durch ein permanentes Leuchten der LED "FW-ACKN" signalisiert und muss mit den Bestätigungssequenzen "SK-XCHG" quittiert werden. Anschließend ist ein vollständiger Funktionstest vorgeschrieben.

Gefahr!

Das Tauschen eines SafeKEYs aktiviert die auf dem SafeKEY gespeicherte Sicherheitsapplikation. Prüfen Sie in jedem Fall die Projekt CRC und das Projektspeicherdatum der am SafeKEY gespeicherten Sicherheitsapplikation.

Gefahr!

Führen Sie in jedem Fall eine Validierung der gesamten Sicherheitsfunktion durch!

7.5.3 Austauschen der Applikation an der SafeLOGIC mittels SafeKEY Tausch

Am SafeKEY sind alle relevanten Konfigurationsdaten und alle Daten und Parameter zur Applikation gespeichert. Um im Falle eines Applikationstausches die bisherigen Konfigurationsdaten auf einen neuen SafeKEY zu übertragen, ist die folgende Sequenz anzuwenden:

- Auswahlschalter auf die Stellung "SK-COPY" stellen.
- Betätigen der Bestätigungstaste - Aktion wird mit der "ENTER" LED quittiert.
- Die Konfigurationsdaten des SafeKEYs werden nun in der SafeLOGIC gespeichert. Dabei blinkt die LED "SKEY" bei jedem Zugriff.
- Nach dem Kopiervorgang blinkt die "FW-ACKN" LED. Nun kann der bisherige SafeKEY gegen den SafeKEY mit der neuen Applikation getauscht werden. Für diesen Vorgang sind max. 30 Sekunden vorgesehen. Die Blinkfrequenz der "FW-ACKN" LED wird nach 20 Sekunden erhöht, um das Ende der Tauschphase zu signalisieren.
- Nachdem der neue SafeKEY gesteckt wurde, muss erneut die Bestätigungstaste gedrückt werden. Der Auswahlschalter bleibt dabei weiterhin auf der Stellung "SK-COPY".
- Die intern zwischengespeicherten Konfigurationsdaten werden auf den neuen SafeKEY gespeichert. Anschließend wird automatisch ein Reset ausgelöst und die Daten vom neuen SafeKEY werden übernommen.
- Nach dem Reset muss der Austausch des SafeKEYs bestätigt werden. Dazu den Auswahlschalter auf die Stellung "SK-XCHG" stellen.
- Betätigen der Bestätigungstaste - Aktion wird mit der "ENTER" LED quittiert.
- Durchführen eines vollständigen Funktionstests.

Information:

Wird nach 30 Sekunden der neue SafeKEY nicht quittiert, so endet die Funktion, d. h. falls die Funktion ungewollt ausgelöst wurde, so beendet sich die Kopierfunktion automatisch nach 30 Sekunden. Wird nach 30 Sekunden kein SafeKEY gesteckt, geht die SafeLOGIC in den BOOT Zustand über (Leuchten der Buchstaben LEDs "F", "I" und "L").

Gefahr!

Dieser Vorgang aktiviert die auf dem neuen SafeKEY gespeicherte Sicherheitsapplikation. Prüfen Sie in jedem Fall die Projekt CRC und das Projektspeicherdatum der am SafeKEY gespeicherten Sicherheitsapplikation.

Gefahr!

Führen Sie in jedem Fall eine Validierung der gesamten Sicherheitsfunktion durch!

Information:

Diese Sequenz kann auch zur Erstellung einer SafeKEY Sicherung genutzt werden, indem ein zweiter SafeKEY mit identischer Sicherheitsapplikation verwendet wird. Nach Ausführen der Sequenz stehen zwei identische SafeKEYs zur Verfügung (Sicherheitskopie).

7.6 Tauschen einer SafeLOGIC

Das Tauschen einer SafeLOGIC läuft mit den gleichen Mechanismen ab, wie ein normaler Modultausch. In der Regel muss beim Tauschen einer SafeLOGIC der SafeKEY von der getauschten SafeLOGIC übernommen werden, um ein Aktivieren einer veralteten, sicherheitstechnischen Applikation zu vermeiden.

Gefahr!

Führen Sie in jedem Fall eine Validierung der gesamten Sicherheitsfunktion durch!

7.7 Autorisierung

Die Funktionen

- Modultausch bestätigen
- Bestätigen eines Firmwaretauschs
- Bestätigen eines SafeKEY Tauschs
- Sicherung des SafeKEYs
- Tauschen einer SafeLOGIC

können von der funktionalen CPU blockiert werden. Damit können die Aktionen von einem applikationsspezifischen Benutzerkonzept abhängig gemacht werden. Diese Möglichkeit ist jedoch sicherheitstechnisch nicht belastbar, da diese Funktionen in der funktionalen CPU ablaufen.

Hierzu stehen die Objekte im Index 0x2402 zur Verfügung, auf welche über die POWERLINK Library zugegriffen werden kann.

Index:Subindex	Objektbezeichnung	Datentyp	Zugriff	Werte	Beschreibung
0x2402:0x00	Anzahl der Einträge	USINT	R	0x22	Anzahl der Einträge auf diesem Index
0x2402:0x01	EnableAutorization	UDINT	RW	"AENA", 0x41454E41	Aktivieren der Autorisierung
				"ADIS", 0x41444953	Deaktivieren der Autorisierung
0x2402:0x04	EnableModuleExchange	UDINT	RW	"UDID", 0x554444944	Autorisierung zur Bestätigung eines Modultausches ist gegeben
				Alle anderen Werte	Autorisierung zur Bestätigung eines Modultausches ist nicht gegeben
0x2402:0x05	EnableFWMismatch	UDINT	RW	"FWAC“, 0x46574143	Autorisierung zur Bestätigung eines Firmware Updates ist gegeben
				Alle anderen Werte	Autorisierung zur Bestätigung eines Firmware Updates ist nicht gegeben
0x2402:0x06	EnableSKeyExchange	UDINT	RW	"SKEY", 0x534B4559	Autorisierung zur Bestätigung eines SafeKEY Tausches ist gegeben
				Alle anderen Werte	Autorisierung zur Bestätigung eines SafeKEY Tausches ist nicht gegeben

Benutzeranforderungen an der SafeLOGIC für welche die notwendige Autorisierung von der CPU nicht vorliegt, werden mit einer statisch leuchtenden "ENTER" LED signalisiert.

8 POWERLINK Dateninterface

8.1 Fernbedienung

Voraussetzungen

Parameterumfeld	Parameter	Wert
Automation Studio: Properties Dialog "Change Runtime Versions"	Safety Release	>= 1.4
SafeDESIGNER: Parameter der Gruppe Basic der SafeLOGIC	RemoteControlAllowed	JA-Achtung

Gefahr!

- **Der Anwender muss in einer FMEA die Anwendung der Funktion und mögliche Risiken untersuchen. In der FMEA sind vor allem auch mögliche vorhersehbare Fehlanwendungen und typische anwendungsspezifische Fehlerquellen zu berücksichtigen. Mögliche Risiken sind durch zusätzliche Maßnahmen zu minimieren. Erst wenn das ermittelte Restrisiko für die vorgesehene Anwendung als gering genug eingeschätzt wird, darf diese Funktion im SafeDESIGNER freigeschaltet und genutzt werden.**
- **Die an der Ausführung der Funktion beteiligten Programmteile in der funktionalen Applikation müssen den Anforderungen der ISO 13849-1:2007, Kapitel 4.6.4 bzw. IEC 62061, Kapitel 6.11.2 entsprechen. Die korrekte Ausführung der Programmteile gemäß einer dieser Normen ist zu dokumentieren.**
- **Die Funktionen dürfen ausschließlich von hierzu autorisierten Personen ausgeführt werden. Der Zugriff auf die entsprechenden Visualisierungsteile ist mit geeigneten Mitteln abzusichern und auf den autorisierten Personenkreis einzuschränken.**
- **Bei einem Zugriff muss das lokale Personal über den Zugriff informiert werden. Der Anwender muss durch geeignete Maßnahmen sicherstellen, dass Fernzugriffe ohne Wissen des lokalen Personals nicht möglich sind.**
- **Die korrekte Funktion muss in einem vollständigen Funktionstest nachgewiesen werden. Die Durchführung der Tests und die Testergebnisse sind zu dokumentieren. Der Test muss so gestaltet werden, dass mögliche Datenvertauschungen zwischen der Visualisierung und der Sicherheitsapplikation aufgedeckt werden. Die korrekte Funktion muss nach Änderungen am Automation Runtime oder nach Änderungen der Funktionalen Applikation in einem vollständigen Funktionstest erneut nachgewiesen werden.**

Allgemeines

Ab dem Safety Release 1.4 können die für diverse Wartungsszenarien notwendigen Bestätigungssequenzen zusätzlich über fernbedienbare Services von der funktionalen Applikation ausgelöst werden. Zu diesem Zwecke wurde auf der SafeLOGIC eine POWERLINK Objektschnittstelle implementiert, welche im Automation Studio mit Hilfe der Bibliothek "AsEPL" bedient werden kann.

Fernbedienungsschnittstelle

POWERLINK V2 Objekt:

Index:Subindex	Objektbezeichnung	Datentyp	Zugriff	Werte	Beschreibung
0x2406:0x00	NumberOfEntries	USINT	R	0x02	Anzahl der Einträge auf diesem Index
0x2406:0x01	RemoteRequest_OCT	siehe Kommandostruktur	W	-	Auf dieses Element wird die Kommandostruktur geschrieben
0x2406:0x02	RemoteResponse_OCT	siehe Statusstruktur	R	-	Rückgabewert der SafeLOGIC nachdem der Status mitttels Kommando abgefragt wurde

Tabelle 24: SAF_RemoteControl_REC: Fernbedienungsschnittstelle

Kommandostrukur

Um ein Kommando an die SL zu senden, muss eine Kommandostruktur vorbereitet und mit Werten befüllt werden. Diese Struktur muss mittels eines POWERLINK Schreibbefehls auf das Objekt "RemoteRequest_OCT", der Fernbedienungsschnittstelle geschrieben werden.

Die Struktur darf keine Füllbytes enthalten und hat wie folgt auszusehen:

Element	Datentyp	Bemerkung
Command	UINT	Fernbedienungskommando, siehe Kommandos
Number	UINT	Laufende Nummer des Kommandos, vom Programmierer vorzugeben, kann in der Statusstruktur wieder rückgelesen werden
Data	UINT	Daten zum Kommando, siehe Kommandos
Password	USINT[16]	MD5-Hashcode des SafeKEY Passworts
NewPassword	USINT[16]	MD5-Hashcode des neuen SafeKEY Passworts

Tabelle 25: Kommandostrukur

Hinweis:

Der Eintrag "NewPassword" darf nur im Falle des Kommandos "PASSWORD_CHANGE" an die Struktur angehängt und mit übertragen werden.

Kommandos

Command	Bezeichnung	Data	Bemerkung
0x0100	ENTER	0x0020	Bestätigen von mehr als 4 UDID-Mismatches
		0x0030	Bestätigen von 4 UDID-Mismatches
		0x0040	Bestätigen von 3 UDID-Mismatches
		0x0050	Bestätigen von 2 UDID-Mismatches
		0x0060	Bestätigen von 1 UDID-Mismatch
		0x0100	FW-ACKN, Bestätigen einer neuen Firmwareversion
		0x0200	SK-XCHG, Bestätigen eines SafeKEY Tausches
		0x1000	TEST, Starten eines LED-Tests (5s)
		0x2000	SCAN, Start eines Systemscans
		0x3000	SK-COPY, SafeKEY kopieren
		0x4000	Kopieren nach Einstecken eines neuen SafeKEY fortsetzen
		0x5000	Passwort des SafeKEY ändern
		0x6000	SafeKEY formatieren
0x0200	STATUS_SL	0x0000	Status und Zustände der SL Abfragen

Tabelle 26: Kommandos

Hinweise:

- **Passwortschutz:**
  Kommandos werden nur exekutiert, wenn das Passwort korrekt ist, und die Fernbedienung aktiviert ist.

  Ausnahmen

  - Das Kommando STATUS_SL funktioniert auch ohne Passwort und ohne aktivierter Fernbedienung.
  - Beim Kommando "Passwort des SafeKEY ändern" wird das Passwort nicht kontrolliert, wenn keine gültigen Daten auf dem SafeKEY sind.
    Hinweis: dadurch ist es möglich, einen leeren/formatieren SafeKEY neu aufzusetzen.

- **Verriegelung:**
  Die manuelle Bedienung der SL mittels Wahlschalter und ENTER-Taste, und die Fernbedienung sind in der Firmware gegeneinander verriegelt.
  Wird ein manuelles Kommando abgearbeitet, kann kein weiteres per Fernbedienung abgesetzt werden, und umgekehrt.
  Anmerkung: der Befehl SK-COPY kann nach einem SafeKEY Tausch auch direkt an der SL erfolgen (SK-COPY durch Remote Control startet den Kopiervorgang, nach dem SafeKEY-Tausch kann dieser an der SL mittels SK-COPY bestätigt werden).
- Es kann immer nur EIN Kommando abgearbeitet werden. Solange ein Kommando läuft, werden alle neuen Kommandos abgewiesen.

- **Antwort:**
  Jedes Kommando erzeugt automatisch eine Antwort: Um den Zustand der ENTER-Kommandos zu eruieren, muss das Kommando STATUS_SL gesendet werden und die Statusstruktur ausgelesen werden.
- **Protokollierung:**
  Alle Kommandos außer STATUS_SL werden im Safety Log-Buch protokolliert, unabhängig davon, ob diese durchführbar waren oder nicht (z.B. abgewiesen weil keine Autorisierung).

- Die Kommandos "Bestätigen von x UDID-Mismatches" lösen nach deren Ausführung, genau wie bei manueller Bedienung, einen Modul-SCAN aus.
- Die Kommandos SK-XCHG, SK-COPY und FW-ACKN führen, genau wie bei manueller Bedienung, zu einem Neustart der SL.
  Hinweis: ab R1.5 wird der Neustart um 5s verzögert, damit die funktionale CPU die Befehlsantwort noch auswerten kann.
- Bei der Kombination von mehreren Kommandos wird der Modul-SCAN b.z.w. ein Neustart der SL erst nach Ausführung ALLER Kommandos ausgeführt.

Status auslesen

Nachdem der Status der SL, mittels des Kommandos "STATUS_SL", abgefragt wurde, werden die Werte im Objekt "RemoteResponse_OCT" abgelegt. Die Werte können mittels eines POWERLINK Lesebefehls ausgelsen und sind nach folgender Struktur aufgeschlüsselt.

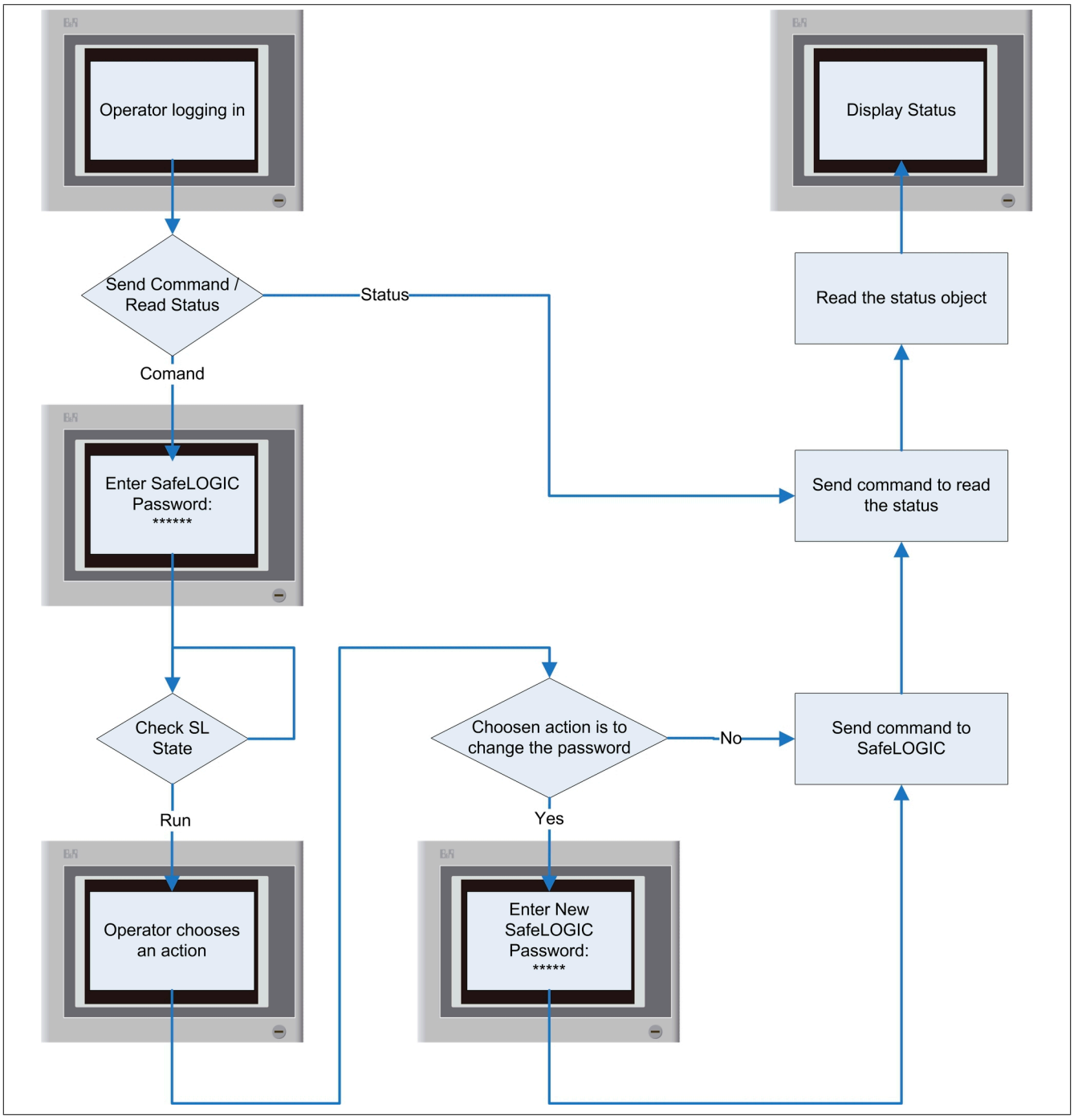
Element	Datentyp	Wert	Bemerkung
Command	UINT	-	Zuletzt empfangenes Kommando
Number	UINT	-	Laufende Nummer des zuletzt empfangenen Kommandos
Status	UINT	-	Die Status-Nummern entsprechen den ins Log-Buch eingetragenen Fehler-Nummern
		0	Das zuletzt empfangene Kommando war gültig und wird ausgeführt
		1	Reserviert: HMI Kommando wurde erfolgreich ausgeführt (Logger)
		2	Reserviert: HMI Kommando wurde fehlerhaft ausgeführt (Logger)
		3	Reserviert: Remote Kommando wurde erfolgreich ausgeführt (Logger)
		4	Reserviert: Remote Kommando wurde fehlerhaft ausgeführt (Logger)
		5	Das Kommando ist unbekannt
		6	Das ENTER-Kommando im Feld Data ist unbekannt
		7	Remote Control ist durch den SafeDESIGNER nicht aktiviert
		8	Falsches Passwort
		9	Remote Control State Machine ist nicht im IDLE (Abarbeitung des letzten Kommandos ist aktiv)
		10	Durch HMI gesperrt (Kommando wurde durch Drehschalter und ENTER-Button aktiviert)
		11	Keine Autorisierung für SK_ACKN Kommando
		12	Keine Autorisierung für FW_ACKN Kommando
		13	Keine Autorisierung für SMX_ACKN bis CMX_ACKN Kommando
		14	Kommando SK_ACKN nicht ausführbar, SafeKEY wurde nicht getauscht
		15	Kommando FW_ACKN nicht ausführbar, keine unterschiedliche Firmware gefunden
		16	Kommando SMX_ACKN nicht ausführbar, keines oder mehrer Module wurden getauscht
		17	Kommando DMX_ACKN nicht ausführbar, weniger oder mehr als zwei Module wurden getauscht
		18	Kommando TMX_ACKN nicht ausführbar, weniger oder mehr als drei Module wurden getauscht
		19	Kommando QMX_ACKN nicht ausfürhbar, weniger oder mehr als vier Module wurden getauscht
		20	Kommando CMX_ACKN nicht ausführbar, weniger oder mehr als fünf Module wurden getauscht
		21	Kommando SK_CONTINUE nicht ausführbar, SK_COPY nicht gestartet oder Zeit für SK_CONTINUE abgelaufen
		22	Kommando ENTER nicht möglich, SK_ACKN nötig
		23	Kommando SK_FORMAT wird abgearbeitet, kein weiteres Kommando absetzbar
		24	Kommando SK_COPY wird abgearbeitet, kein weiteres Kommando absetzbar
		25	Kommando SK_ACKN wird abgearbeitet, kein weiteres Kommando absetzbar
		26	Kommando SMX_ACKN bis CMX_ACKN wird abgearbeitet, kein weiteres Kommando absetzbar
		27	Ein SCAN wird durchgeführt, kein weiteres Kommando absetzbar
		28	Reserviert: Remote Status senden fehlgeschlagen (Logger)
		29	Falsche Länge des Kommandos 0x5000 (Passwort ändern)
		30	Falsche Länge des Kommandos (für Kommandos != 0x5000)
State	UINT	-	State des letzten ENTER Kommandos
		0	IDLE, warten auf nächstes Kommando
		1	ENTER Kommando empfangen
		2	ENTER Kommando ausführen

Tabelle 27: Statusstruktur

Element	Datentyp	Wert	Bemerkung
EnterData	UINT	-	Zuletzt empfangenes ENTER Kommando welches korrekt war und ausgeführt wurde
EnterNumber	UINT	-	Laufende Nummer des zuletzt empfangenen ENTER Kommandos
EnterExecuteStatus	UINT	-	Status des zuletzt empfangenen ENTER Kommandos, selber Wert wie usEnterData, gültiger Wert wenn eState = IDLE
		0x0000	Status zu Beginn der Ausführung, wenn State != IDLE
			Status nach fehlerhafter Ausführung, wenn State = IDLE
SafeOSstate	USINT	-	Status der Sicherheitsapplikation
SafeKeyChanged	USINT	0x01	SafeKEY wurde getauscht, Bestätigung erforderlich
LedTestActive	USINT	0x01	Led-Test aktiv
Scanning	USINT	0x01	Modul-Scan aktiv
openSAFETYstate	USINT	-	Status openSAFETY Stack
FailSafe	USINT	0x55	Modulstatus OK - Status der sicheren Applikation: siehe SafeOSstate
		alle anderen Werte	Modulstatus Fail-Safe - es werden keine gültigen sicheren Daten mehr generiert (**unabhängig von allen anderen Stati**)
NumberOfMissingModules	UINT	0 - n	Anzahl fehlender Module
NumberOfUdidMismatches	UINT	0 - n	Anzahl der getauschten Module
NumberOfDiffFirmware	UINT	0 - n	Anzahl der Module mit geänderter Firmware
SAddr[0..100]	UINT	0 - 1023	Für jeden SN wird die Safety Adresse in dieses Feld eingetragen, 0 = Modul nicht vorhanden
MissingModules[0..15]	USINT	0x00 - 0xFF	Je 128 Bit für die Anzeige fehlender und getauschter Module, und Module mit geänderter Firmware Die Safety Adresse wird im Feld ausSAddr[0..100] eingetragen, dazugehörig werden in diesen Feldern bitweise die jeweiligen Stati eingetragen. Bsp.: Die Safety Adresse des 9. Moduls wird in ausSAddr[8] eingetragen, fehlt dieses Modul wird das 1. Bit in ausMissingModules[1] gesetzt
UdidMismatches[0..15]	USINT	0x00 - 0xFF	
DiffFirmware[0..15]	USINT	0x00 - 0xFF	

Tabelle 27: Statusstruktur

Ablauf der Fernbedienung



8.2 Maschinenoptionsdownload

Voraussetzungen

Parameterumfeld	Parameter	Wert
Automation Studio: Properties Dialog "Change Runtime Versions"	Safety Release	>= 1.4
SafeDESIGNER: Parameter der Gruppe Basic der SafeLOGIC	ExternalMachineOptions	JA-Achtung
SafeDESIGNER: Parameter der Gruppe Basic der SafeLOGIC	ExternalStartupFlags	JA-Achtung

Gefahr!

- **Der Anwender muss in einer FMEA die Anwendung der Funktion und mögliche Risiken untersuchen. In der FMEA sind vor allem auch mögliche vorhersehbare Fehlanwendungen und typische anwendungsspezifische Fehlerquellen zu berücksichtigen. Mögliche Risiken sind durch zusätzliche Maßnahmen zu minimieren. Erst wenn das ermittelte Restrisiko für die vorgesehene Anwendung als gering genug eingeschätzt wird, darf diese Funktion im SafeDESIGNER freigeschaltet und genutzt werden.**
- **Die an der Ausführung der Funktion beteiligten Programmteile in der funktionalen Applikation müssen den Anforderungen der ISO 13849-1:2007, Kapitel 4.6.4 bzw. IEC 62061, Kapitel 6.11.2 entsprechen. Die korrekte Ausführung der Programmteile gemäß einer dieser Normen ist zu dokumentieren.**
- **Die Funktionen dürfen ausschließlich von hierzu autorisierten Personen ausgeführt werden. Der Zugriff auf die entsprechenden Visualisierungsteile ist mit geeigneten Mitteln abzusichern und auf den autorisierten Personenkreis einzuschränken.**
- **Bei einem Zugriff muss das lokale Personal über den Zugriff informiert werden. Der Anwender muss durch geeignete Maßnahmen sicherstellen, dass Fernzugriffe ohne Wissen des lokalen Personals nicht möglich sind.**
- **Die für die Maschinenoptionen genutzten Informationen dürfen in der funktionalen Applikation nicht verändert, invertiert oder in einer anderen Form manipuliert werden. Anforderungen dieser Art (z.B. aus der Aktivierung des Maschinentypes A resultiert das Aktivieren der Maschinenoptionen 1, 2 und 3) sind in der sicheren Applikation im SafeDESIGNER zu implementieren und nicht in der funktionalen Applikation.**
- **Die an der Bestätigung der rückgelesenen Konfiguration beteiligten Programmteile sind diversitär zu jenen Programmteilen auszuführen, welche die Konfiguration an die SafeLOGIC übertragen. Die verwendeten Visualisierungsobjete müssen so gestaltet werden, dass für die Darstellung der Daten am Bidlschirm unterschiedliche Pixel Positionen verwendet werden.**
- **Die korrekte Funktion muss in einem vollständigen Funktionstest nachgewiesen werden. Die Durchführung der Tests und die Testergebnisse sind zu dokumentieren. Der Test muss so gestaltet werden, dass mögliche Datenvertauschungen zwischen der Visualisierung und der Sicherheitsapplikation aufgedeckt werden. Die korrekte Funktion muss nach Änderungen am Automation Runtime oder nach Änderungen der Funktionalen Applikation in einem vollständigen Funktionstest erneut nachgewiesen werden. Gefahren auflisten!**

Allgemeines

Ab dem Safety Release 1.4 können Maschinenkonfigurationen von der funktionalen Applikation übernommen werden. Zu diesem Zwecke wurde auf der SafeLOGIC eine POWERLINK Objektschnittstelle implementiert, welche im Automation Studio mit Hilfe der Bibliothek "AsEPL" bedient werden kann.

Mit dieser Schnittstelle können Signale für externe Maschinenoptionen, das Startup Verhalten der Module und UDIDs der Module vorgegeben werden. Wird eine solche Struktur auf die SL übertragen, werden die darin vorgenommenen Einstellungen nach einem Neustart übernommen.

Die Einstellungen können über die Visualisierung erfolgen. Der Maschinenbediener kann in der Visualisierung Parameter verändern und muss nach einem erfolgreichen Download alle getätigten Einstellung kontrollieren und bestätigen.

Schnittstelle

POWERLINK V2 Objekte:

Index:Subinde	Objektbezeichnung	Datentyp	Zugriff	Werte	Beschreibung
0x2405:0x00	NumberOfEntries	USINT	R	0x08	Anzahl der Einträge auf diesem Index
0x2405:0x01	Authorization_DOM	USINT[16]	W	-	Autorisierung der Datenübertragung mittels Schreiben des MD5 Hashcode des SafeKEY Passwortes auf dieses Objekt
0x2405:0x02	FileStreamData_DOM	-	W	-	Daten zur Übertragung auf die SL werden auf dieses Ojekt geschrieben
0x2405:0x03	ParserStatus_U16	UINT	R	0	Kein Fehler bei der Datenübertragung
				1	Falsche Protokollversion oder Fehler im Header
				2	Datei ist bereits geöffnet
				3	Datei ist ungültig
				4	Datei ist zu groß
				5	Fehler während des Schreibens
				6	Fehler am Ende des Streams
				7	Prüfsumme nicht korrekt
				8	Falsche UDID
				9	Falsche Dateigröße
				10	Keine Berechtigung zum Schreiben
0x2405:0x04	UnlockStatus_U16	UINT	R	0	Kein Fehler aufgetreten
				1	Fehler beim Beziehen der Dateiinfomation
				2	Fehler beim Lesen
				3	Fehler beim Schreiben
0x2405:0x05	Busy_BOOL	BOOL	R	FALSE	Datenübertragung, oder Verriegelung im Idle
				TRUE	Datenübertragung, oder Verriegelung busy
0x2405:0x06	Reboot_DOM	USINT[16]	W	-	Neustart der SL mittels Schreiben des MD5 Hashcodes des Passwortes auf dieses Objekt
0x2405:0x07	ProjectKey_U64	LREAL	W	-	Freigeben der Appliktion mittels Schreiben des Entsperrschlüssels auf dieses Objekt
0x2405:0x08	AutoCnfKey_U64	LREAL	W	-	Freigeben der Maschinenoptionen mittels Schreiben des Entsperrschlüssels auf dieses Objekt
0x2405:0x09	ProjectID_U32	UDINT	R	-	Projekt-CRC des SafeDESIGNER-Projektes
0x2405:0x0A	AutoCnfID_U32	UDINT	R	-	Wert "Zeitstempel der Datei" - siehe "Format"

Tabelle 28: SAF_FileParser_REC: Dateischnittstelle

Format

Um diese Einstellungen extern vorzugeben, muss eine Datei erstellt werden die diese Informationen beinhaltet. Diese Datei kann entweder auf einem PC vorbereitet werden und in der funktionalen Steuerung abgelegt werden, oder erst während dem laufenden Betrieb in der funktionalen Steuerung erstellt werden. Dies kann über die Visualisierung erfolgen. Der Maschinenbediener welcher diese Datei über die Visualisierung auswählt oder erstellt, muss nach einem erfolgreichen Download alle getätigten Einstellung kontrollieren und bestätigen.

Abschnitt	Bezeichnung	Offset innerhalb der Sektion	Byte	Bedeutung
Header	Anzahl	0	2	Anzahl der beschriebenen Sektionen, typisch 3
	Länge	2	2	Länge des Headers, typisch 64
	Version	4	2	Versionsnummer für das Format des Headers (Standard 0x0400)
	Offset	6	2	Position der Beschreibung der 1. Sektion, typisch 8
	Zeitstempel der Datei	8	4	Einzigartiger Zeitstempel zur eindeutigen Identifizierung der Datei
	Länge Sektion 1	12	4	Länge der 1. Sektion, abhängig von der Anzahl getauschter Module
	Offset Sektion 1	16	4	Absolute Position der 1. Sektion, typisch 64
	Länge Sektion 2	20	4	Länge der 2. Sektion, typisch 76
	Offset Sektion 2	24	4	Absolute Position der 2. Sektion, abhängig von der Länge der 1. Sektion
	Länge Sektion 3	28	4	Länge der 3. Sektion, typisch 268
	Offset Sektion 3	32	4	Absolute Position der 3. Sektion, abhängig von der Länge der 1. und 2. Sektion
	Reserve	36	24	Reserve
	CRC32	60	4	CRC32 des Headers, Anzahl bis Reserve[1)]
UDID Liste (Sektion 1)	Anzahl	0	2	Anzahl der getauschten Module (<=101)
	Länge	2	2	Länge eines Eintrags, typisch 8
	Version	4	2	Versionsnummer für das Format der 1. Sektion, typisch 0x0300
	Offset	6	2	Sektionsoffset des ersten Eintrags, typisch 8
	SADR des 1. Safety Nodes	8	2	Safety Adresse des 1. Moduls
	UDID des 1. Safety Nodes	10	2	UDID des 1. Moduls
	...			
	SADR des n. Safety Nodes	8 + (n-1)*8	2	Safety Adresse des n. Moduls
	UDID des n. Safety Nodes	10 + (n-1)*8	6	UDID des n. Moduls
	CRC32	8 + n*8	4	CRC32 über die 1. Sektion, Anzahl bis letzte UDID[1)]
Maschinenoptionen (Sektion 2)	Anzahl	0	2	Anzahl der Maschinenoptionen, typisch 512
	Länge	2	2	Länge der Daten, typisch 64
	Version	4	2	Versionsnummer für das Format der Maschinenoptionen, typisch 0x0100
	Offset	6	2	Offset der Daten, typisch 8
	Daten	8	64	512 Bit Maschinenoptionen
	CRC32	72	4	CRC32 über die 2. Sektion, Anzahl bis Daten[1)]
Modul-Flags (Sektion 3)	Anzahl	0	2	Anzahl der Modul-Flags
	Länge	2	2	Länge der Daten
	Version	4	2	Versionsnummer für das Format der Modul-Flags, typisch 0x0100
	Offset	6	2	Offset der Modul-Flags, typisch 8
	Optional-Flags	8	128	1024 Bit für Optional
	Startup-Flags	136	128	1024 Bit für Startup
	CRC32	264	4	CRC32 über die 3. Sektion, Azahl bis Startup-Flags[1)]
Gesamt-CRC	CRC32	0	4	CRC32 über die gesamte Datei[1)]

1) CRC32 Berechnung, Polynom 0x1edc6f41, Startwert 0

UDID-Liste

In der UDID-Liste kann der SL vorgegeben werden an welcher Safety Adresse welche UDID beim Hochlauf gefunden werden soll. Stimmt diese extern vorgegebene UDID mit der physikalischen Konfiguration überein, ist eine Quittierung eines getauschten oder neu hinzugefügten Moduls nicht mehr erforderlich, da die UDID der SL schon bekannt ist. Die UDID eines Moduls kann im Automation Studio über das IO-Mapping ausgelesen werden.

Externe Maschinenoptionen

Die externen Maschinenoptionen bieten 512 im sicheren Code verwendbare, Variablen. Diesen Variablen kann in der Maschinenoptionsdatei ein Wert, TRUE oder FALSE, zugewiesen werden. Nachdem diese Datei auf die SL übertragen und ein Neustart durchgeführt wurde, werden die Variablen mit dem vorgegebenen Wert initialisiert. Die externen Maschinenoptionen verhalten sich wie Konstanten.

Modul Flags

Für jedes Modul kann im SafeDESIGNER eingestellt werden wie sich die sichere Applikation verhällt, wenn das Modul nicht mehr gefunden werden kann. Diese Einstellung kann auch extern über die "Maschinenoptionsdatei" vorgegeben werden. Hierbei kann für jede Safety Adresse einzeln eingestellt werden, ob der "Optional-Parameter" des zugehörigen Moduls auf "optional", "Startup" oder "No" konfiguriert werden soll.

Struktur

Die Maschinenoptionsstruktur muss vor dem Download in eine übergeordnete Struktur eingehängt werden.

Abschnitt	Bezeichnung	Datentyp	Bedeutung
Header	Version	UINT	Version des File-Containers, es muss der Wert 0x0100 eingetragen werden
	Anzahl	UINT	Anzahl der folgenden Dateien, es muss der Wert 0x0001 eingetragen werden, eine Datei soll übertragen werden, die Maschinenoptionsstruktur
	UDID	USINT[6]	UDID der SL auf welche die Struktur übertragen wird
Maschinenoptionsstruktur	Dateilänge	UDINT	Dateilänge der Maschinenoptionsstruktur
	Dateiname	USINT[13]	Name der Maschinenoptionsstruktur, hier muss "AUTOCNF.BIN" eingetragen werden
	Datei	-	Maschinenoptionsstruktur
Checksum	Prüfsumme	UDINT	Additive Prüfsumme über die gesamte Struktur

Tabelle 29: Downloadstruktur

Ablauf Maschinenoptionsdownload

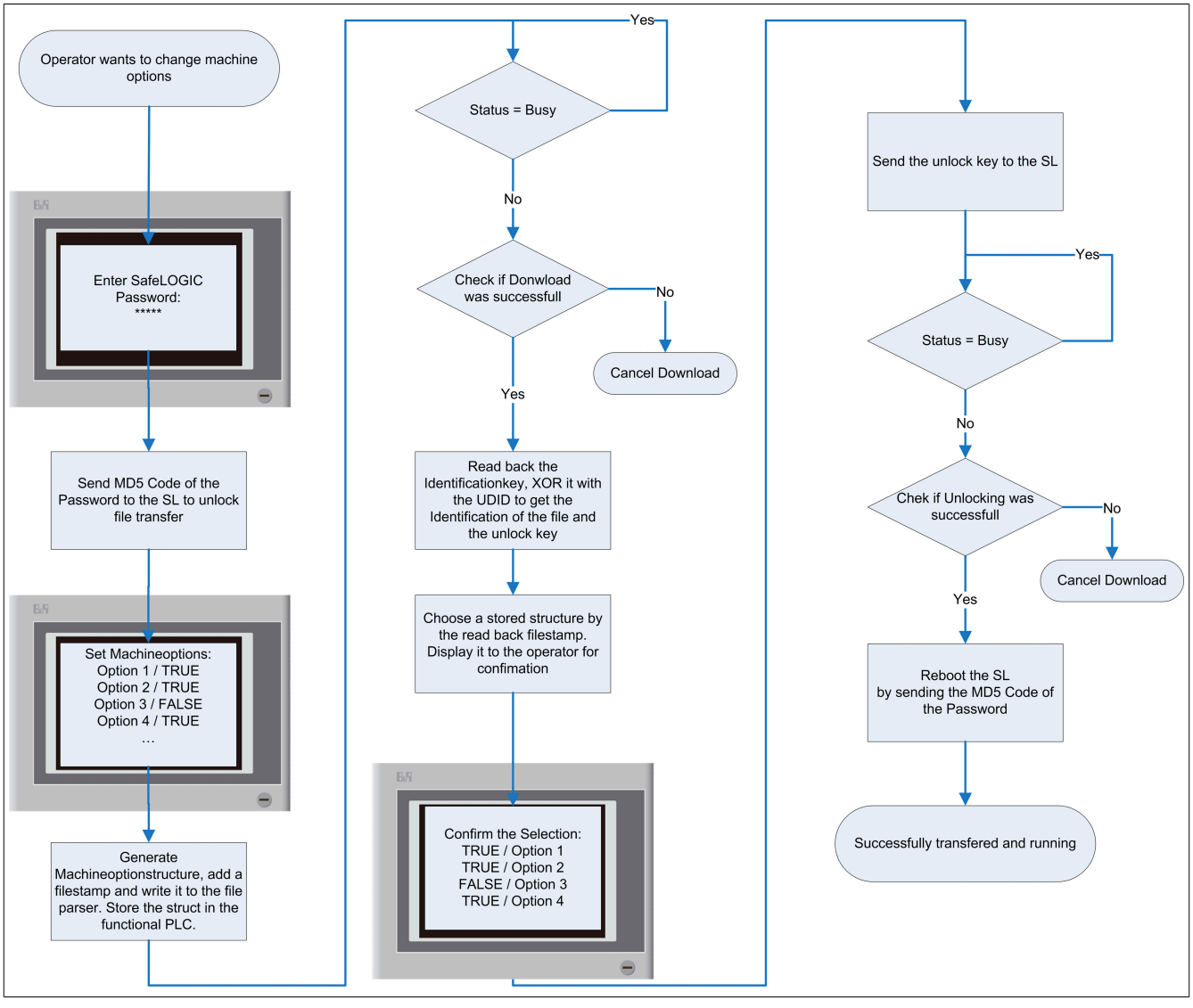


Abbildung 10: Ablaufdiagramm Maschinenoptionsdownload

Um Maschinenoptionen von der funktionalen Steuerung aus auf die SL zu übertragen ist ein vorgegebenes Schema einzuhalten. Es ist unbedingt notwendig dass der Downloadvorgang vom Maschinenbediener manuell und bewusst initiiert wird. Nach erfolgter Übertragung der Daten müssen diese verifiziert werden. Hierzu müssen dem Bediener nach dem Donwload alle getätigten Änderungen und Einstellung angezeigt werden. Die eingestellten Parameter müssen vom Bediener bestätigt werden.

Um einen Downloadvorgang erfolgreich durchzuführen müssen nun folgende Schritte eingehalten werden:

- Freischalten des Downloads durch das Schreiben des MD5 Hash-Codes des SafeKEY Passwortes auf das Objekt "Authorization_DOM".
- Senden der Donwloadstruktur indem diese auf das Objekt "FileStreamData_DOM" geschrieben wird.
- Ermittlen ob die Übertragung abgeschlossen ist, indem das Objekt "Busy_BOOL" ausgelesen wird.
- Abfragen ob die Daten vollständig empfangen wurden indem das Objekt "ParserStatus_U16" ausgelesen wird.
- Auslesen des Identifikations-/Schlüsselobjektes. Hierzu muss das Objekt "AutoCnfKey_U64" ausgelesen werden. Dieses Objekt muss byteweise mit der UDID der SL verknüpft werden. Dadurch erhält man die Identifikation der übertragenen Datei, und den zugehörigen Entsperrschlüssel.

Die UDID muss nach folgendem Schema mit dem Identifikations-/Schlüsselobjekt XOR verknüpft werden.

FileIdent[0] = EPLKey[0];

FileIdent[1] = EPLKey[1];

FileIdent[2] = EPLKey[2] ^ SL_UDID[0];

FileIdent[3] = EPLKey[3] ^ SL_UDID[1];

UnlockKey[0] = EPLKey[4] ^ SL_UDID[2];

UnlockKey[1] = EPLKey[5] ^ SL_UDID[3];

UnlockKey[2] = EPLKey[6] ^ SL_UDID[4];

UnlockKey[4] = EPLKey[7] ^ SL_UDID[5];

Ergebnis der Verknüpfung:

Byte	Bedeutung
0	Identifikation, entspricht dem Wert des Elements "Zeitstempel der Datei" in der Maschinenoptionsstruktur. Mittels dieses Wertes muss dem Bediener die zugehörige Maschinenoptionsstruktur angezeigt werden.
1	
2	
3	
4	Entsperrschlüssel für die Maschinenoptionsstruktur
5	
6	
7	

Tabelle 30: Ergebnis UDID XOR-Verknüpfung

- Schreiben des Entsperrschlüssels auf das Objekt "AutoCnfKey_U64". Hierbei muss der Entsperrschlüssel in die ersten 4 Byte geschrieben werden.
- Ermittlen ob die Enstschlüsselung abgeschlossen ist, indem das Objekt "Busy_BOOL" ausgelesen wird.
- Abfragen ob bei der Entschlüsselung der Daten auf der SL ein Fehler aufgetreten ist, hierzu muss das Objekt "UnlockStatus_U16" ausgelesen werden.
- Neustart der SL initiieren indem der MD5 Hash-Code des SafeKEY Passwortes auf das Objekt "Reboot_DOM" geschrieben wird.

8.3 Applikationsdownload

Voraussetzungen

Parameterumfeld	Parameter	Wert
Automation Studio: Properties Dialog "Change Runtime Versions"	Safety Release	>= 1.4

Gefahr!

- **Der Anwender muss in einer FMEA die Anwendung der Funktion und mögliche Risiken untersuchen. In der FMEA sind vor allem auch mögliche vorhersehbare Fehlanwendungen und typische anwendungsspezifische Fehlerquellen zu berücksichtigen. Mögliche Risiken sind durch zusätzliche Maßnahmen zu minimieren. Erst wenn das ermittelte Restrisiko für die vorgesehene Anwendung als gering genug eingeschätzt wird, darf diese Funktion im SafeDESIGNER freigeschaltet und genutzt werden.**
- **Die an der Ausführung der Funktion beteiligten Programmteile in der funktionalen Applikation müssen den Anforderungen der ISO 13849-1:2007, Kapitel 4.6.4 bzw. IEC 62061, Kapitel 6.11.2 entsprechen. Die korrekte Ausführung der Programmteile gemäß einer dieser Normen ist zu dokumentieren.**
- **Die Funktionen dürfen ausschließlich von hierzu autorisierten Personen ausgeführt werden. Der Zugriff auf die entsprechenden Visualisierungsteile ist mit geeigneten Mitteln abzusichern und auf den autorisierten Personenkreis einzuschränken.**
- **Bei einem Zugriff muss das lokale Personal über den Zugriff informiert werden. Der Anwender muss durch geeignete Maßnahmen sicherstellen, dass Fernzugriffe ohne Wissen des lokalen Personals nicht möglich sind.**
- **Die an der Bestätigung der rückgelesenen Konfiguration beteiligten Programmteile sind diversitär zu jenen Programmteilen auszuführen, welche die Konfiguration an die SafeLOGIC übertragen. Die verwendeten Visualisierungsobjete müssen so gestaltet werden, dass für die Darstellung der Daten am Bidlschirm unterschiedliche Pixel Positionen verwendet werden.**
- **Die korrekte Funktion muss in einem vollständigen Funktionstest nachgewiesen werden. Die Durchführung der Tests und die Testergebnisse sind zu dokumentieren. Der Test muss so gestaltet werden, dass mögliche Datenvertauschungen zwischen der Visualisierung und der Sicherheitsapplikation aufgedeckt werden. Die korrekte Funktion muss nach Änderungen am Automation Runtime oder nach Änderungen der Funktionalen Applikation in einem vollständigen Funktionstest erneut nachgewiesen werden. Gefahren auflisten! Gefahren auflisten**

Allgemeines

Ab dem Safety Release 1.4 kann die sicherheitstechnische Applikation von der funktionalen Applikation auf den SafeKEY der SafeLOGIC übertragen werden. Zu diesem Zwecke wurde auf der SafeLOGIC eine POWERLINK Objektschnittstelle implementiert, welche im Automation Studio mit Hilfe der Bibliothek "AsEPL" bedient werden kann.

Mit dieser Schnittstlle kann ein Container File mit einer vordefinierten Struktur auf die SafeLOGIC übertragen werden. Wird eine solche Struktur auf die SL übertragen, wird die darin enthaltene Applikation nach einem Neustart übernommen.

Information:

Um einen leeren SafeKEY (z.B.: neu oder formatiert) aufzusetzen, muss man zuerst ein Passwort setzen (siehe Kommando "Passwort des SafeKEY ändern" in Abschnitt "Kommando").

Dateischnittstelle

POWERLINK V2 Objekte:

Index:Subinde	Objektbezeichnung	Datentyp	Zugriff	Werte	Beschreibung
0x2405:0x00	NumberOfEntries	USINT	R	0x08	Anzahl der Einträge auf diesem Index
0x2405:0x01	Authorization_DOM	USINT[16]	W	-	Autorisierung der Datenübertragung mittels Schreiben des MD5 Hashcode des SafeKEY Passwortes auf dieses Objekt
0x2405:0x02	FileStreamData_DOM	-	W	-	Daten zur Übertragung auf die SL werden auf dieses Ojekt geschrieben
0x2405:0x03	ParserStatus_U16	UINT	R	0	Kein Fehler bei der Datenübertragung
				1	Falsche Protokollversion oder Fehler im Header
				2	Datei ist bereits geöffnet
				3	Datei ist ungültig
				4	Datei ist zu groß
				5	Fehler während des Schreibens
				6	Fehler am Ende des Streams
				7	Prüfsumme nicht korrekt
				8	Falsche UDID
				9	Falsche Dateigröße
				10	Keine Berechtigung zum Schreiben
0x2405:0x04	UnlockStatus_U16	UINT	R	0	Kein Fehler aufgetreten
				1	Fehler beim Beziehen der Dateiinfomation
				2	Fehler beim Lesen
				3	Fehler beim Schreiben
0x2405:0x05	Busy_BOOL	BOOL	R	FALSE	Datenübertragung, oder Verriegelung im Idle
				TRUE	Datenübertragung, oder Verriegelung busy
0x2405:0x06	Reboot_DOM	USINT[16]	W	-	Neustart der SL mittels Schreiben des MD5 Hashcodes des Passwortes auf dieses Objekt
0x2405:0x07	ProjectKey_U64	LREAL	W	-	Freigeben der Appliktion mittels Schreiben des Entsperrschlüssels auf dieses Objekt
0x2405:0x08	AutoCnfKey_U64	LREAL	W	-	Freigeben der Maschinenoptionen mittels Schreiben des Entsperrschlüssels auf dieses Objekt
0x2405:0x09	ProjectID_U32	UDINT	R	-	Projekt-CRC des SafeDESIGNER-Projektes
0x2405:0x0A	AutoCnfID_U32	UDINT	R	-	Wert "Zeitstempel der Datei" - siehe "Format"

Tabelle 31: SAF_FileParser_REC: Dateischnittstelle

Downloadstruktur

In der Downloaddatei müssen alle Dateien zusammengefasst werden, welche an die SL übertragen werden sollen. Eine sichere Applikation wird nach dem Kompilieren im SafeDESIGNER, im Projektverzeichnis abgelegt. Im Ordner "*AS-PROJEKTPFAD*\Physical*NAME_AS-KONFIGURATION*\PLC1*NAME_SD-PROJEKT*\DLFiles" werden zehn Dateien abgelegt. Diese Dateien müssen in die Downloadstruktur eingehängt werden.

Alle Dateien, die an die SL übertragen werden, müssen im Little Endian Format erstellt werden.

Dateiformat:

Abschnitt	Bezeichnung	Datentyp	Bedeutung
Header	Version	UINT	Version des File-Containers, hier muss der Wert 0x0100 eingetragen werden
	Anzahl	UINT	Anzahl der folgenden Dateien, eine Applikation besteht aus zehn Dateien, es muss der Wert 0x000A eingetragen werden
	UDID	USINT[6]	UDID der SL auf welche die Datei übertragen wird
Datei 1	Dateilänge	UDINT	Dateilänge der 1. Datei
	Dateiname	USINT[13]	Name der 1. Datei ("BUR_PARA.SAF"; siehe Abschnitt Applikationsdateien)
	Dateiinhalt	-	Daten der 1. Datei aus dem Ordner DLFiles ("dlfile01.sos"; siehe Abschnitt Applikationsdateien)
...			
Datei 10	Dateilänge	UDINT	Dateilänge der 10. Datei
	Dateiname	USINT[13]	Name der 10. Datei
	Dateiinhalt	-	Daten der 10. Datei
Checksum	CRC32	UDINT	Additive Prüfsumme über die gesamte Downloaddatei[1)]

Tabelle 32: Downloaddatei

1) CRC32 Berechnung, Polynom 0x1edc6f41, Startwert 0

Applikationsdateien

In die Downloaddatei müssen vordefinierte Namen für die Dateien "dlfile01.sos" bis "dlfile10.sos" vergeben werden, damit diese von der SL identifieziert werden können. In folgender Tabelle sind diese Namen aufgelistet.

Dateiname im Projektverzeichnis	Name in der Downloaddatei
dlfile01.sos	BuR_Para.saf
dlfile02.sos	CFooLibs.dll
dlfile03.sos	impldiag.zip
dlfile04.sos	sdevpara.saf
dlfile05.sos	Bootfile.pro
dlfile06.sos	ProjCRC.img
dlfile07.sos	SwapList.pr2
dlfile08.sos	Bootfile.pr2
dlfile09.sos	BusNvCRC.img
dlfile10.sos	SysFlags.dat

Tabelle 33: Dateinamen - Applikationsdownload

Downloadablauf

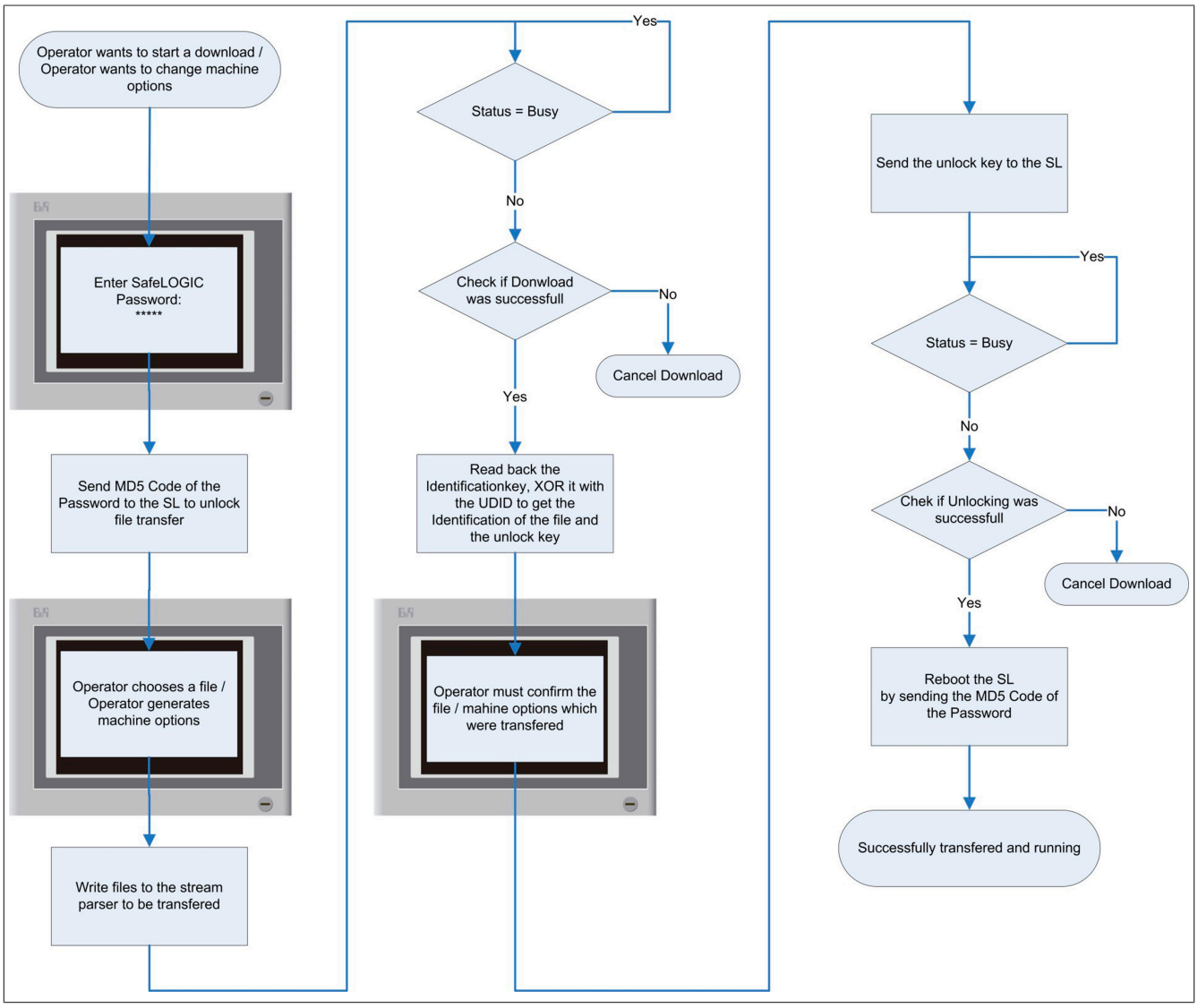


Abbildung 11: Ablaufdiagramm Dateidownload

Information:

- **Dem Bediener muss im Falle eines Applikationsdownloads die CRC vor der Übertragung bekannt sein. Mittels des Rückgabewertes welcher die CRC beinhaltet, muss dem Bediener angezeigt werden welche Datei übertragen wurde. Der Bediener muss bestätigen, dass die von ihm gewünschte Datei übertragen wurde.**
- **Im Falle einer Maschinenoptionsdatei muss diese nach dem Download mittels des Zeitstempels identifiziert werden. Dem Bediener müssen alle Einstellungen die in dieser Datei konfiguriert wurden in der Visualisierung angezeigt werden. Der Bediener muss bestätigen, dass die Einstellungen, den von ihm gewünschten entsprechen, und dies bestätigen.**
- **Erst nachdem der Bediener die gesendete Datei bestätigt hat, darf der Entsperrschlüssel auf die SL übertragen werden.**

Um eine sichere Applikation von der funktionalen Steuerung aus auf die SL zu übertragen ist ein vorgegebenes Schema einzuhalten. Es ist unbedingt notwendig dass der Downloadvorgang vom Maschinenbediener manuell und bewusst initiiert wird. Nach erfolgter Übertragung der Daten muss überprüft werden ob diese auch richtig auf der SL angekommen sind. Dem Bediener muss die Prüfsumme angezeigt werden. Die Prüfsumme muss vom Bediener bestätigt werden. Danach muss die SL neu gestartet werden um die übertragene sichere Applikation zu starten.

Um einen Downloadvorgang erfolgreich durchzuführen müssen nun folgende Schritte eingehalten werden:

- Freischalten des Downloads durch das Schreiben des MD5 Hash-Codes des SafeKEY Passwortes auf das Objekt "Authorization_DOM".
- Senden der Downloaddatei indem diese auf das Objekt "FileStreamData_DOM" geschrieben wird.
- Ermittlen ob die Übertragung abgeschlossen ist, indem das Objekt "Busy_BOOL" ausgelesen wird.
- Abfragen ob die Daten vollständig empfangen wurden indem das Objekt "ParserStatus_U16" ausgelesen wird.
- Auslesen des Identifikations-/Schlüsselobjektes. Das Objekt "ProjectKey_U64", muss hierzu ausgelesen werden. Dieses Objekt muss byteweise mit der UDID der SL verknüpft werden. Dadurch erhält man die Identifikation der übertragenen Datei, und den zugehörigen Entsperrschlüssel.

Die UDID muss nach folgendem Schema mit dem Identifikations-/Schlüsselobjekt XOR verknüpft werden.

FileIdent[0] = EPLKey[0];

FileIdent[1] = EPLKey[1];

FileIdent[2] = EPLKey[2] ^ SL_UDID[0];

FileIdent[3] = EPLKey[3] ^ SL_UDID[1];

UnlockKey[0] = EPLKey[4] ^ SL_UDID[2];

UnlockKey[1] = EPLKey[5] ^ SL_UDID[3];

UnlockKey[2] = EPLKey[6] ^ SL_UDID[4];

UnlockKey[4] = EPLKey[7] ^ SL_UDID[5];

Ergebnis der Verknüpfung:

Byte	Bedeutung
0	Identifikation, Im Falle eines Applikationsdownloads die CRC der Applikation wie im SafeDESIGNER angezeigt, im Falle einer Maschinenoptionsdatei, der Wert des Elements "Zeitstempel der Datei". Mittels dieses Wertes muss dem Bediener angezeigt werden welche Datei übertragen wurde.
1	
2	
3	
4	Entsperrschlüssel für die Applikation/Maschinenoptionsdatei
5	
6	
7	

Tabelle 34: Ergebnis UDID Identifikations-/Schlüsselobjekt XOR-Verknüpfung

- Schreiben des Entsperrschlüssels auf das Objekt "ProjectKey_U64". Hierbei muss der Entsperrschlüssel in die ersten 4 Byte geschrieben werden.
- Ermittlen ob die Enstschlüsselung abgeschlossen ist, indem das Objekt "Busy_BOOL" ausgelesen wird.

- Abfragen ob bei der Entschlüsselung der Daten auf der SL ein Fehler aufgetreten ist, hierzu wird das Objekt "UnlockStatus_U16" gelesen.
- Neustart der SL initiieren indem der MD5 Hash-Code des SafeKEY Passwortes auf das Objekt "Reboot_DOM" geschrieben wird.

8.4 Erweiterte Statusdaten

Folgende Statusdaten können über POWERLINK ausgelesen werden:

Index:Subindex	Objektbezeichnung	Datentyp	Zugriff	Werte	Beschreibung
0x2000:0x08	Project_CRC	UDINT	R	-	CRC des SafeDESIGNER Projektes
0x2000:0x09	Project_Time	DATE_AND_TIME	R	-	Zeitstempel
0x2000:0x0C	Project_Name	STRING (ohne Nullterminierung)	R	-	Projektname
0x2000:0x0D	Project_Author	STRING (ohne Nullterminierung)	R	-	Name des Autors
0x2000:0x0E	SafeOS_RUN_STATE	BOOL	R	0	SafeOS ist nicht in RUN (ident zu SafeOSstate!=0x66)
				1	SafeOS ist in RUN (ident zu SafeOSstate==0x66)
0x2000:0x0F	BOOT_STATE	UDINT	R	Allgemeiner Hochlauf-Status der Firmware	
				0x00	Hochlauf noch nicht begonnen
				0x01	Initialisierung gestartet
				0x10	zyklische Hardwaretests laufen
				0x11	openSAFETY-Stack läuft
				0x12	SafeOS läuft
0x2000:0x10	openSAFETYstate	UDINT	R	0	Preoperational State (alle zyklischen sicheren Daten werden genullt)
				1	Operational State
0x2000:0x11	SafeOSstate	UDINT	R	Status der Sicherheitsapplikation (entspricht der R/E-LED der SafeLOGIC).	
				0x00	ungültig (z.B.: SafeKEY leer) oder Hochlauf noch aktiv (BOOT_STATE!=0x12)
				0x0F	ON (Hochlauf / interne Initialisierung) oder Fehler (Logbuch kontrollieren)
				0x33	Loading (Hochlauf / interne Initialisierung)
				0x55	Stop [Safe]
				0x66	Run [Safe]
				0x99	Halt [Debug]
				0xAA	Stop [Debug]
				0xCC	Run [Debug]
				0xF0	No Execution

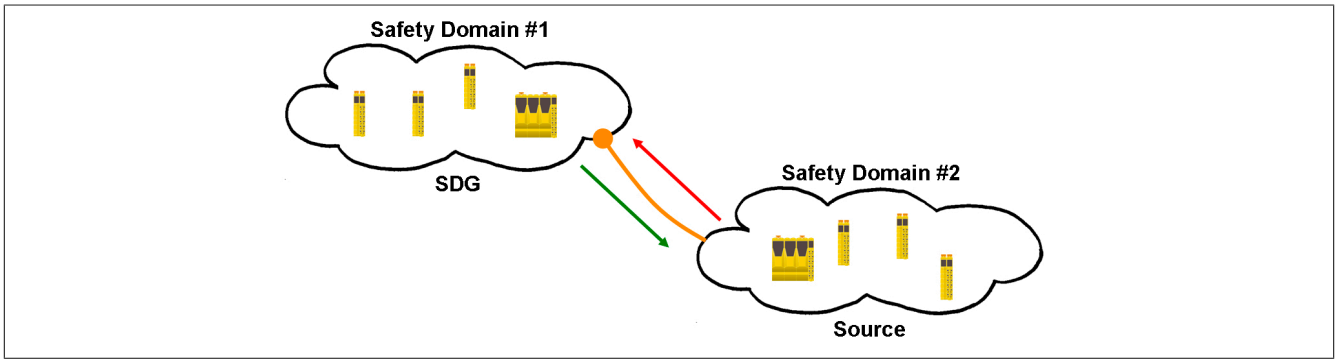
Tabelle 35: Systemstatusdaten

Index:Subindex	Objektbezeichnung	Datentyp	Zugriff	Werte	Beschreibung
0x2001:0x05	openSAFETY_Instance	USINT	RW	-	Nummer der openSAFETY-Instanz, von der man einen Statistikzähler auslesen will.
				0	Safe I/O-Module
				1-10	SDG-Verbindungen zu anderen SafeLOGICen (siehe "Tab. 13: Parameter I/O Konfiguration: POWERLINK parameters" auf Seite 10)
0x2001:0x06	Module_Index	USINT	RW	-	Index des Modules, dessen Statistikzähler man auslesen will.
				0-255	Safe I/O-Module - diese werden, bei 0 beginnend, lückenlos aufgelistet (sortiert nach aufsteigender SafeMODULE ID)
				0	für die SDG-Verbindung zu einer anderen SafeLOGIC
0x2001:0x07	Statistics_Counter	UDINT	R	-	Statistikzähler für das mit den Subindizes 05 und 06 definierte Modul. Der Statistikzähler inkrementiert bei jedem Abbruch der sicheren zyklischen Datenverbindung. **Hinweise** • Der Wert steht erst zur Verfügung, nachdem die Subindizes 05 und 06 beschrieben worden sind • Der Wert wird ca. alle 30s aktualisiert

Tabelle 36: Statistikzähler sichere zyklische Datenverbindungen

9 SafeLOGIC to SafeLOGIC Communication

Das Safety-System bietet die Möglichkeit sichere Informationen zwischen zwei Sicherheitssteuerungen (SafeLOGIC) auszutauschen. Dies kann dazu verwendet werden um z.B. einen globalen Not-Aus in einem Maschinenverbund zu realisieren oder wenn eine Abhängigkeit zwischen den Sicherheitsapplikation von zwei oder mehreren Maschinen besteht. Es kann eine zentrale Sammelstelle für Sicherheitsinformationen gebildet werden welche in weiterer Folge die aktuellen Werte an alle relevanten Stellen verteilt.



Hinweis:

Die Nummer der Safety Domain ergibt sich aus der SafeLOGIC ID. Um die Kommunikation nutzen zu können müssen die SafeLOGIC IDs eindeutig sein. Auf die Eindeutigkeit sollte schon von Beginn an geachtet werden.

Zu diesem Zweck stellt eine SafeLOGIC ein Safety Domain Gateway (SDG) zur Verfügung an welches mehrere andere SafeLOGICs (Source) verbunden werden können. Über diese Gateway-Funktionalität ist es somit möglich zwischen mehreren Safety Domains zu kommunizieren. Die Verbindung zwischen Source SafeLOGIC und SDG SafeLOGIC stellt sich im Projekt der Source SafeLOGIC als zusätzliches Safety Modul dar, welches Kommunikationskanäle zur Verfügung stellt. Eine SDG SL kann für sich wieder als Source verwendet werden und mit einer weiteren SDG SL verbunden werden. Dadurch kann eine Kaskadierung der Kommunikationsbeziehungen erreicht werden.

Eine Source SL kann auch mehrere Mal an die gleiche SDG SL verbunden sein. Weiters ist es auch möglich, dass die Source SL mit mehreren SDG SLs kommuniziert. Dadurch ergeben sich mehrere Möglichkeiten wie die SafeLOGIC to SafeLOGIC Communication aufgebaut werden kann.

Hinweis:

Bei einer SDG SL handelt es sich immer um die PLUS Variante der SafeLOGIC. Source SLs können sowohl Standard SLs als auch PLUS SLs sein.

9.1 Möglichkeiten

Das System unterstützt verschiedene Möglichkeiten bei der Kommunikation. Die entsprechende Kommunikationsart wird über Parameter im Automation Studio festgelegt.

Fixe Kommunikation

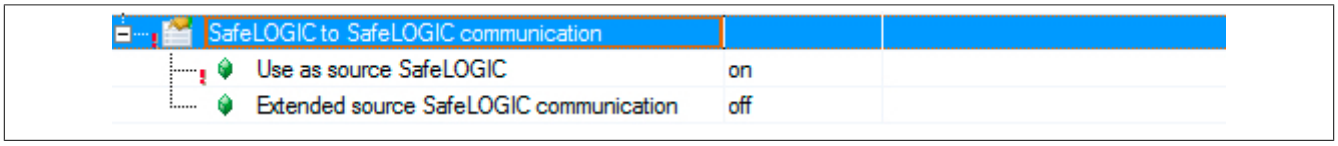
- 8 BOOL Kanäle (1 Byte) je Kommunikationsrichtung
- eine Source SL kann immer nur mit einer SDG SL kommunizieren
- keine Konstellation jede mit jeder

Extended Kommunikation (ab Release 1.4 und AS 3.0.90)

- Kommunikationskanäle frei konfigurierbar
- Limitierung auf 16 Kanäle (wobei je 8 BOOL als 1 Kanal gerechnet werden; andere Datentypen werden 1:1 eingerechnet).
- eine Source SL kann mit mehreren SDG SLs kommunizieren
- Konstellation jede mit jeder möglich

9.2 Konfiguration im Automation Studio

Um die SafeLOGIC to SafeLOGIC Communication nutzen zu können ist zuerst eine SafeLOGIC als Source SL zu konfigurieren. Dies wird über die I/O Configuration durchgeführt.

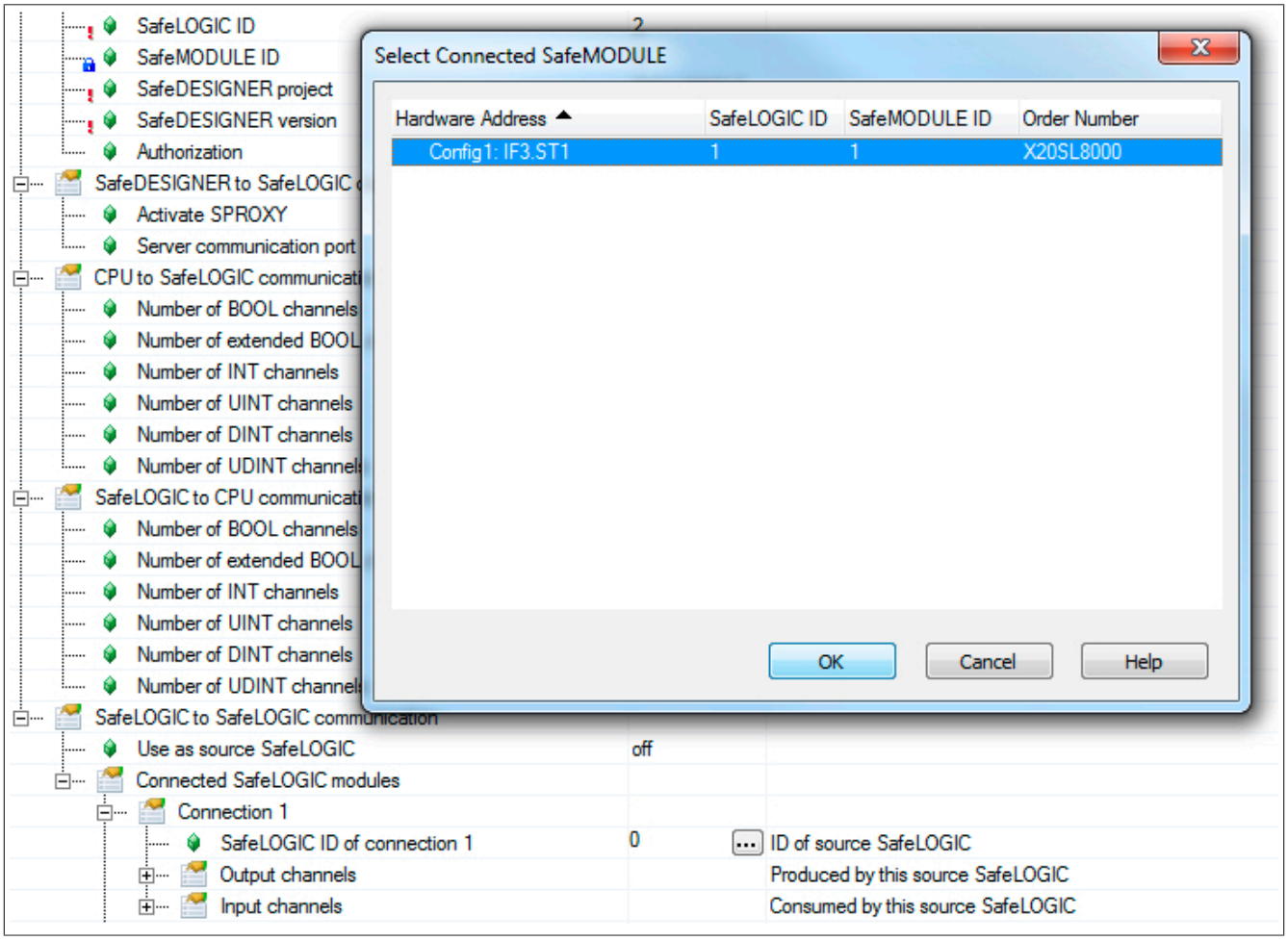


Zusätzlich kann nach dem Aktivieren des Parameters "Use as source SafeLOGIC" die Ausprägung - fix oder extended - der SafeLOGIC to SafeLOGIC Communication konfiguriert werden. Ist der Parameter "Extended source SafeLOGIC communication" nicht aktiviert so wird die fixe Kommunikation verwendet.

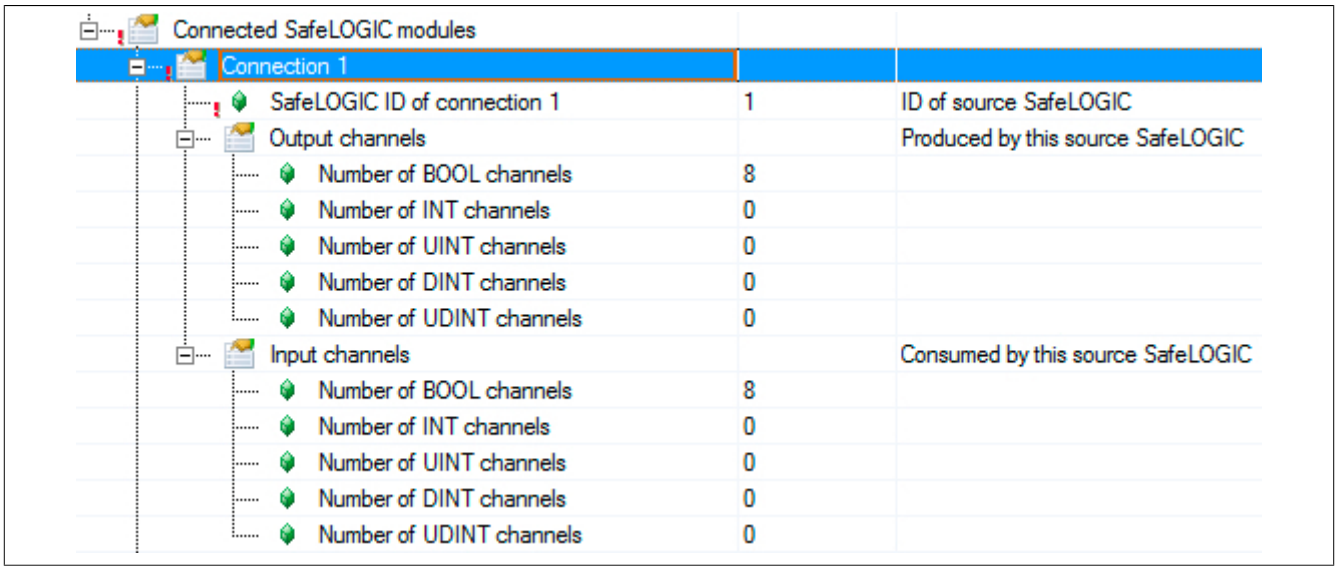
Hinweis:

Sollte zu einem späteren Zeitpunkt die Kommunikationsart - fix oder extended - geändert werden kann dies zu Kanalüberschneidungen im SafeDESIGNER führen und es sind die Kommunikationskanäle neu zu verbinden.

Im nächsten Schritt wird die Source SL mit der SDG SL verbunden. Dazu gibt es im Automation Studio unter der I/O Configuration einer SafeLOGIC Plus entsprechende Verbindungspunkte. Über die Connection Sections wird mit Hilfe des Wizards im Automation Studio die jeweilige SafeLOGIC ID (Safety Domain) spezifiziert.



Unter jeder Connection sind die benötigten Kommunikationskanäle zu definieren. Bei fixer Kommunikation sind diese auf 8 BOOL Kanäle je Richtung limitiert.



9.3 Darstellung im SafeDESIGNER

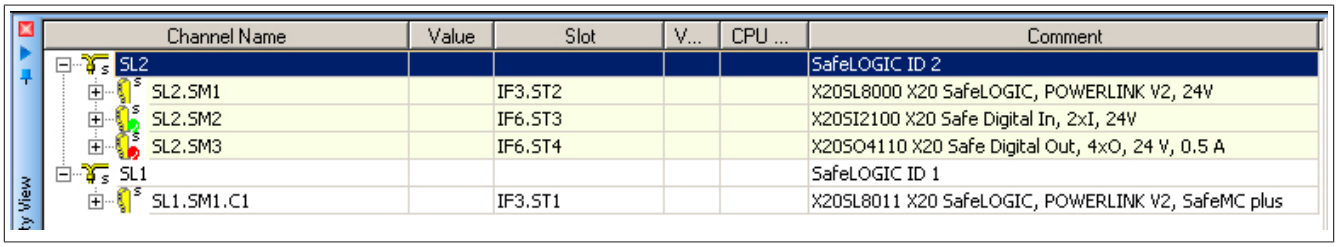
Im SafeDESIGNER Projekt der jeweiligen SafeLOGIC (Source oder SDG) finden sich die Kommunikationskanäle wieder.

Vorsicht!

Alle im Projekt verwendeten Kommunikationskanäle müssen in beiden SafeDESIGNER Projekten mit dem gleichen Variablennamen gemappt werden. Über die Kanäle bzw. Variablennamen wird eine Checksumme gerechnet und zur Laufzeit überprüft. Sollte die Checksumme nicht übereinstimmen setzt das System eine entsprechende Logger-Meldung im Safety Logger ab und die Kommunikation funktioniert nicht.

9.3.1 SafeDESIGNER Projekt Source SL

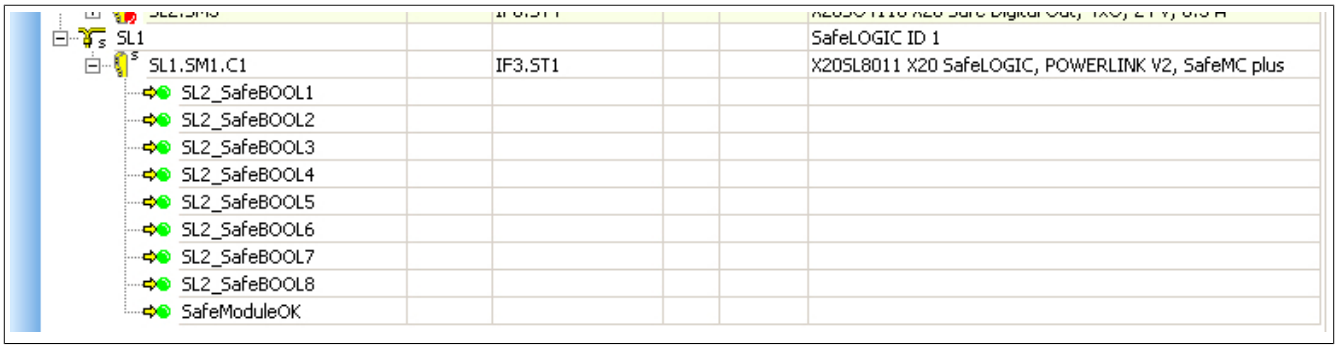
Die Kommunikation stellt sich im SafeDESIGNER Projekt der Source SL wie ein zusätzliches Modul dar. Das Modul befindet sich unter einem eigenen Knoten, dieser repräsentiert die Verbindung zu dieser Safety Domain.



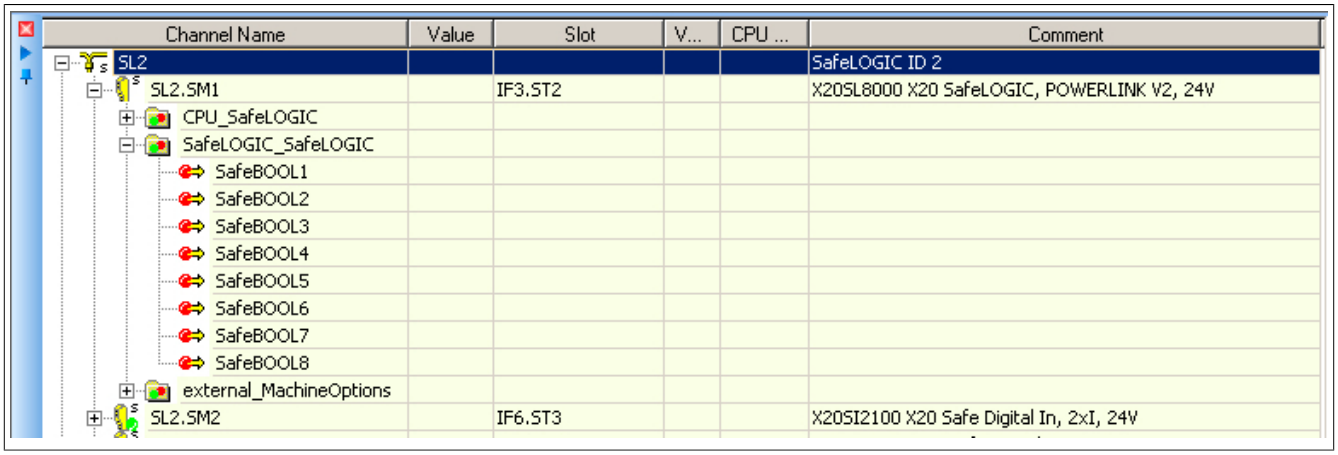
Wird dieses Modul ausgewählt können dafür sicherheitstechnische Parameter eingestellt werden (siehe Abschnitt Parameter für Verbindung).

Fixe Kommunikation

Unter dem Modul finden sich die Eingangskanäle, welche von der SDG SL an die Source SL geschickt werden, sowie eine Bitinformation zum Zustand der Verbindung.

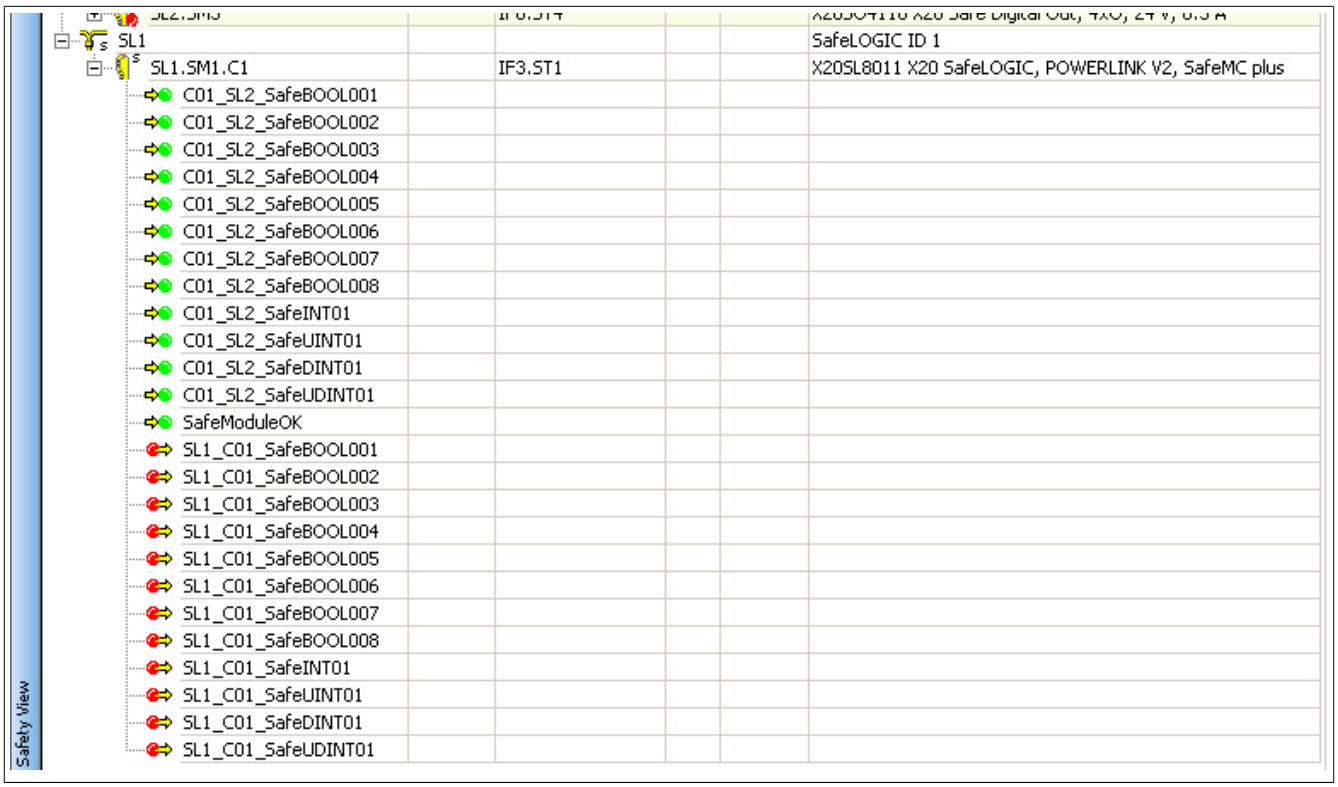


Unter der eigentlichen SL des Projekts finden sich die Ausgangskanäle, welche von der Source SL an die SDG SL geschickt werden, im Bereich "SafeLOGIC_SafeLOGIC".



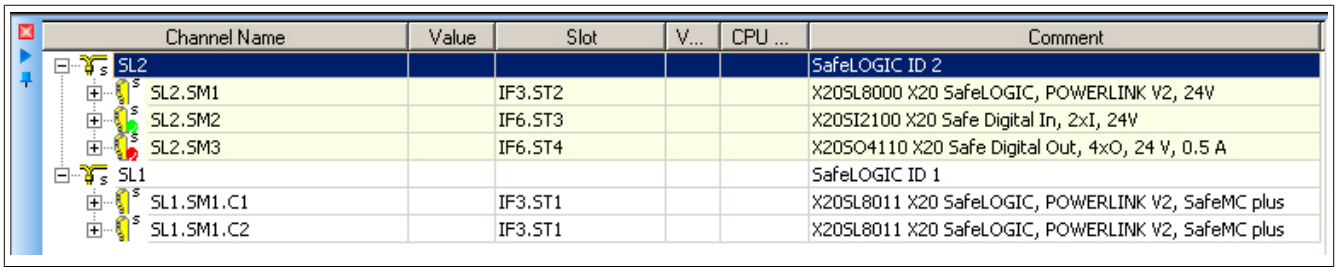
Extended Kommunikation

Unter dem Modul finden sich die Eingangskanäle, die Ausgangskanäle sowie eine Bitinformation zum Zustand der Verbindung.



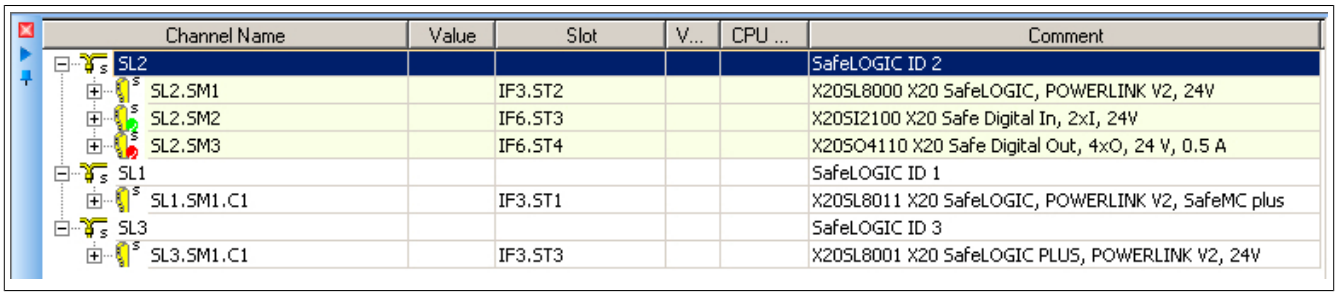
Weitere Verbindung

Sollte die Source SL ein weiteres Mal auf die gleiche SDG SL verbunden sein so gibt es unter dem gleichen Knoten ein weiteres Modul mit Parametern sowie den Kommunikationskanälen.



Channel Name	Value	Slot	V...	CPU ...	Comment
SL2					SafeLOGIC ID 2
SL2.SM1		IF3.ST2			X20SL8000 X20 SafeLOGIC, POWERLINK V2, 24V
SL2.SM2		IF6.ST3			X20SI2100 X20 Safe Digital In, 2xI, 24V
SL2.SM3		IF6.ST4			X20SO4110 X20 Safe Digital Out, 4xO, 24 V, 0.5 A
SL1					SafeLOGIC ID 1
SL1.SM1.C1		IF3.ST1			X20SL8011 X20 SafeLOGIC, POWERLINK V2, SafeMC plus
SL1.SM1.C2		IF3.ST1			X20SL8011 X20 SafeLOGIC, POWERLINK V2, SafeMC plus

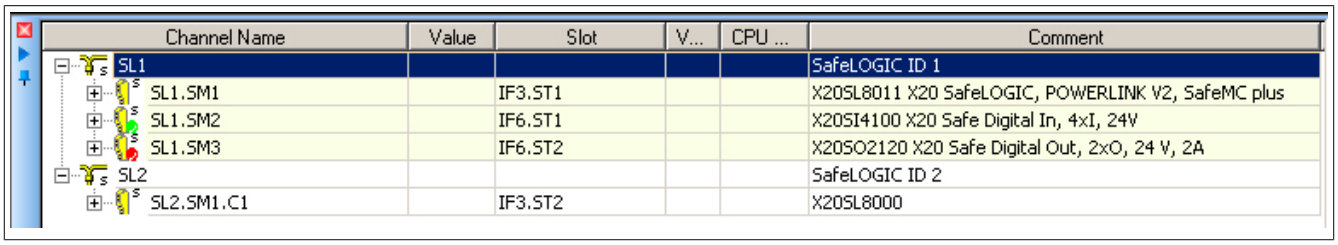
Sollte die Source SL auf eine weitere SDG SL verbunden sein so gibt es einen zusätzlichen Knoten für die Safety Domain sowie ein Modul mit Parametern und den Kommunikationskanälen.



Channel Name	Value	Slot	V...	CPU ...	Comment
SL2					SafeLOGIC ID 2
SL2.SM1		IF3.ST2			X20SL8000 X20 SafeLOGIC, POWERLINK V2, 24V
SL2.SM2		IF6.ST3			X20SI2100 X20 Safe Digital In, 2xI, 24V
SL2.SM3		IF6.ST4			X20SO4110 X20 Safe Digital Out, 4xO, 24 V, 0.5 A
SL1					SafeLOGIC ID 1
SL1.SM1.C1		IF3.ST1			X20SL8011 X20 SafeLOGIC, POWERLINK V2, SafeMC plus
SL3					SafeLOGIC ID 3
SL3.SM1.C1		IF3.ST3			X20SL8001 X20 SafeLOGIC PLUS, POWERLINK V2, 24V

9.3.2 SafeDESIGNER Projekt SDG SL

Die Kommunikation stellt sich im SafeDESIGNER Projekt der SDG SL wie ein zusätzliches Modul dar. Das Modul befindet sich unter einem eigenen Knoten, dieser repräsentiert die Verbindung zu dieser Safety Domain.



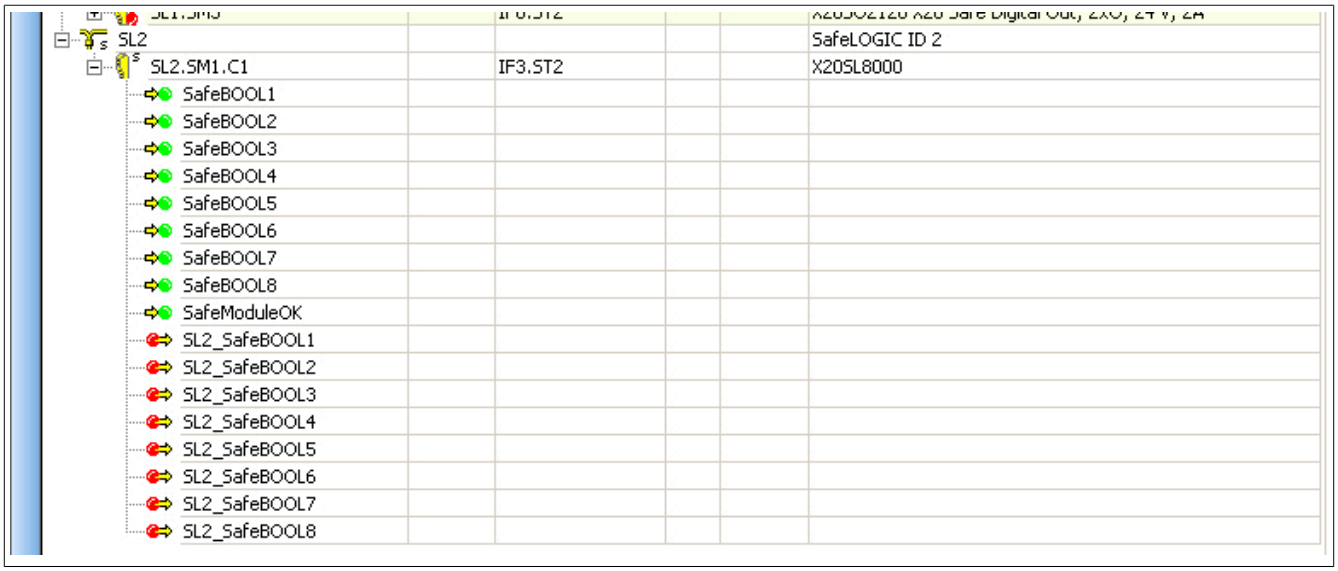
Channel Name	Value	Slot	V...	CPU ...	Comment
SL1					SafeLOGIC ID 1
SL1.SM1		IF3.ST1			X20SL8011 X20 SafeLOGIC, POWERLINK V2, SafeMC plus
SL1.SM2		IF6.ST1			X20SI4100 X20 Safe Digital In, 4xI, 24V
SL1.SM3		IF6.ST2			X20SO2120 X20 Safe Digital Out, 2xO, 24 V, 2A
SL2					SafeLOGIC ID 2
SL2.SM1.C1		IF3.ST2			X20SL8000

Hinweis:

Im Projekt der SDG SL stehen für die Verbindung keine Parameter zur Verfügung. Diese müssen im Projekt der Source SL eingestellt werden.

Fixe Kommunikation

Unter dem Modul finden sich die Eingangskanäle, die Ausgangskanäle sowie eine Bitinformation zum Zustand der Verbindung.

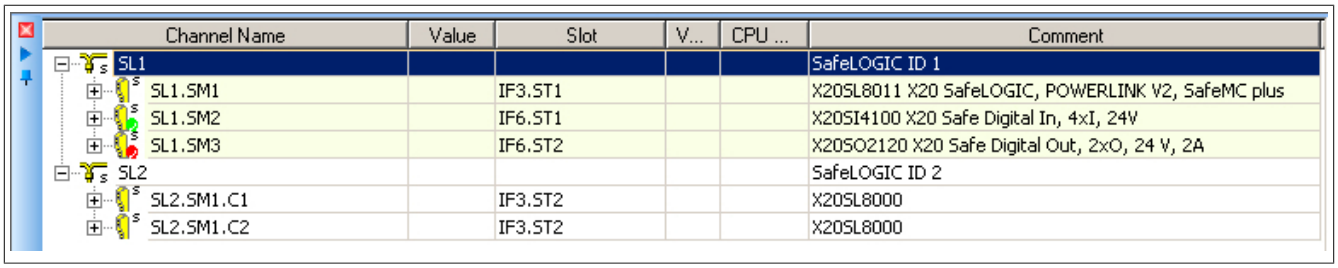


Extended Kommunikation

Unter dem Modul finden sich die Eingangskanäle, die Ausgangskanäle sowie eine Bitinformation zum Zustand der Verbindung.

Weitere Verbindung

Sollte die Source SL ein weiteres Mal auf die SDG SL verbunden sein so gibt es unter dem gleichen Knoten ein weiteres Modul mit den entsprechenden Kommunikationskanälen.



Channel Name	Value	Slot	V...	CPU ...	Comment
SL1					SafeLOGIC ID 1
SL1.SM1		IF3.ST1			X20SL8011 X20 SafeLOGIC, POWERLINK V2, SafeMC plus
SL1.SM2		IF6.ST1			X20SI4100 X20 Safe Digital In, 4xI, 24V
SL1.SM3		IF6.ST2			X20SO2120 X20 Safe Digital Out, 2xO, 24 V, 2A
SL2					SafeLOGIC ID 2
SL2.SM1.C1		IF3.ST2			X20SL8000
SL2.SM1.C2		IF3.ST2			X20SL8000

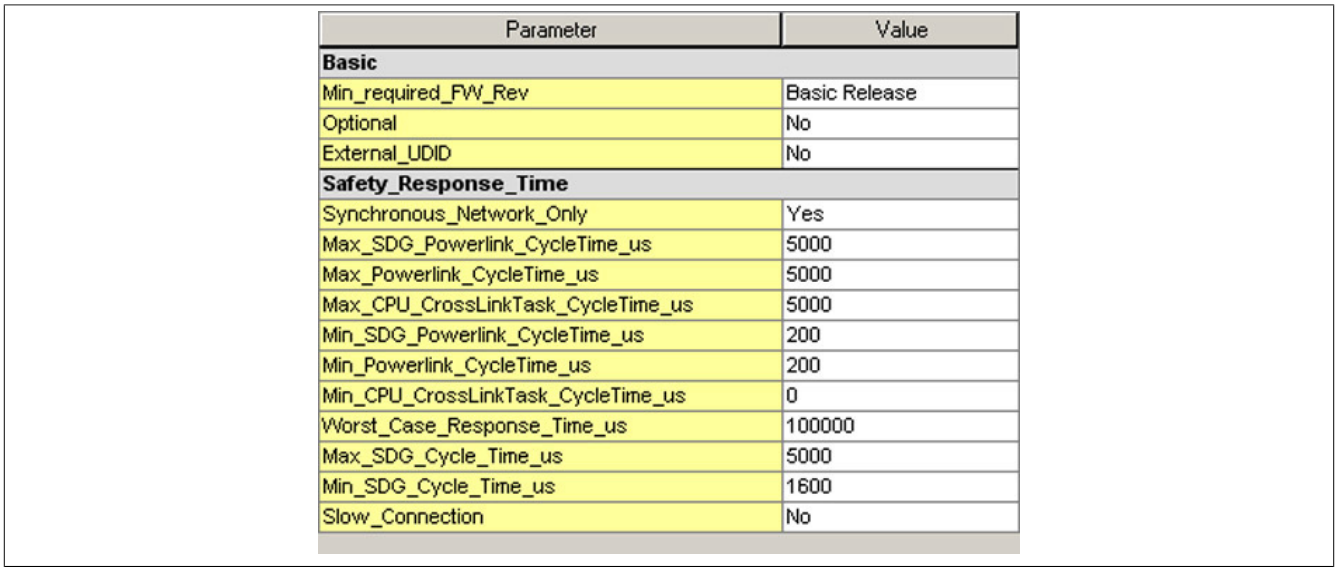
9.4 Parameter für Verbindung

Ab Safety Release 1.4:

Für die Kommunikation stehen ebenfalls Zykluszeitparameter zur Verfügung um die Worst Case Response Time zu definieren. Wie auch bei der Kommunikation mit anderen Safety Modulen handelt es sich dabei um einen Timeout-Wert der im Fehlerfall (z. B. Netzwerkverbindung geht verloren) abläuft.

Hinweis:

Da sich die SafeLOGIC to SafeLOGIC Communication wie ein zusätzliches Safety Modul an der Source SL darstellt, sind die Parameter für die Verbindung im Projekt der Source SL verfügbar und einzustellen.



Parameter	Value
Basic	
Min_required_FW_Rev	Basic Release
Optional	No
External_UDID	No
Safety_Response_Time	
Synchronous_Network_Only	Yes
Max_SDG_Powerlink_CycleTime_us	5000
Max_Powerlink_CycleTime_us	5000
Max_CPU_CrossLinkTask_CycleTime_us	5000
Min_SDG_Powerlink_CycleTime_us	200
Min_Powerlink_CycleTime_us	200
Min_CPU_CrossLinkTask_CycleTime_us	0
Worst_Case_Response_Time_us	100000
Max_SDG_Cycle_Time_us	5000
Min_SDG_Cycle_Time_us	1600
Slow_Connection	No

Gruppe: Basic

<table>
<tr><th>Parameter</th><th>Beschreibung</th><th>Default Wert</th><th>Einheit</th></tr>
<tr><td>Min_required_FW_Rev</td><td>Dieser Parameter ist für zukünftige Funktionserweiterungen reserviert.</td><td>Basic Release</td><td>-</td></tr>
<tr><td>Optional</td><td>Mittels diesem Parameter kann das Modul "optional" parametriert werden. Optionale Module müssen nicht vorhanden sein, d. h. falls solche Module fehlen, wird von der SafeLOGIC das Fehlen nicht signalisiert. Dieser Parameter hat jedoch keinen Einfluss auf die Signal- bzw. Statusdaten des Moduls.</td><td>Nein</td><td>-</td></tr>
<tr><td></td><td colspan="3">
<table>
<tr><th>Parameter Wert</th><th>Beschreibung</th></tr>
<tr><td>Nein</td><td>Das Modul ist für die Applikation zwingend erforderlich.

Das Modul muss nach dem Hochlauf im Operational Mode und die sichere Kommunikation zur SafeLOGIC muss fehlerfrei aufgebaut sein (SafeModulOk = SAFE-TRUE). Der Start der Abarbeitung der sicheren Applikation in der SafeLOGIC wird nach dem Hochlauf verzögert, bis dieser Zustand für alle Module mit "Optional = Nein" erreicht ist.

Nach dem Hochlauf werden Modulprobleme mittels schnell blinkender MXCHG LED an der SafeLOGIC signalisiert. Ausserdem erfolgt ein Eintrag ins Logbuch.</td></tr>
<tr><td>Ja</td><td>Das Modul ist für die Applikation nicht erforderlich.

Das Modul wird beim Hochlauf nicht betrachtet, d.h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Ja" im Operational Mode sind bzw. ob die sichere Kommunikation dieser Module zur SafeLOGIC korrekt aufgebaut ist oder nicht.

Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender MXCHG LED an der SafeLOGIC signalisiert. Ausserdem erfolgt KEIN Eintrag ins Logbuch.</td></tr>
<tr><td>Hochlauf</td><td>Das Modul ist optional, während des Hochlaufs wird über das weitere Verhalten des Moduls entschieden.

Wird während des Hochlaufs erkannt, dass das Modul physikalisch vorhanden ist (unabhänig davon, ob es sich im Mode Operational befindet oder nicht) so verhält sich das Module wie bei "Optional = Nein".

Wird wärend des Hochlaufs erkannt, dass das Modul phyiskalisch nicht vorhanden ist, verhält sich das Module wie bei "Optional = Ja".</td></tr>
</table>
</td></tr>
<tr><td>External_UDID</td><td>Dieser Parameter aktiviert zum Modul die Möglichkeit, die erwartete UDID extern von der CPU vorgeben zu lassen.</td><td>Nein</td><td>-</td></tr>
<tr><td></td><td colspan="3">
<table>
<tr><th>Parameter Wert</th><th>Beschreibung</th></tr>
<tr><td>Ja-ACHTUNG</td><td>Die UDID wird von der CPU vorgegeben, bei einer Änderung der UDID ist ein Neustart der SafeLOGIC notwendig.</td></tr>
<tr><td>Nein</td><td>Die UDID wird mittels eines Teach In Verfahrens während der Inbetriebnahme vorgegeben.</td></tr>
</table>
</td></tr>
</table>

Tabelle 37: Parameter SafeDESIGNER: Basic

Gefahr!

Falls die Funktion "External_UDID = Ja-ACHTUNG" benutzt wird, können durch falsche Vorgaben von der CPU sicherheitskritische Situationen entstehen.
Führen Sie deshalb eine FMEA durch um diese Situationen zu erkennen und mittels zusätzlicher, sicherheitstechnischer Maßnahmen abzusichern.

Gruppe: Safety_Response_Time

<table>
<tr><th>Parameter</th><th>Beschreibung</th><th>Default Wert</th><th>Einheit</th></tr>
<tr><td>Synchronous_Network_Only</td><td>Dieser Parameter legt die Synchronisationseigenschaften des Zugrunde liegenden Netzwerks fest.

<table><tr><th>Parameter Wert</th><th>Beschreibung</th></tr><tr><td>Ja</td><td>Für die Berechnung der sicheren Reaktionszeit werden ausschließlich synchrone Netzwerke mit gleichen Zykluszeiten oder ganzzahligen Verhältnissen der Zykluszeiten vorausgesetzt.</td></tr><tr><td>Nein</td><td>Keine Anforderung an die Synchronität der Netzwerke.</td></tr></table></td><td>Ja</td><td>-</td></tr>
<tr><td>Max_SDG_Powerlink_CycleTime_us</td><td>Dieser Parameter gibt die max. Zykluszeit des POWERLINK-Netzwerkes an, in dem die andere SafeLOGIC betrieben wird.
• Erlaubte Werte: 200 - 30000 µs</td><td>5000</td><td>µs</td></tr>
<tr><td>Max_Powerlink_CycleTime_us</td><td>Dieser Parameter gibt die max. POWERLINK Zykluszeit für die Berechnung der sicheren Reaktionszeit an.
• Erlaubte Werte: 200 - 30000 µs</td><td>5000</td><td>µs</td></tr>
<tr><td>Max_CPU_CrossLinkTask_CycleTime_us</td><td>Dieser Parameter gibt die max. Zykluszeit für das Kopieren der Daten zwischen den zwei Powerlink-Netzwerken an. Ein Wert von "0" signalisiert, dass sich beide SafeLOGICen in demselben Powerlink-Netzwerk befinden.
• Erlaubte Werte: 0 - 3000000 µs</td><td>5000</td><td>µs</td></tr>
<tr><td>Min_SDG_Powerlink_CycleTime_us</td><td>Dieser Parameter gibt die max. Zykluszeit des POWERLINK-Netzwerkes an, in dem die andere SafeLOGIC betrieben wird.
• Erlaubte Werte: 200 - 30000 µs</td><td>200</td><td>µs</td></tr>
<tr><td>Min_Powerlink_CycleTime_us</td><td>Dieser Parameter gibt die min. POWERLINK Zykluszeit für die Berechnung der sicheren Reaktionszeit an.
• Erlaubte Werte: 200 - 30000 µs</td><td>200</td><td>µs</td></tr>
<tr><td>Min_CPU_CrossLinkTask_CycleTime_us</td><td>Dieser Parameter gibt die min. Zykluszeit für das Kopieren der Daten zwischen den zwei Powerlink-Netzwerken an. Ein Wert von "0" signalisiert, dass sich beide SafeLOGICen in demselben Powerlink-Netzwerk befinden.
• Erlaubte Werte: 0 - 3000000 µs</td><td>0</td><td>µs</td></tr>
<tr><td>Worst_Case_Response_Time_us</td><td>Dieser Parameter gibt den Grenzwert für die Überwachung der sicheren Reaktionszeit an.
• Erlaubte Werte: 3000 - 12500000 µs
Hinweis: bei großen Werte auch den Parameter "Slow_Connection" beachten!</td><td>100000</td><td>µs</td></tr>
<tr><td>Max_SDG_Cycle_Time_us</td><td>Dieser Parameter gibt die max. Zykluszeit der anderen SafeLOGIC für die Berechnung der sicheren Reaktionszeit an.
• Erlaubte Werte: 800 - 20000</td><td>5000</td><td>µs</td></tr>
<tr><td>Min_SDG_Cycle_Time_us</td><td>Dieser Parameter gibt die min. Zykluszeit der anderen SafeLOGIC für die Berechnung der sicheren Reaktionszeit an.
• Erlaubte Werte: 800 - 20000</td><td>1600</td><td>µs</td></tr>
<tr><td>Slow_Connection</td><td>Dieser Parameter gibt an, ob es sich bei dieser Verbindung um eine langsame Verbindung handelt.

<table><tr><th>Parameter Wert</th><th>Beschreibung</th></tr><tr><td>Ja</td><td>Es handelt sich um eine Verbindung mit großem Verhältnis zwischen SafeLOGIC-Zykluszeit und Telegrammlaufzeit (wirkt sich intern auf die Parameterberechnung aus).
Faustregel: "Ja" ab Verhältnis 50:1</td></tr><tr><td>Nein</td><td>Standard-Verbindung. Parameterberechnung unverändert.</td></tr></table></td><td>Nein</td><td>-</td></tr>
</table>

Tabelle 38: Parameter SafeDESIGNER: Safety_Response_Time

Hinweis:

Der Parameter CPU_CrossLinkTask_CycleTime_us wird benötgit wenn sich Source SL und SDG SL in unterschiedlichen Netzwerken oder auf unterschiedlichen Steuerungen befinden. Wenn dies nicht der Falls ist, dann ist der Minimal-Wert bzw. Maximal-Wert auf 0 zu setzen.

Für diesen Parameter ist die ganze Verbindungsstrecke zwischen den Steuerungen zu beachten - auch Kopierzeit zwischen den beteiligten Interfaces.

Hinweis:

Über den Parameter Slow_Connection kann zusätzlich noch angegeben werden, dass es sich bei der Verbindung zwischen Source SL und SDG SL um eine langsame Verbindung handelt. Wird für das Timeout der Verbindung ein Wert von einigen Sekunden benötigt so muss der Parameter aktiviert werden.

10 Bestimmungsgemäße Verwendung

10.1 Qualifiziertes Personal

Die Anwendung der sicherheitstechnischen Produkte ist ausschließlich auf folgende Personen begrenzt:

- qualifiziertes Personal, das mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und Vorschriften vertraut ist.
- qualifiziertes Personal, das Sicherheitseinrichtungen für Maschinen und Anlagen plant, entwickelt, einbaut und in Betrieb nimmt.

Qualifiziertes Personal im Sinne der sicherheitstechnischen Hinweise dieses Handbuches sind Personen, die aufgrund ihrer Ausbildung, Erfahrung und Unterweisung sowie ihrer Kenntnisse über einschlägige Normen, Bestimmungen, Unfallverhütungsvorschriften und Betriebsverhältnisse berechtigt sind, die jeweils erforderlichen Tätigkeiten auszuführen und dabei mögliche Gefahren erkennen und vermeiden können.
In diesem Sinne werden auch ausreichende Sprachkenntnisse für das Verständnis dieses Handbuches vorausgesetzt.

10.2 Anwendungsbereich

Die in diesem Handbuch beschriebenen, sicherheitsgerichteten Steuerungskomponenten von B&R sind für die besonderen Aufgabenstellungen im Maschinen- und Personenschutz entworfen, entwickelt und hergestellt. Diese sind nicht geeignet für einen Gebrauch, der verhängnisvolle Risiken oder Gefahren birgt, die ohne Sicherstellung außergewöhnlich hoher Sicherheitsmaßnahmen zu Tod oder Verletzung vieler Personen oder schwerer Umweltbeeinträchtigungen führen könnte. Solche stellen insbesondere die Verwendung bei der Überwachung von Kernreaktionen in Kernkraftwerken, von Flugleitsystemen, bei der Flugsicherung, bei der Steuerung von Massentransportmitteln, bei medizinischen Lebenserhaltungssystemen, und Steuerung von Waffensystemen dar.

Beim Einsatz aller sicherheitsgerichteter Steuerungskomponenten sind die für die industriellen Steuerungen geltenden Sicherheitsmaßnahmen (Absicherung durch Schutzeinrichtungen wie z. B. Not-Aus etc.) gemäß den jeweils zutreffenden nationalen bzw. internationalen Vorschriften zu beachten. Dies gilt auch für alle weiteren angeschlossenen Geräte wie z. B. Antriebe oder Lichtgitter.

Die Sicherheitshinweise, die Angaben zu den Anschlussbedingungen (Typenschild und Dokumentation) und die in den technischen Daten angegebenen Grenzwerte sind vor der Installation und Inbetriebnahme sorgfältig durchzulesen und unbedingt einzuhalten.

10.3 Haftungsausschluss

Der Anwender muss den Einsatz der B&R sicherheitsgerichteten Steuerungskomponenten in eigener Verantwortung mit der für ihn zuständigen Behörde abstimmen und einhalten.

B&R übernimmt keine Haftung oder Gewähr für Schäden, die entstehen durch:

- Unsachgemäßen Gebrauch
- Nichtbeachtung von Normen und Richtlinien
- Unerlaubte Änderungen an Geräten, Verbindungen und Einstellungen
- Verwendung von nicht zugelassenen oder ungeeigneten Geräten oder Gerätegruppen
- Nichtbeachtung der in diesem Handbuch angeführten Sicherheitshinweise

10.4 Installationshinweise

Die Produkte müssen gegen unzulässige Verschmutzung geschützt werden. Für die Produkte ist eine maximale Verschmutzung entsprechend dem Verschmutzungsgrad II der IEC 60664 zulässig.

Üblicherweise kann Verschmutzungsgrad II mit einer Umhausung in der Schutzart IP 54 erreicht werden wobei aber der Betrieb in kondensierender Luftfeuchtigkeit NICHT erlaubt ist.

Gefahr!

Bei stärkeren Verschmutzungen als es Verschmutzungsgrad II der IEC 60664 beschreibt kann es zu gefahrbringenden Ausfällen kommen. Sorgen Sie unbedingt für eine ordnungsgemäße Betriebsumgebung.

Gefahr!

Um eine definierte Spannungsversorgung zu gewährleisten, muss für die Bus-, SafeIO- und SafeLOGIC-Versorgung ein SELV-Netzteil gemäß IEC 60204 verwendet werden.

Sofern die Spannungsversorgung geerdet wird (PELV System) so ist ausschließlich eine Erdverbindung mit GND zulässig. Erdungsvarianten, in denen die Erde mit +24V verbunden werden, sind nicht erlaubt.

Wie in nachfolgender Abbildung dargestellt sind die X20 Potenzialgruppen jeweils mit einer Sicherung mit maximal 10 A abzusichern.

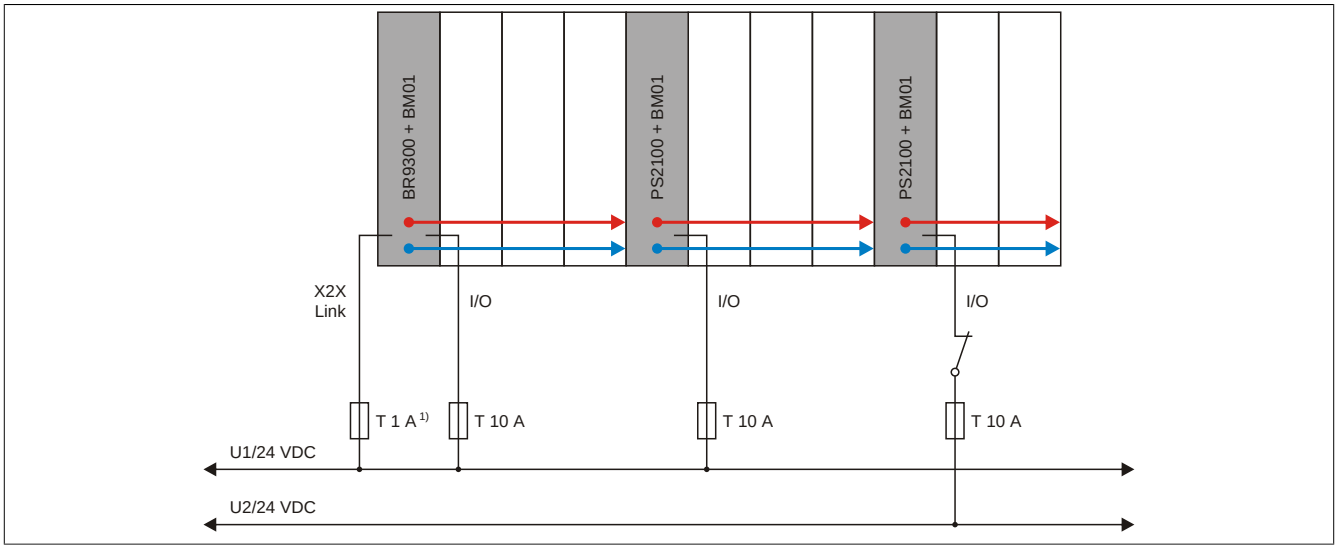


Abbildung 12: Absicherung verschiedener Potenzialgruppen

1) Empfohlen zur Leitungsabsicherung

10.5 Sicherer Zustand

Als Folge eines vom Modul aufgedeckten Fehlers (interner Fehler oder Verdrahtungsfehler) aktivieren die Module den sicheren Zustand. Der sichere Zustand ist konstruktiv als Low Zustand bzw. Abschalten festgelegt und kann nicht verändert werden.

Gefahr!

Für Anwendungen in denen der sichere Zustand das aktive Einschalten eines Aktors bewirken muss, sind zusätzliche, externe sicherheitstechnische Maßnahmen vorzusehen (z. B. mechanische Bremsen bei hängender Last).

10.6 Gebrauchsdauer

Alle Safety Module haben eine maximale Gebrauchsdauer von 20 Jahren.

Dies bedeutet, dass alle Safety Module spätestens eine Woche vor Ablauf dieser 20 Jahre (gerechnet ab dem Auslieferungsdatum von B&R) außer Betrieb zu nehmen sind.

Gefahr!

Ein Betrieb der Safety Module über die spezifizierte Gebrauchsdauer hinaus ist nicht zulässig! Der Anwender muss sicherstellen, dass alle Safety Module vor Überschreiten ihrer Gebrauchsdauer außer Betrieb genommen bzw. durch neue Safety Module ersetzt werden.

11 Releaseinformation

Eine Handbuchversion beschreibt immer den zugehörigen Funktionsumfang eines Produktset Release. Die nachfolgende Tabelle zeigt die Abhängigkeit zwischen der Handuchversion und Release.

Handbuchversion	gültig für		
V1.51 V1.50 V1.42 V1.41 V1.40 V1.20 V1.10	**Version**	**ab**	**bis**
	Produktset	Release 1.2	Release 1.5
	SafeDESIGNER	2.70	2.99
	Firmware	270	299
	Upgrades	1.2.0.0	1.5.999.999
V1.02 V1.01 V1.00	**Version**	**ab**	**bis**
	Produktset	Release 1.0	Release 1.1
	SafeDESIGNER	2.58	2.69
	Firmware	256	269
	Upgrades	1.0.0.0	1.1.999.999

Tabelle 39: Releaseinformation

12 Handbuchhistorie

Version	Datum	Kommentar
1.51	März 2012	Abschnitt 6.1 Registerbeschreibung - Parameter in der I/O Konfiguration - Gruppe General • Erweitert um Parameter "Authorization" Abschnitt 7.3 Wartungsszenarien - Bestätigung eines Firmwaretauschs • Erweitert um Gefahrenhinweis zu zulässigen Firmwareversionen Abschnitt 8.1 POWERLINK Dateninterface - Fernbedienung • Diverse Korrekturen und Erweiterungen Abschnitt 8.2 und 8.3 POWERLINK Dateninterface - Maschinenoptions- und Applikationsdownload • Schnittstelle - POWERLINK V2 Objekte erweitert um Index:Subindex 0x2405:0x09 und 0x2405:0x0A
1.50	Februar 2012	Abschnitt 9 NEU - SafeLOGIC to SafeLOGIC Communication
1.42	Oktober 2011	Abschnitt 9.4 Bestimmungsgemäße Verwendung - Installationshinweise • Um Installationshinweis zur zulässigen Erdung ergänzt
1.41	Februar 2011	Abschnitt 8.1 POWERLINK Dateninterface - Fernbedienung - Fernbedienungsschnittstelle • Korrektur des "Index:Subindex" des POWERLINK V2 Objekts Abschnitt 8.1 POWERLINK Dateninterface - Fernbedienung - Status auslesen • Korrektur der Beschreibungen der Werte 19-21
1.40	Februar 2011	Erste Ausgabe als produktspezifisches Handbuch

Tabelle 40: Handbuchhistorie