

X20(c)SL81xx

Information:

B&R ist bemüht das Datenblatt so aktuell wie möglich zu halten. Aus sicherheitstechnischer Sicht muss jedoch immer die aktuelle Datenblatt-Version verwendet werden.

Das zertifizierte und damit aktuell gültige Datenblatt ist auf der B&R Homepage www.br-automation.com als Download verfügbar.

Gestaltung von Hinweisen

Sicherheitshinweise

Enthalten **ausschließlich** Informationen, die vor gefährlichen Funktionen oder Situationen warnen.

Signalwort	Beschreibung
Gefahr!	Bei Missachtung der Sicherheitsvorschriften und -hinweise werden Tod, schwere Verletzungen oder große Sachschäden eintreten.
Warnung!	Bei Missachtung der Sicherheitsvorschriften und -hinweise können Tod, schwere Verletzungen oder große Sachschäden eintreten.
Vorsicht!	Bei Missachtung der Sicherheitsvorschriften und -hinweise können leichte Verletzungen oder Sachschäden eintreten.
Achtung!	Bei Missachtung der Sicherheitsvorschriften und -hinweise können Sachschäden eintreten.

Tabelle 1: Gestaltung von Sicherheitshinweisen

Allgemeine Hinweise

Enthalten **nützliche** Informationen für Anwender und Angaben zur Vermeidung von Fehlfunktionen.

Signalwort	Beschreibung
Information:	Nützliche Informationen, Anwendungstipps und Angaben zur Vermeidung von Fehlfunktionen.

Tabelle 2: Gestaltung von Allgemeinen Hinweisen

1 Allgemeines

Die Module verfügen über eine SafeLOGIC-Funktionalität, welche es erlaubt die im SafeDESIGNER applizierten Anwendungen sicher abzarbeiten. Die Module können dabei für sicherheitstechnische Anwendungen bis PL e bzw. SIL 3 eingesetzt werden.

Die SafeLOGIC koordiniert weiters die sicherheitstechnische Kommunikation aller an der Applikation beteiligten Module. In diesem Kontext überwacht die SafeLOGIC auch die Konfiguration dieser Module und führt, falls notwendig, autonom Parameterdownloads auf die Module durch. Damit wird über alle Modultauch- und Wartungs-szenarien hinweg immer eine konsistente und sicherheitstechnisch korrekte Modulkonfiguration im Netzwerk garantiert. Bei SafeLOGIC-Produkten werden diese Services von der SafeLOGIC ausgeführt, bei Produkten der SafeLOGIC-X-Ausprägung werden diese Services im Zusammenwirken mit dem Automation Runtime auf der funktionalen CPU ausgeführt. Die sicherheitstechnischen Eigenschaften für Anwendungen bis PL e bzw. SIL 3 sind jedoch in beiden Varianten gegeben.

Die SafeLOGIC-X-Produkte verfügen zusätzlich über die identischen I/O-Eigenschaften wie ihre zugehörigen SafeI/O-Produkte.

- openSAFETY Manager für bis zu 10 / 20 / 100 / 280 SafeNODES
- Flexibel programmierbar mit Automation Studio / SafeDESIGNER
- Innovatives Management sicherer Maschinoptionen (SafeOPTION)
- Parameter- und Konfigurations-Management

1.1 Funktion

SafeLOGIC-Funktion

Das Modul verfügt über eine SafeLOGIC-Funktionalität, welche es erlaubt die im SafeDESIGNER applizierten Anwendungen sicher abzuarbeiten. Das Modul kann dabei für sicherheitstechnische Anwendungen bis PL e bzw. SIL 3 eingesetzt werden.

Das Modul koordiniert weiters die sicherheitstechnische Kommunikation aller an der Applikation beteiligten Module. In diesem Kontext überwacht das Modul auch die Konfiguration dieser Module und führt, falls notwendig, autonom Parameterdownloads auf die Module durch. Damit wird über alle Modultausch- und Wartungsszenarien hinweg immer eine konsistente und sicherheitstechnisch korrekte Modulkonfiguration im Netzwerk garantiert. Bei SafeLOGIC-Produkten werden diese Services von der SafeLOGIC ausgeführt, bei Produkten der SafeLOGIC-X Ausprägung werden diese Services im Zusammenwirken mit dem Automation Runtime auf der funktionalen CPU ausgeführt. Die sicherheitstechnischen Eigenschaften für Anwendungen bis PL e bzw. SIL 3 sind jedoch in beiden Varianten gegeben.

Blackout-Modus

Im Blackout-Modus ist die Modulfunktion auch bei einem Ausfall des Netzwerks weiter gegeben. Ohne diese Funktion würde bei einem Netzwerkausfall auf den betroffenen Modulen immer der sichere Zustand eingeleitet werden. Mit dem Blackout-Modus können darüber hinaus der Betrieb teilweise fortgesetzt oder koordiniert Abschaltsszenarien eingeleitet werden. Zudem ermöglicht dieser Modus das Booten eines Moduls ohne Netzwerk auf der Basis einer zuvor am Modul abgespeicherten Konfiguration.

openSAFETY

Für die Übertragung der Daten auf den unterschiedlichen Bussystemen nutzt das Modul die Schutzmechanismen von openSAFETY. Durch die sichere Kapselung der Daten im openSAFETY-Container müssen die an der Übertragung beteiligten Komponenten des Netzwerkes keinen sicherheitstechnischen Beitrag leisten. An dieser Stelle sind lediglich die in den technischen Daten angegebenen sicherheitstechnischen Kennwerte für openSAFETY heranzuziehen. Die Daten im openSAFETY-Container werden erst in der Gegenstelle der Datenübertragung sicherheitstechnisch bearbeitet und deshalb ist erst diese Komponente wieder Bestandteil der sicherheitstechnischen Betrachtung. Ein lesender Zugriff auf die Daten im openSAFETY-Container, für Anwendungen ohne sicherheitstechnische Eigenschaften, ist an jeder Stelle des Netzwerkes erlaubt, ohne die sicherheitstechnischen Eigenschaften von openSAFETY zu beeinflussen.

open SAFETY

1.2 Coated Module

Coated Module sind X20 Module mit einer Schutzbeschichtung der Elektronikbaugruppe. Die Beschichtung schützt X20c Module vor Betauung.

Die Elektronik der Module ist vollständig funktionskompatibel zu den entsprechenden X20 Modulen.

Information:

In diesem Datenblatt werden zur Vereinfachung nur Bilder und Modulbezeichnungen der unbeschichteten Module verwendet.

Die Beschichtung wurde nach folgenden Normen qualifiziert:

- Betauung: BMW GS 95011-4, 2x 1 Zyklus
- Schadgas: EN 60068-2-60, Methode 4, Exposition 21 Tage

Entgegen den Angaben bei Modulen des X20 Systems ohne Safety Zertifizierung sind die X20 Safety Module trotz der durchgeführten Tests **NICHT für Anwendungen mit Schadgas (EN 60068-2-60) geeignet!**



2 Bestelldaten

		
X20SL8100	X20SL8101	X20SL8110
Bestellnummer	Kurzbeschreibung	
	Zentraleinheiten	
X20SL8100	X20 SafeLOGIC, sichere Steuerung, openSAFETY Gateway, tauschbarer Programmspeicher: SafeKEY, 1 POWERLINK-Schnittstelle, Controlled Node, integrierter 2-fach Hub, inkl. Einspeisemodul, Feldklemme 1x X20TB52 und X20 Abschlussplatte rechts X20AC0SR1 beiliegend, SafeKEY und SafeLOGIC-Funktionsumfang über X20MK-Konfigurator bestellen!	
X20cSL8100	X20 SafeLOGIC, beschichtet, sichere Steuerung, openSAFETY Gateway, tauschbarer Programmspeicher: SafeKEY, 1 POWERLINK-Schnittstelle, Controlled Node, integrierter 2-fach Hub, inkl. Einspeisemodul, Feldklemme 1x X20TB52 und X20 Abschlussplatte rechts X20AC0SR1 beiliegend, SafeKEY und SafeLOGIC-Funktionsumfang über X20MK-Konfigurator bestellen!	
X20SL8101	X20 SafeLOGIC mit X20 Bus Controller, sichere Steuerung, openSAFETY Gateway, tauschbarer Programmspeicher: SafeKEY, 1 POWERLINK-Schnittstelle, Controlled Node, integrierter 2-fach Hub, inkl. Einspeisemodul für interne I/O-Versorgung und X2X Link Versorgung, Feldklemme 1x X20TB52 und X20 Abschlussplatte rechts X20AC0SR1 beiliegend, SafeKEY und SafeLOGIC-Funktionsumfang über X20MK-Konfigurator bestellen!	
X20cSL8101	X20 SafeLOGIC mit X20 Bus Controller, beschichtet, sichere Steuerung, openSAFETY Gateway, tauschbarer Programmspeicher: SafeKEY, 1 POWERLINK-Schnittstelle, Controlled Node, integrierter 2-fach Hub, inkl. Einspeisemodul für interne I/O-Versorgung und X2X Link Versorgung, Feldklemme 1x X20TB52 und X20 Abschlussplatte rechts X20AC0SR1 beiliegend, SafeKEY und SafeLOGIC-Funktionsumfang über X20MK-Konfigurator bestellen!	
X20SL8110	X20 SafeLOGIC, sichere Steuerung, openSAFETY Gateway, tauschbarer Programmspeicher: SafeKEY, 1 POWERLINK-Schnittstelle, 1 Steckplatz für ein X20 Schnittstellenmodul, Controlled Node, integrierter 2-fach Hub, inkl. Einspeisemodul, Feldklemme 1x X20TB52 und X20 Abschlussplatte rechts X20AC0SR1 beiliegend, SafeKEY und SafeLOGIC-Funktionsumfang über X20MK-Konfigurator bestellen!	
	Erforderliches Zubehör	
	Zubehör	
X20MKXXXX.XXX.XXX	Für die SafeLOGIC der X20SL81xx bzw. X20cSL81xx Serie wird der für die Anwendung verfügbare Funktionsumfang durch das "Safety Technology Guarding" definiert. Der SafeKEY stellt dabei das Trägermedium für die Lizenzen dar. Der für die Anwendung benötigte Funktionsumfang muss durch eine Auswahl der verfügbaren SafeKEY Speichergröße bzw. coated und nicht-coated Variante und Technologiefunktionen im X20MK-Konfigurator zusammengestellt werden. Die Lieferung erfolgt ausschließlich im Set bestehend aus SafeKEY und den darauf freigeschalteten Lizenzen für die ausgewählten Technologiefunktionen.	

Tabelle 3: X20SL8100, X20cSL8100, X20SL8101, X20cSL8101, X20SL8110 - Bestelldaten

3 Technische Daten

Bestellnummer	X20SL8100	X20cSL8100	X20SL8101	X20cSL8101	X20SL8110
Kurzbeschreibung					
Schnittstellen	POWERLINK				
Systemmodul	Zentraleinheit				
Allgemeines					
Kühlung	Lüfterlos				
B&R ID-Code	0xDD61	0xE287	0xE649	0xE926	0xE64A
Systemvoraussetzungen					
Automation Studio	ab 4.0.16		ab 4.1.6		ab V4.2.5
Automation Runtime	ab V3.08 (für AsSafety Bibliothek ab F4.06)		ab F4.09, ab F4.10, ab A4.23		ab B4.25
SafeDESIGNER	ab 3.1.0		ab 4.1.0		ab V4.2
Safety Release	ab 1.7				ab 1.10
Statusanzeigen	CPU-Funktion, POWERLINK, SafeKEY				
Diagnose					
CPU Funktion	Ja, per Status-LED				
POWERLINK	Ja, per Status-LED				
SafeKEY	Ja, per Status-LED				
Leistungsaufnahme	4,3 W		5,3 W		3,9 W ¹⁾
Blackout-Modus					
Gültigkeitsbereich	-		Netzwerksegment		-
Funktion	-		Programmierbar		-
Standalone-Modus	-		Ja		-
Leistungsaufnahme für X2X Link Versorgung	-		1,42 W ²⁾		-
Leistungsaufnahme					
I/O-intern	-		0,6 W ²⁾		-
Potenzialtrennung					
Feldbus - X2X Link	-		Ja		-
Feldbus - I/O	-		Ja		-
Zulassungen					
CE	Ja				
EAC	Ja				
UL	cULus E115267 Industrial Control Equipment				cULus E115267 Industrial Control Equipment
HazLoc	cCSAus 244665 Process Control Equipment for Hazardous Locations Class I, Division 2, Groups ABCD, T5				-
ATEX	Zone 2, II 3G Ex nA nC IIA T5 Gc IP20, Ta (siehe X20 Anwenderhandbuch) FTZÚ 09 ATEX 0083X				
DNV GL	Temperature: A (0 - 45 °C) Humidity: B (up to 100%) Vibration: A (0.7 g) EMC: B (bridge and open deck)				In Vorbereitung
Functional Safety	cULus FSPC E361559 Energy and Industrial Systems Certified for Functional Safety ANSI UL 1998:2013				
Functional Safety	IEC 61508:2010, SIL 3 EN 62061:2013, SIL 3 EN ISO 13849-1:2015, Cat. 4 / PL e IEC 61511:2004, SIL 3				
Functional Safety	EN 50156-1:2004				
Sicherheitstechnische Kennwerte					
EN ISO 13849-1:2015					
Kategorie	KAT 4				
PL	PL e				
DC	>94%				
MTTFD	2500 Jahre				
Gebrauchsdauer	max. 20 Jahre				
IEC 61508:2010, IEC 61511:2004, EN 62061:2013					
SIL CL	SIL 3				
SFF	>90%				
PFH / PFH _d					
Modul	<1*10 ⁻¹⁰				
openSAFETY drahtgebunden	Vernachlässigbar				
openSAFETY drahtlos	<1*10 ⁻¹⁴ * Anzahl der openSAFETY Pakete je Stunde				
PFD	<2*10 ⁻⁵				
Proof Test Interval (PT)	20 Jahre				

Tabelle 4: X20SL8100, X20cSL8100, X20SL8101, X20cSL8101, X20SL8110 - Technische Daten

Bestellnummer	X20SL8100	X20cSL8100	X20SL8101	X20cSL8101	X20SL8110
Funktionalität					
Kommunikation untereinander	Ja				
Unterstützung von Maschinenoptionen					
BOOL	512				
INT	64				
UINT	64				
DINT	64				
UDINT	64				
Unterstützung von SafeMOTION	Ja, abhängig von den verfügbaren Funktionslizenzen am SafeKEY				
Zeitliche Genauigkeit	Zeit * 0,05 + Zykluszeit der Sicherheitsapplikation				
Kürzeste Taskklassen-Zykluszeit	1 ms				
max. Anzahl openSAFETY Nodes	100, abhängig von den verfügbaren Funktionslizenzen am SafeKEY		280, abhängig von den verfügbaren Funktionslizenzen am SafeKEY und den verfügbaren Ressourcen		
max. Anzahl POWERLINK Controlled Nodes	50		100		
Datenaustausch zwischen CPU und SL					
max. Gesamtdatenbreite pro Richtung	128 Byte				
max. Anzahl der Datenpunkte pro Richtung					
BOOL	352 (96 + 256 extended)				
INT	30				
UINT	30				
DINT	15				
UDINT	15				
Datenaustausch zwischen SL und SL					
max. Gesamtanzahl Datenpunkte pro Richtung ³⁾	16				
max. Anzahl der Datenpunkte pro Richtung					
BOOL	128				
INT	16				
UINT	16				
DINT	16				
UDINT	16				
Grenzwerte für SafeDESIGNER Applikation					
max. Ressourcen für SafeDESIGNER Info Fenster Angaben ⁴⁾					
FB-Instanzen	4096				
Merkerspeicher	131.072 Byte				
Stackspeicher	32.768 Byte				
Speicher für sichere Eingangsdaten	2048 Byte				
Speicher für sichere Ausgangsdaten	2048 Byte				
Speicher für funktionale Eingangsdaten	1024 Byte				
Speicher für funktionale Ausgangsdaten	1024 Byte				
Merkerzähler	8192				
weitere SafeDESIGNER Grenzwerte					
max. Anzahl Funktionsbaustein-Typen	512				
max. Anzahl Force-Variablen	64				
max. Anzahl Variablen im Variablen-Status	1023				
Eingang SL / BC / X2X Link Versorgung					
Eingangsspannung	24 VDC -15% / +20%				
Eingangsstrom	max. 0,25 A		max. 0,9 A		max. 0,25 A
Sicherung	-		Integriert, nicht tauschbar		-
Verpolungsschutz	Ja				
Ausgang SL / BC / X2X Link Versorgung					
Ausgangsnennleistung	-		7 W		-
Parallelschaltung	-		Ja ⁵⁾		-
Redundanzbetrieb	-		Ja		-
Überlastverhalten	-		Kurzschlussfest, kurzzeitige Überlast		-
Eingang I/O-Versorgung					
Eingangsspannung	-		24 VDC -15% / +20%		-
Sicherung	-		Erforderliche Vorsicherung max. T 10 A		-
Verpolungsschutz	-		Ja		-
Ausgang I/O-Versorgung					
Ausgangsnennspannung	-		24 VDC		-
Verhalten bei Kurzschluss	-		Erforderliche Vorsicherung		-
Zulässige Kontaktbelastung	-		10 A		-

Tabelle 4: X20SL8100, X20cSL8100, X20SL8101, X20cSL8101, X20SL8110 - Technische Daten

Bestellnummer	X20SL8100	X20cSL8100	X20SL8101	X20cSL8101	X20SL8110
Schnittstellen					
Feldbus	POWERLINK Controlled Node				
Typ	Typ 3 ⁶⁾				
Ausführung	2x geschirmter RJ45-Port (Hub)				
Leitungslänge	max. 100 m zwischen 2 Knoten (Segmentlänge)				
Übertragungsrate	100 MBit/s				
Übertragung	100 BASE-TX				
Physik	100 BASE-TX				
Halbduplex	Ja				
Voll duplex	Nein				
Autonegotiation	Ja				
Auto-MDI/MDIX	Ja				
Min. Zykluszeit ⁷⁾	200 µs				
Feldbus	200 µs				
X2X Link	-		200 µs		-
Synchronisation zw. Bussen möglich	-		Ja		-
Einsatzbedingungen					
Einbaulage					
waagrecht	Ja				
senkrecht	Ja				
Aufstellungshöhe über NN (Meeresspiegel)	0 bis 2000 m, keine Einschränkung				
Schutzart nach EN 60529	IP20				
Umgebungsbedingungen					
Temperatur					
Betrieb					
waagrechte Einbaulage	0 bis 60°C	-40 bis 60°C ⁸⁾	0 bis 60°C	-40 bis 60°C ⁹⁾	0 bis 60°C
senkrechte Einbaulage	0 bis 45°C	-40 bis 45°C ¹⁰⁾	0 bis 45°C	-40 bis 45°C ¹¹⁾	0 bis 45°C
Derating	- Siehe Abschnitt "Derating"				-
Lagerung	-40 bis 85°C				
Transport	-40 bis 85°C				
Luftfeuchtigkeit					
Betrieb	5 bis 95%, nicht kondensierend	Bis 100%, kondensierend	5 bis 95%, nicht kondensierend	Bis 100%, kondensierend	5 bis 95%, nicht kondensierend
Lagerung	5 bis 95%, nicht kondensierend				
Transport	5 bis 95%, nicht kondensierend				
Mechanische Eigenschaften					
Anmerkung	SafeKEY und SafeLOGIC-Funktionsumfang über X20MK-Konfigurator bestellen X20 Abschlussplatte rechts ist im Lieferumfang enthalten X20 Feldklemme 12-polig, Safety codiert, ist im Lieferumfang enthalten SafeKEY Abdeckung ist im Lieferumfang enthalten				
Abmessungen					
Breite	62,5 ^{+0,2} mm				
Höhe	99 mm				
Tiefe	75 mm				
Gewicht	190 g				

Tabelle 4: X20SL8100, X20cSL8100, X20SL8101, X20cSL8101, X20SL8110 - Technische Daten

- 1) Leistungsaufnahme ohne Schnittstellenmodul
- 2) Die angegebenen Werte sind Maximalangaben. Beispiele für die genaue Berechnung sind im X20 System Anwenderhandbuch im Abschnitt "Mechanische und elektrische Konfiguration" zu finden.
- 3) Es ist zu beachten, dass jeweils 8 BOOL als 1 Datenpunkt zählen.
- 4) Parameterbeschreibung siehe Dokumentation SafeDESIGNER, Abschnitt "Meldungsfenster".
- 5) Im Parallelbetrieb darf nur mit 75% Nennleistung gerechnet werden. Es ist darauf zu achten, dass alle parallel betriebenen Netzteile gleichzeitig ein- bzw. ausgeschaltet werden.
- 6) Siehe Automation Help unter "Kommunikation, POWERLINK, Allgemeines, Hardware - CN" für weitere Informationen. Es ist jedoch zu beachten, dass die SafeLOGIC "Vorgezogenes Schreiben der Ausgangsdaten" nicht unterstützt. Der Einsatz von "PollResponse Chaining" wird für Controlled Nodes im selben POWERLINK-Strang nicht empfohlen.
- 7) Die minimale Zykluszeit gibt an, bis zu welcher Zeit der Buszyklus heruntergefahren werden kann, ohne dass Kommunikationsfehler auftreten.
- 8) Bis Hardware-Upgrade <1.10.5.0 und Hardware-Revision <F0: -25 bis 60°C
- 9) Bis Hardware-Upgrade <1.10.5.0 und Hardware-Revision <E0: -25 bis 60°C
- 10) Bis Hardware-Upgrade <1.10.5.0 und Hardware-Revision <F0: -25 bis 45°C
- 11) Bis Hardware-Upgrade <1.10.5.0 und Hardware-Revision <E0: -25 bis 45°C

Gefahr!

Der Betrieb außerhalb der technischen Daten ist nicht zulässig und kann zu gefährlichen Zuständen führen.

Information:

Nähere Informationen zur Installation sind Kapitel "Installationshinweise X20-Module" auf Seite 78 zu entnehmen.

X20SL8101: Derating für SafeLOGIC / Bus Controller / X2X Link Versorgung

Die Ausgangsnennleistung der X2X Link Versorgung ist 7 W.

Die Ausgangsnennleistung ist abhängig von der Betriebstemperatur und der Einbaulage. Die resultierende Ausgangsnennleistung kann der folgenden Tabelle entnommen werden.

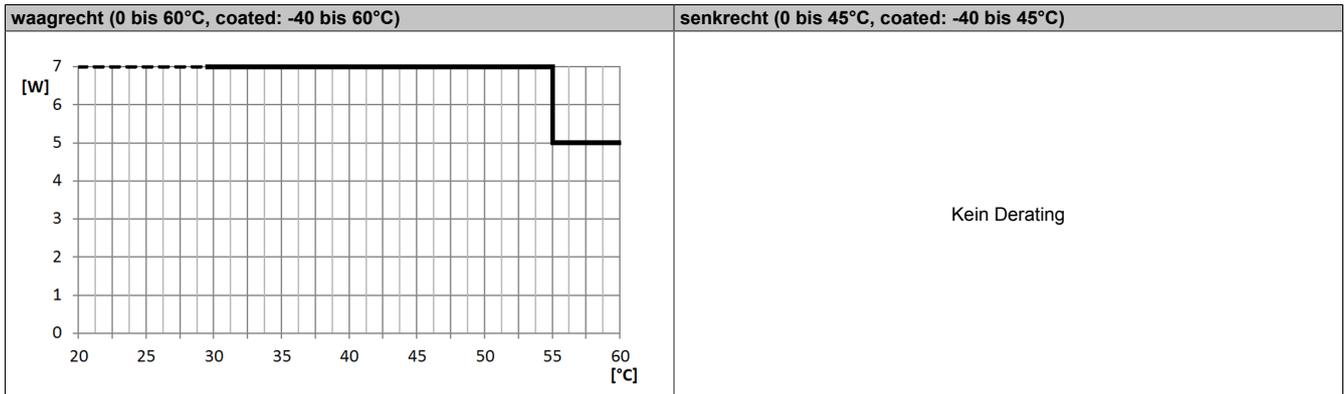


Tabelle 5: Derating für SafeLOGIC / Bus Controller / X2X Link Versorgung

Information:

Unabhängig von den in der Derating-Kurve angegebenen Werten ist der Betrieb der Module auf die in den technischen Daten angegebenen Werte beschränkt.

4 Bedien- und Anschlusselemente

Für die Bedienung der SafeLOGIC sind LEDs und Taster/Schalter vorgesehen. Mit diesen Elementen können folgende Aktionen bedient werden:

- Tauschen eines Moduls inkl. Überprüfen der gesamten Modulkonfiguration (Kapitel "Tauschen von Modulen")
- Tauschen der Firmware (Kapitel "Bestätigung eines Firmware-Tauschs")
- Tauschen des SafeKEYs, evtl. inklusive Übernahme der Modulkonfiguration vom alten SafeKEY (Kapitel "Austauschen der Applikation an der SafeLOGIC mittels SafeKEY Tausch (nur X20SL8xxx Serie)")
- Tauschen der SafeLOGIC (Kapitel "Tauschen einer SafeLOGIC")

Mit Hilfe der AsSafety Bibliothek (Kapitel "Bedienung über AsSafety Bibliothek") kann auch eine Bedienung der SafeLOGIC über eine Visualisierung realisiert werden.

Eine SafeLOGIC verfügt über folgende Bedien- und Anschlusselemente:

X20SL810x

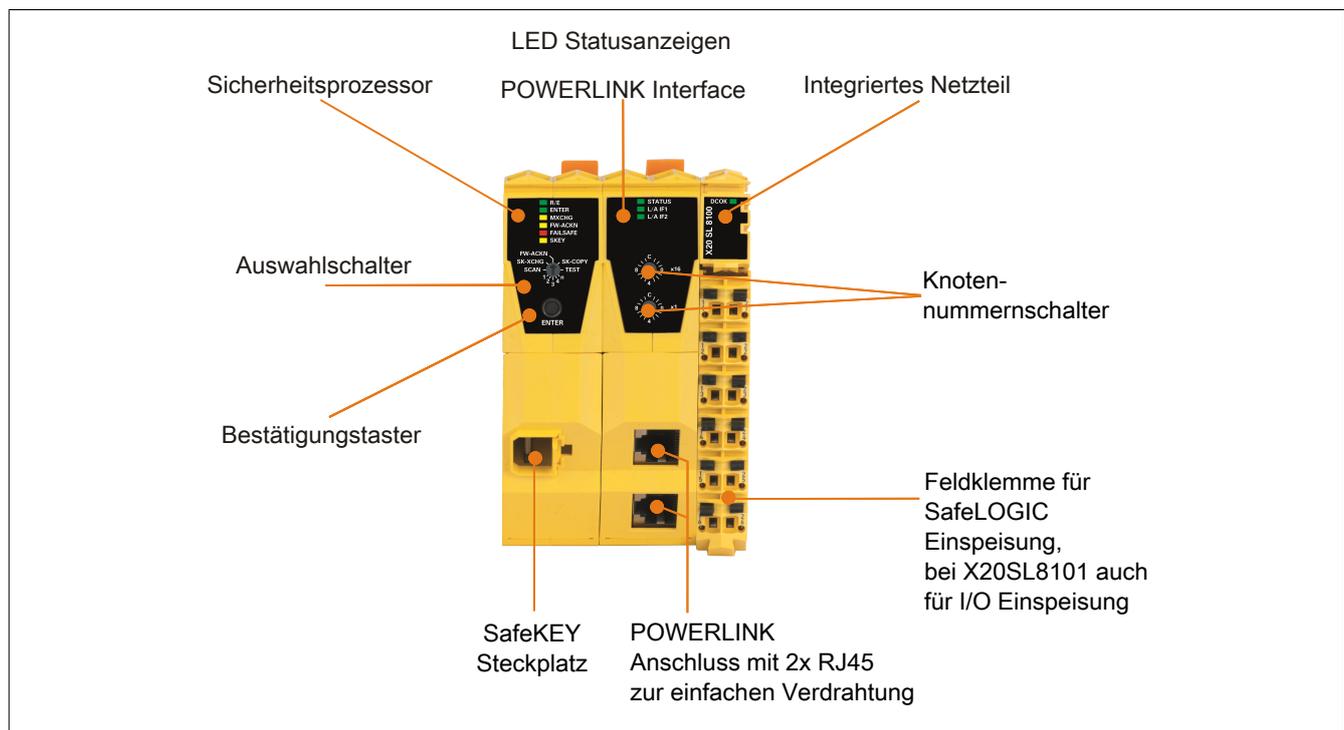


Abbildung 1: X20SL810x Bedienelemente

X20SL8110

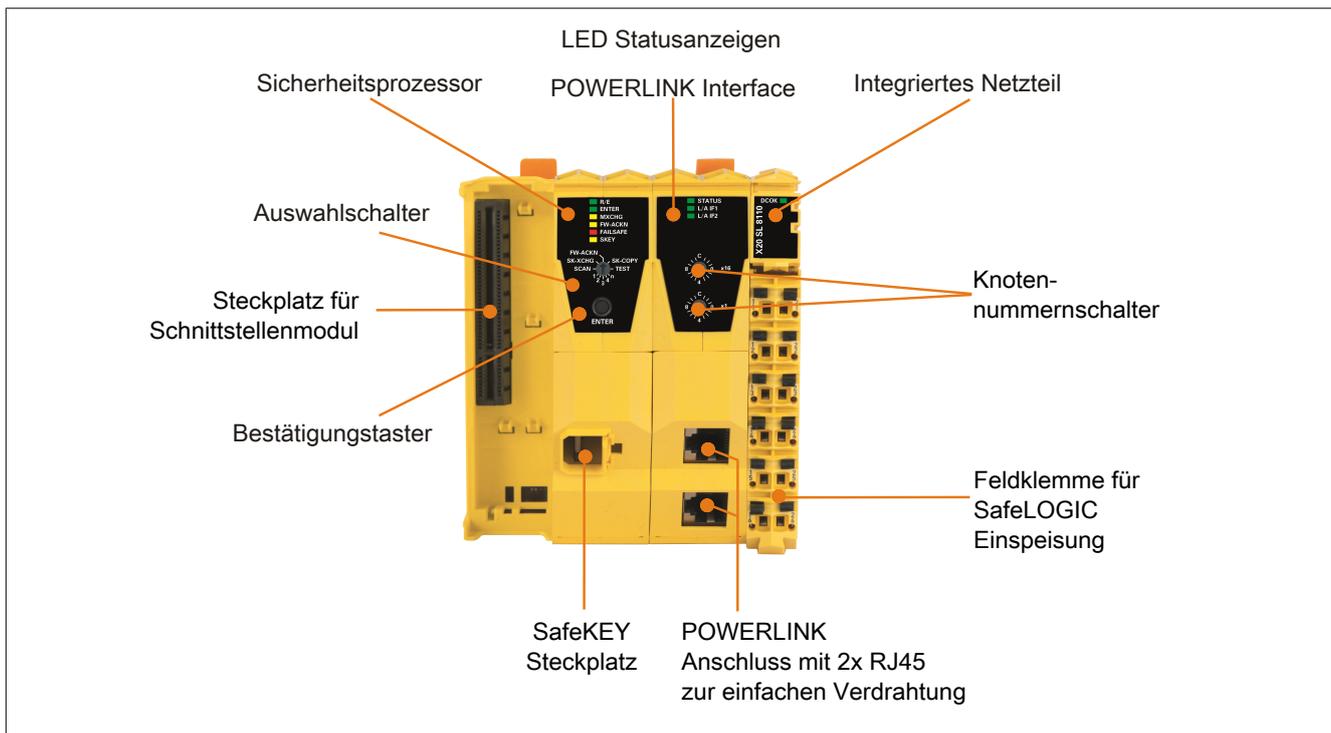


Abbildung 2: X20SL8110 Bedienelemente

Steckplatz für Schnittstellenmodule

Die SafeLOGIC X20SL8110 ist mit einem Steckplatz für Schnittstellenmodule ausgestattet.

Durch Auswahl des entsprechenden Schnittstellenmoduls lassen sich flexibel verschiedene Bus- bzw. Netzwerke in das X20 System integrieren.

Folgende Schnittstellenmodule können in der SafeLOGIC X20SL8110 betrieben werden:

Modul	Beschreibung
X20IF10E3-1	X20 Schnittstellenmodul für DTM-Konfiguration, 1 PROFINET RT Device (Slave) Schnittstelle, potenzialgetrennt

4.1 Sicherheitsprozessor

4.1.1 Status LEDs des Sicherheitsprozessors



LED	Farbe	Status	Beschreibung
R/E	Grün	Aus	Hochlaufphase
		Ein	Applikation ist vorhanden und wird abgearbeitet.
		Blinkend	Applikation ist 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). Zusätzlich sind die Bootstates 0x1840 bis 0x3440 unter Index:Subindex 0x2410:0x01 in Abschnitt "Kanalliste der SafeLOGIC" zu prüfen.
	Orange	Ein	SafeDESIGNER ist im "Debug" Mode.
		Blinken mit 0,5 Hz Blinken mit 1 Hz	SafeDESIGNER ist im "Debug" Mode, Applikation im "Stop". Keine Applikation am SafeKEY vorhanden
ENTER	Grün	Ein	Fehlende Autorisierung - siehe "Autorisierung (nur X20SL8xxx Serie)"
		1x Blinken für 0,8 s	Bestätigung einer korrekten Eingabe
		Blinkend (1 Hz) für 5 sec.	Fehlbedienung
MXCHG	Orange	Aus	Modulkonfiguration OK
			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, siehe Abschnitt "Status LEDs für das POWERLINK Interface", kontrollieren!)
FAILSAFE	Rot	Aus	Safety Firmware OPERATIONAL State
			Bootphase
			Safety Firmware PRE_OPERATIONAL State oder "SafeOSstate!=RUN"
			Sicherer Kommunikationskanal nicht OK, openSAFETY Connection Valid Problem oder "SafeOSstate!=RUN" Verbleibt die SafeLOGIC für eine längere Zeit in diesem Zustand, so ist der Parameter "Default Safe Data Duration" der "Gruppe: Safety Response Time Defaults" zu kontrollieren.
			Bootphase, fehlerhafte Firmware, Setup-Modus aktiv (ab Hardware-Upgrade 1.10.2.x) Details bzgl. Setup-Modus sind Abschnitt "Setup-Modus" zu entnehmen.

Tabelle 6: Statusanzeige Sicherheitsprozessor

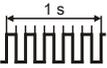
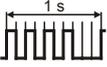
			Test- bzw. Pilot-Firmware oder Safety Applikation mit Test- bzw. Pilot-Version des SafeDESIGNER erstellt
			SafeDESIGNER im "Debug" Mode
		Ein	Gesamtmodul betreffender Sicherheitszustand aktiv (= Zustand "FailSafe")
		Aus	Kein Zugriff auf den SafeKEY
SKEY	Orange	Blinkend	Zugriff auf den SafeKEY

Tabelle 6: Statusanzeige Sicherheitsprozessor

Gefahr!

Eine statisch leuchtende FAILSAFE LED signalisiert einen möglicherweise sicherheitsrelevanten Systemfehler.

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

4.1.2 LED-Test

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

- Auswahlschalter auf TEST stellen
- Bestätigungstaster ENTER drücken
- Exakt für die Dauer der Betätigung des Bestätigungstasters werden alle LEDs des Sicherheitsprozessors (linkes Modul der SafeLOGIC) eingeschaltet.

4.1.3 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 3: Auswahlschalter und Bestätigungstaster

Schalterstellung	Funktionalität	Beschreibung
FW-ACKN	Firmware Acknowledge	Bestätigung Firmware-Tausch bei einem oder mehreren Modulen ¹⁾
unbeschriftete Position zwischen FW-ACKN und SK-COPY (=0xD)	Setup-Modus (ab Hardware-Upgrade 1.10.2.x)	Setup-Modus aktivieren/deaktivieren Details bzgl. Setup-Modus sind Abschnitt "Setup-Modus" zu entnehmen.
SK-COPY	SafeKEY Copy	Kopieren der Konfigurationsdaten vom SafeKEY ²⁾
TEST	Test	Durchführung eines LED-Tests
unbeschriftete Position zwischen TEST und n	CLEAR DATA	Löschen folgender "User Daten": <ul style="list-style-type: none"> • Remanente Daten • Konfigurationsdatei der funktionalen Applikation • Erweiterte Maschinenoptionen • Tabellenobjekte • Nachladbare Parameterdatei - ab Firmware-Version V322
1,2,3,4,n	Modultausch	Tausch von 1, 2, 3, 4 oder mehr als 4 Modulen bestätigen
SCAN	Scannen	Auslösen eines Modul-Scans
SK-XCHG	SafeKEY Exchange	Bestätigung SafeKEY Tausch ¹⁾
unbeschriftete Position zwischen FW-ACKN und SK-XCHG	SafeKEY Format	SafeKEY formatieren (ab Release 1.4) ²⁾

Tabelle 7: Bestätigungsmodi

- 1) Für Firmware-Versionen $\leq V322$ wird ein Neustart ausgelöst.
- 2) Löst einen automatischen Neustart aus.

Bestätigung (alle Funktionen außer "SafeKEY Format")

Für eine Bestätigung muss der Bestätigungstaster für eine Dauer von 0,5 bis 5 s gedrückt werden. Nach 0,5 s beginnt die LED ENTER (siehe Kapitel "Status LEDs des Sicherheitsprozessors") 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. Soll z. B. der Modultausch von genau einem Modul bestätigt werden, dann muss der Auswahlschalter auf der Stellung "1" stehen (siehe Kapitel "Tauschen eines einzelnen Moduls"). 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 bis 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.

4.2 Steckplatz für Programmspeicher (SafeKEY)

Zum Betrieb der SafeLOGIC ist ein Programmspeicher (SafeKEY) zum Speichern des Programms, der Parameter und der Systemkonfiguration erforderlich.

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

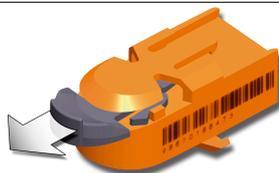


Abbildung 4: SafeKEY entriegelt

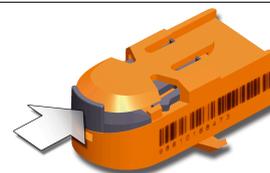


Abbildung 5: SafeKEY verriegelt

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.

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

Information:

Es ist zu berücksichtigen, dass Module, welche am lokalen X2X der X20SL8101 betrieben werden, nur richtig konfiguriert werden, wenn ein gültiges Safety-Projekt am SafeKEY vorliegt. Andernfalls bleibt "ModuleOk" im Automation Studio auf FALSE.

4.3 POWERLINK Interface

4.3.1 Status LEDs für das POWERLINK Interface

Abbildung	LED	Farbe	Status	Beschreibung
	STATUS ¹⁾	Grün/Rot		Status/Error LED; Die LED Stati sind im Abschnitt 4.3.2 "LED "STATUS"" 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 8: Statusanzeige POWERLINK Interface

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

4.3.2 LED "STATUS"

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

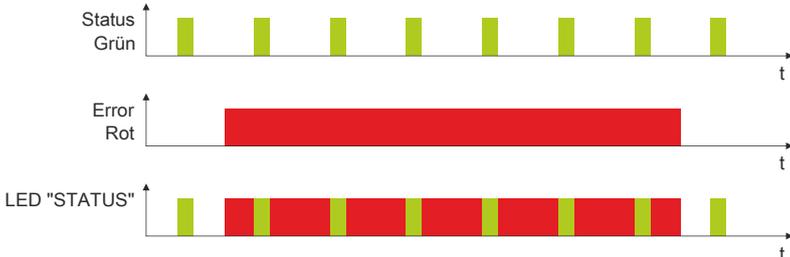
Farbe rot - Error	Beschreibung
Ein	<p>Der Controlled Node (CN) befindet sich in einem Fehlerzustand (Ausfall von Ethernet Frames, Häufung von Kollisionen am Netzwerk usw.). Wenn in den folgenden Zuständen ein Fehler auftritt, wird die rote LED von der grün blinkenden LED überlagert:</p> <ul style="list-style-type: none"> • PRE_OPERATIONAL_1 • PRE_OPERATIONAL_2 • READY_TO_OPERATE  <p>Anmerkung:</p> <ul style="list-style-type: none"> • Direkt nach dem Einschalten werden einige rote Blinksignale angezeigt. Dabei handelt es sich aber um keine Fehler. • Bei CN mit der eingestellten physikalischen Knotennummer 0, welchen noch keine Knotennummer per Dynamic Node Allocation (DNA) zugewiesen wurde, leuchtet die LED rot.

Tabelle 9: Status/Error-LED leuchtet rot: LED zeigt Fehlerzustand an

Farbe grün - Status	Beschreibung
Aus	Keine Versorgung oder Modus NOT_ACTIVE. Der Controlled Node (CN) ist entweder nicht versorgt oder befindet sich im Zustand NOT_ACTIVE. In diesem Zustand wartet der CN nach einem Neustart ungefähr 5 s. Es ist keine Kommunikation mit dem CN möglich. Wird in diesen 5 s keine POWERLINK-Kommunikation erkannt, geht der CN in den Zustand BASIC_ETHERNET über (flackernd). Wenn jedoch vor Ablauf der Zeit eine POWERLINK-Kommunikation erkannt wird, geht der CN direkt in den Zustand PRE_OPERATIONAL_1 über.
Grün flackernd (ca. 10 Hz)	Modus BASIC_ETHERNET. Der CN hat keine POWERLINK-Kommunikation erkannt. In diesem Zustand ist es möglich, mit dem CN direkt (z. B. mit UDP, IP usw.) zu kommunizieren. Wird während dieses Zustands eine POWERLINK-Kommunikation erkannt, geht der CN in den Zustand PRE_OPERATIONAL_1 über.
Single Flash (ca. 1 Hz)	Modus PRE_OPERATIONAL_1. Der CN wartet auf den Empfang eines SoC-Frames und wechselt dann in den Zustand PRE_OPERATIONAL_2.
Double Flash (ca. 1 Hz)	Modus PRE_OPERATIONAL_2. In diesem Zustand wird der CN üblicherweise vom Manager konfiguriert. Danach wird der CN per Kommando in den Zustand READY_TO_OPERATE weitergeschaltet.
Tripple Flash (ca. 1 Hz)	Modus READY_TO_OPERATE. Der CN wird vom Manager per Kommando in den Zustand OPERATIONAL weitergeschaltet.
Ein	Modus OPERATIONAL. PDO-Mapping ist aktiv und zyklische Daten werden ausgewertet.
Blinkend (ca. 2,5 Hz)	Modus STOPPED. Ausgangsdaten werden nicht ausgegeben und es werden keine Eingangsdaten geliefert. Dieser Zustand kann nur durch ein entsprechendes Kommando vom Manager erreicht und wieder verlassen werden.

Tabelle 10: Status/Error-LED leuchtet grün: LED zeigt Betriebszustand an

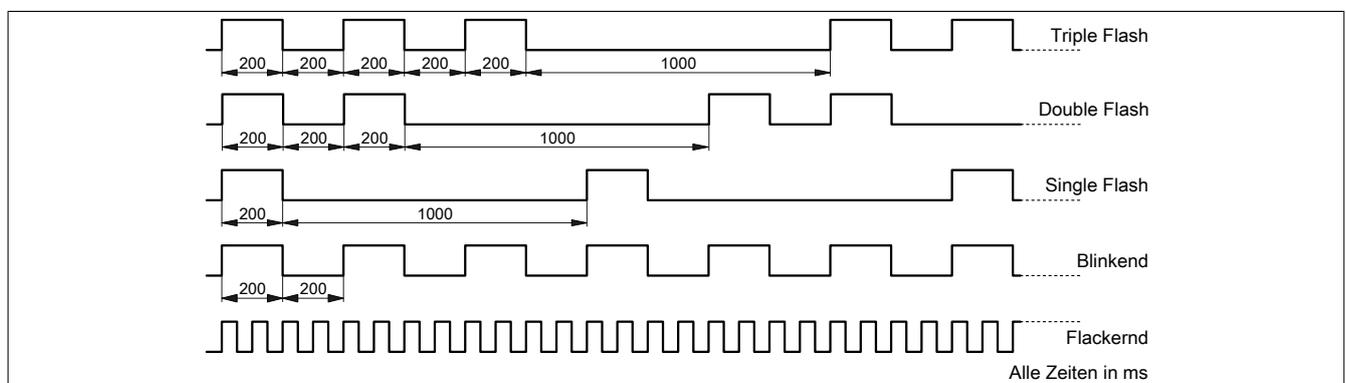


Abbildung 6: Status-LEDs - Blinkzeiten

4.3.3 POWERLINK Stationsnummer

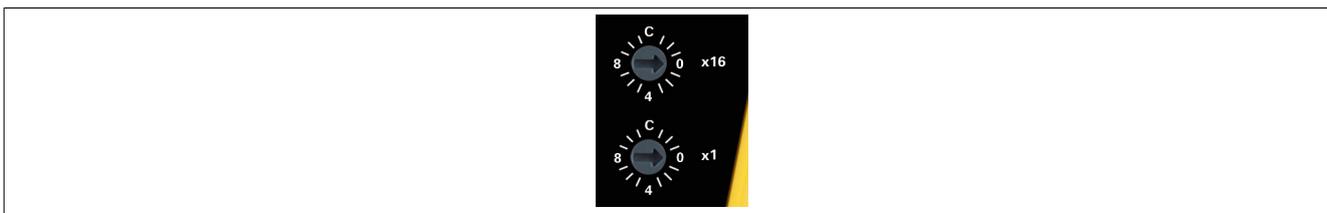


Abbildung 7: POWERLINK Stationsnummernschalter

Mittels der beiden Nummernschalter wird die Stationsnummer der POWERLINK Station eingestellt. Stationsnummern im Bereich 0x01 bis 0xEF sind erlaubt.

Schalterstellung	Beschreibung
0x00	Reserviert; Schalterstellung ist nicht erlaubt.
0x01 bis 0xEF	Stationsnummer der POWERLINK Station; Betrieb als Controlled Node (CN).
0xF0 bis 0xFF	Reserviert; Schalterstellung ist nicht erlaubt.

Tabelle 11: Stationsnummer POWERLINK

4.3.4 RJ45 Ports

Hinweise für die Verkabelung von X20 Modulen mit Ethernet-Schnittstelle sind im X20 Anwenderhandbuch, Abschnitt "Mechanische und elektrische Konfiguration - Verkabelungsvorschrift für X20 Module mit Ethernet Kabel" zu finden.

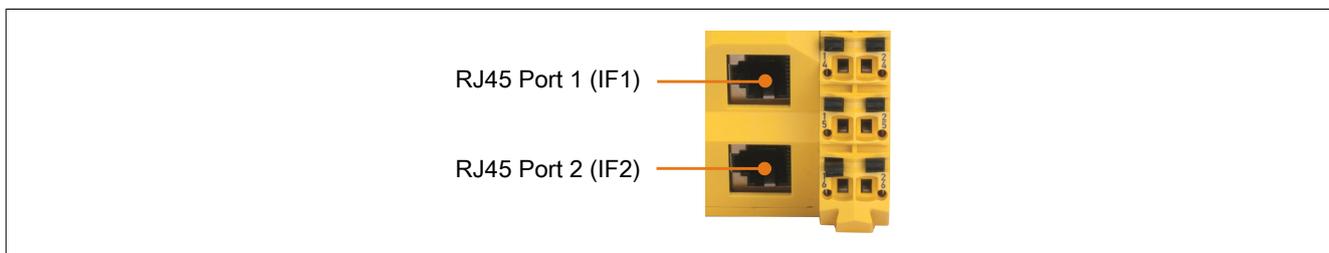


Abbildung 8: RJ45 Ports

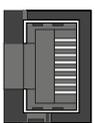
Schnittstelle	Anschlussbelegung		
	Pin	Ethernet	
 Geschirmter RJ45 Port	1	RXD	Empfange (Receive) Daten
	2	RXD\	Empfange (Receive) Daten\
	3	TXD	Sende (Transmit) Daten
	4	Termination	
	5	Termination	
	6	TXD\	Sende (Transmit) Daten\
	7	Termination	
	8	Termination	

Tabelle 12: Pinbelegung für RJ45 Port

4.4 SG Unterstützung

SG3 / SGC

Die SafeLOGIC wird zurzeit 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 Firmware-Version auf der funktionalen CPU hinterlegt.

Bei unterschiedlicher Firmware-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 Firmware-Tauschs](#)" angeführten Maßnahmen durchzuführen.

4.5 Integriertes Netzteil

Für die Versorgung der SafeLOGIC ist ein Netzteil integriert.

4.5.1 Status LEDs für integriertes Netzteil

X20SL81x0

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

Tabelle 13: X20SL81x0 - Statusanzeige integriertes Netzteil

X20SL8101

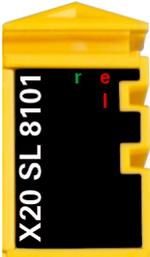
Abbildung	LED	Farbe	Status	Beschreibung
	r	Grün	Aus	Modul nicht versorgt
			Single Flash	Modus RESET
			Blinkend	Modus PREOPERATIONAL
			Ein	Modus RUN
	e	Rot	Aus	Modul nicht versorgt oder alles in Ordnung
			Double Flash	LED zeigt einen der folgenden Zustände an: <ul style="list-style-type: none"> Die SafeLOGIC / Bus Controller / X2X Link Versorgung des Netzteils ist überlastet I/O Versorgung zu niedrig Eingangsspannung für SafeLOGIC / Bus Controller / X2X Link Versorgung zu niedrig
	e + r		Rot Ein / Grüner Single Flash	Firmware ist ungültig
l	Rot	Aus	Die SafeLOGIC / Bus Controller / X2X Link Versorgung liegt im gültigen Bereich.	
		Ein	Die SafeLOGIC / Bus Controller / X2X Link Versorgung des Netzteils ist überlastet.	

Tabelle 14: X20SL8101 - Statusanzeige integriertes Netzteil

4.5.2 Anschlussbelegungen für das integrierte Netzteil

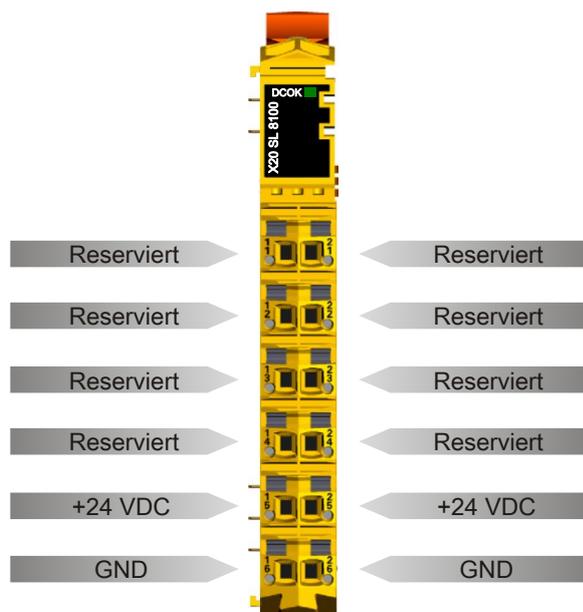


Abbildung 9: X20SL81x0 - Anschlussbelegung des integrierten Netzteils

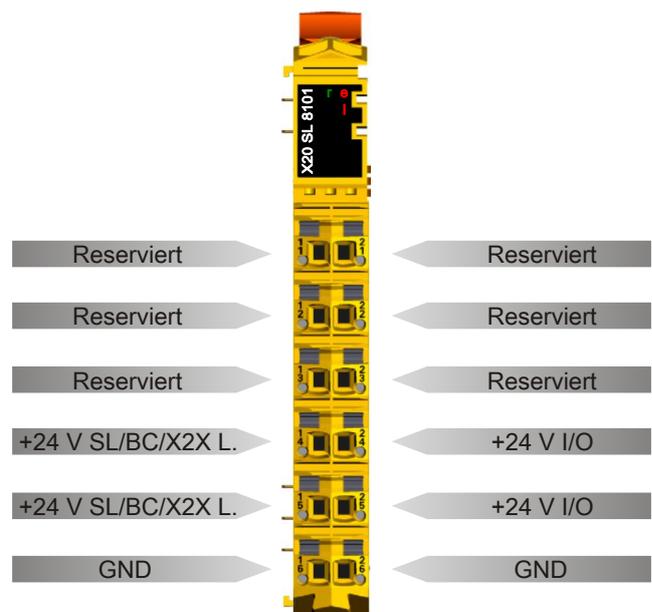


Abbildung 10: X20SL8101 - Anschlussbelegung des integrierten Netzteils

4.5.3 Anschlussbeispiele

X20SL81x0

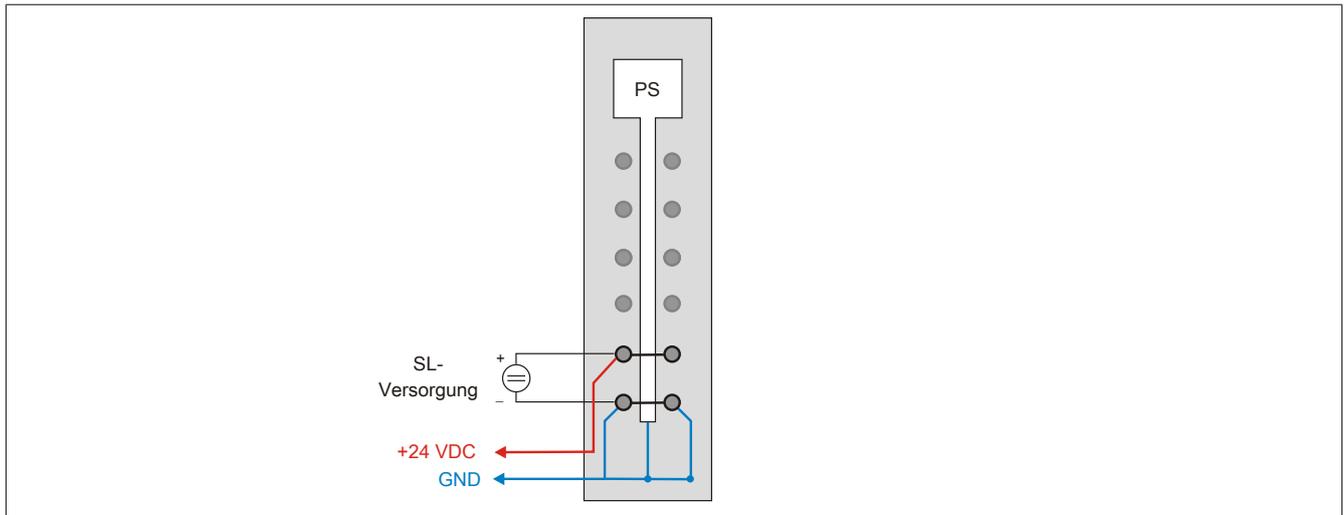


Abbildung 11: X20SL81x0 - Anschlussbeispiel

X20SL8101 - Mit 2 getrennten Versorgungen

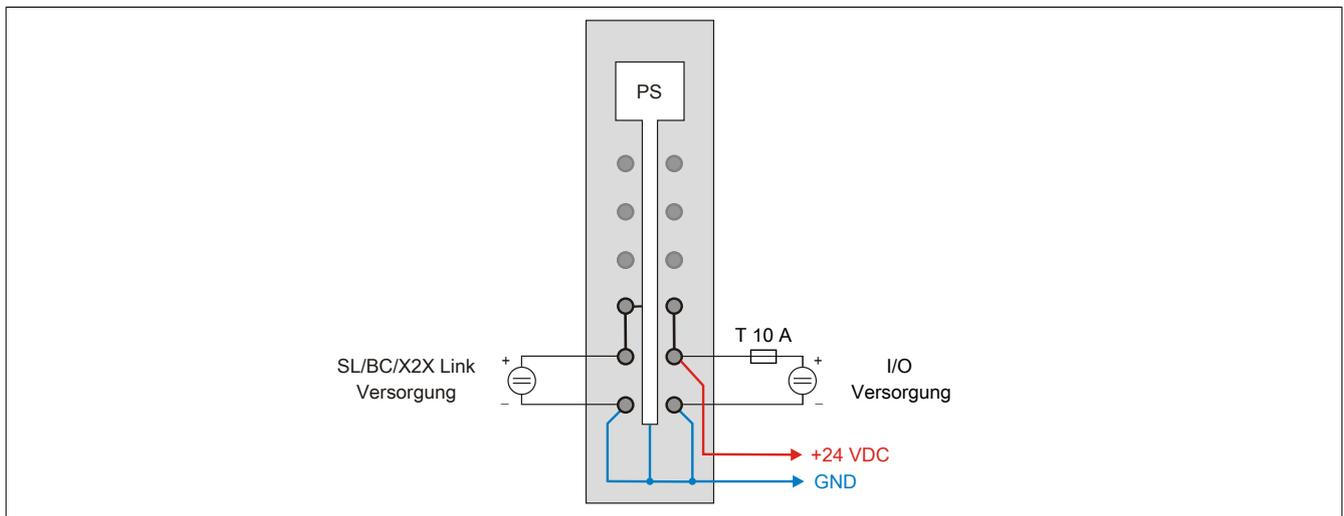


Abbildung 12: X20SL8101 - Anschlussbeispiel mit 2 getrennten Versorgungen

X20SL8101 - Mit einer Versorgung und Drahtbrücke

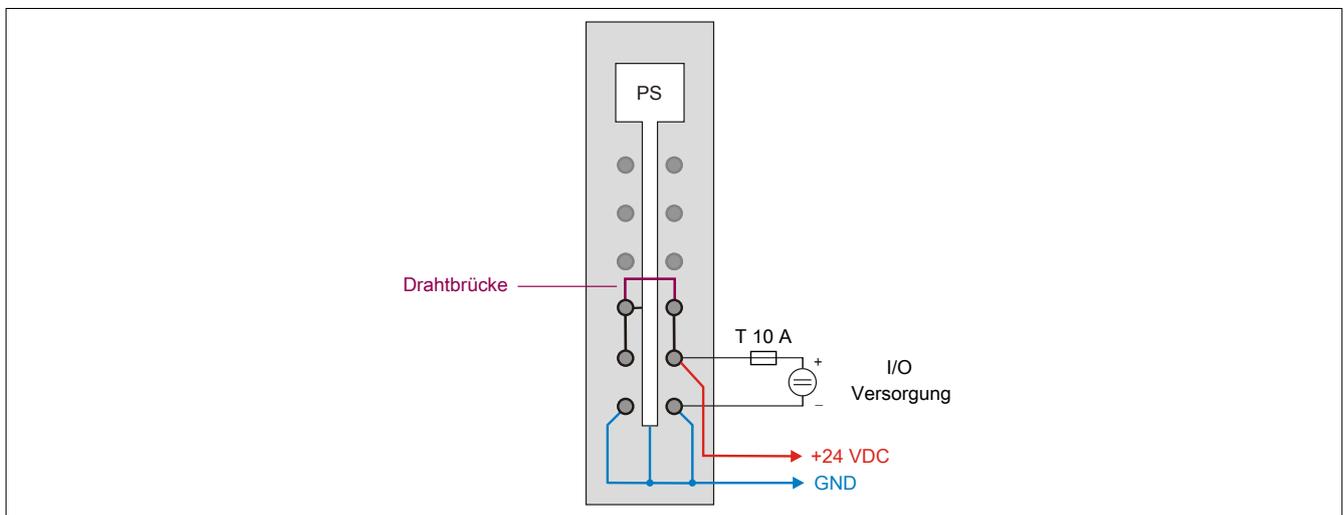


Abbildung 13: X20SL8101 - Anschlussbeispiel mit einer Versorgung und Drahtbrücke

5 Registerbeschreibung

5.1 Parameter in der I/O Konfiguration

Gruppe: POWERLINK parameters

Parameter	Beschreibung	Default Wert	Einheit
Mode	Die SafeLOGIC kann nur als "controlled node" (CN) betrieben werden. Der "managing node" (MN) wird nicht unterstützt.	controlled node	-

Tabelle 15: Parameter I/O Konfiguration: POWERLINK parameters

Information:

Es stehen zusätzliche Konfigurationsparameter zur Verfügung.

Details dazu siehe Automation Help unter "Kommunikation -> POWERLINK -> AR-Konfiguration -> POWERLINK Controlled Node Konfiguration (SG4)".

Gruppe: Function model

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

Tabelle 16: Parameter I/O Konfiguration: Function model

Gruppe: General

Parameter	Beschreibung	Default Wert	Einheit
Module supervised	Systemverhalten bei fehlendem Modul	On	-
	Parameter Wert	Beschreibung	
	On	Fehlendes Modul löst Service Mode aus	
	Off	Fehlendes Modul wird ignoriert	
Interface Slot Enable (nur X20SL8110, ab Hardware-Upgrade 1.10.1.3)	Dieser Parameter aktiviert die Datenübertragung an der Schnittstellenkarte.	On	-
	Parameter Wert	Beschreibung	
	On	Die Datenübertragung an der Schnittstellenkarte ist aktiviert.	
	Off	Die Datenübertragung an der Schnittstellenkarte ist deaktiviert.	
Node used as IP gateway	Dieser Parameter ist für zukünftige Funktionserweiterungen reserviert.	240	-
Standalone mode (nur X20SL8101, ab Hardware-Upgrade 1.10.2.x und Automation Runtime A4.32)	Dieser Parameter aktiviert den Standalone-Modus (siehe Abschnitt Blackout-Modus in der Automation Help unter: Hardware → X20 System → Zusätzliche Informationen → Blackout-Modus) und ermöglicht ein Hochfahren der SafeLOGIC ohne aktiven Master.	Off	-
	Parameter Wert	Beschreibung	
	On	Der Standalone-Modus ist aktiviert.	
	Off	Der Standalone-Modus ist deaktiviert.	
SafeLOGIC ID	Bei Applikationen mit mehreren SafeLOGICen legt dieser Parameter die eindeutige SafeLOGIC Adresse fest. <ul style="list-style-type: none"> Erlaubte Werte: 1 bis 1024 	wird automatisch vergeben	-
SafeMODULE ID	Eindeutige Safety Adresse des Moduls <ul style="list-style-type: none"> Erlaubte Werte: 1 	1	-
SafeDESIGNER project	Name des Sicherheitsprojekts	wird automatisch vergeben	-
SafeDESIGNER version	SafeDESIGNER Version für das Sicherheitsprojekt dieser SafeLOGIC	wird automatisch vergeben	-
Authorization	Aktivierung der Funktion "Autorisierung" - siehe "Autorisierung (nur X20SL8xxx Serie)".	Disabled	-
	Parameter Wert	Beschreibung	
	Enabled	Funktion "Autorisierung" ist aktiviert; funktionale CPU kann Quittier-Aktionen der SafeLOGIC blockieren	
	Disabled	Funktion "Autorisierung" ist deaktiviert; kein Einfluss der funktionalen CPU auf die Quittier-Funktionen	

Tabelle 17: 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	On	-
Server communication port	TCP/IP Portnummer, über die die SafeLOGIC erreichbar ist <ul style="list-style-type: none"> Empfohlene Werte: 50.000 bis 50.100 Hinweis: Wenn mehrere SafeLOGICen im Projekt vorhanden sind, muss für jede SafeLOGIC eine andere Portnummer eingestellt werden!	50000	-

Tabelle 18: 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 30; 	0	-
Number of UINT channels	Anzahl der UINT Kanäle von der CPU zur SafeLOGIC <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 30; 	0	-
Number of DINT channels (Safety Release 1.4 und Automation Runtime V3.08 erforderlich)	Anzahl der DINT Kanäle von der CPU zur SafeLOGIC <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 15; 	0	-
Number of UDINT channels	Anzahl der UDINT Kanäle von der CPU zur SafeLOGIC <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 15; 	0	-

Tabelle 19: 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 30; 	0	-
Number of UINT channels	Anzahl der UINT Kanäle von der SafeLOGIC zur CPU <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 30; 	0	-
Number of DINT channels (Safety Release 1.4 und Automation Runtime V3.08 erforderlich)	Anzahl der DINT Kanäle von der SafeLOGIC zur CPU <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 15; 	0	-
Number of UDINT channels	Anzahl der UDINT Kanäle von der SafeLOGIC zur CPU <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 15; 	0	-

Tabelle 20: 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.	Off	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>On</td> <td>Diese SafeLOGIC steht als Datenquelle für eine weitere SafeLOGIC zur Verfügung.</td> </tr> <tr> <td>Off</td> <td>Diese SafeLOGIC steht nicht als Datenquelle für weitere SafeLOGICen zur Verfügung.</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	On	Diese SafeLOGIC steht als Datenquelle für eine weitere SafeLOGIC zur Verfügung.	Off	Diese SafeLOGIC steht nicht als Datenquelle für weitere SafeLOGICen zur Verfügung.
	Parameter Wert	Beschreibung							
On	Diese SafeLOGIC steht als Datenquelle für eine weitere SafeLOGIC zur Verfügung.								
Off	Diese SafeLOGIC steht nicht als Datenquelle für weitere SafeLOGICen zur Verfügung.								
Extended source SafeLOGIC communication (Safety Release 1.4 und Automation Runtime V3.08 erforderlich)	Aktiviert die Möglichkeit, die Anzahl der Datenpunkte der SafeLOGIC to SafeLOGIC communication zu parametrieren (für Verbindungen bei denen diese SafeLOGIC als Datenquelle für eine weitere SafeLOGIC dient).	Off	-						
Gruppe: Connected SafeLOGIC modules (ab Safety Release 1.4)									
Gruppe: Connection xx Parametrierung der maximalen SafeLOGICen zu denen diese SafeLOGIC eine Verbindung aufbaut.									
SafeLOGIC ID of connection xx	SafeLOGIC ID zu der eine Verbindung aufgebaut werden soll	0	-						
Gruppe: Output channels (Safety Release 1.4 und Automation Runtime 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 Automation Runtime 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 21: Parameter I/O Konfiguration: SafeLOGIC to SafeLOGIC communication

Gruppe: Power Supply Parameter (nur X20SL8101)

Parameter	Beschreibung	Default Wert	Einheit
Module status information	Dieser Parameter aktiviert/deaktiviert zusätzliche Statusinformationen im I/O Mapping.	On	-
Current/voltage information	Dieser Parameter aktiviert/deaktiviert zusätzliche Strom- und Spannungs-Informationen im I/O Mapping.	Off	-

Tabelle 22: Parameter I/O Konfiguration: Power Supply Parameter

5.2 Parameter im SafeDESIGNER - bis Release 1.9

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. <ul style="list-style-type: none"> Erlaubte Werte: 800 bis 20.000 µs (entspricht 0,8 bis 20 ms) 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 SafeLOGIC Zyklen <ul style="list-style-type: none"> Erlaubte Werte: 800 bis 21.000 µs (entspricht 0,8 bis 21 ms) ACHTUNG: Der Wert sollte nicht genau gleich der tatsächlichen Zykluszeit sein. Eventuelle Netzwerkjitter müssen berücksichtigt werden. Die tatsächliche Zykluszeit wird durch den Parameter "Cycle_Time_us" beeinflusst.	21000	µs
SSDO_Creation	Dieser Parameter definiert die Anzahl der asynchronen Bearbeitungen pro SafeLOGIC Zyklus. Mit diesem Parameter lässt sich das Hochlaufverhalten des Systems optimieren.	Time dependent	-
	Parameter Wert	Beschreibung	
	Time dependent	Abhängig von der SafeLOGIC Zykluszeit <ul style="list-style-type: none"> bei Zykluszeiten ≤3 ms = 1 je 5 Zyklen bei Zykluszeiten >3 ms = 1 je Zyklus 	
	1 per 5 cycles	Eine asynchrone Bearbeitung wird auf 5 SafeLOGIC Zyklen verteilt <ul style="list-style-type: none"> kann zu langen Hochlaufzeiten führen geringster Kommunikationsoverhead im Zyklus 	
	1 per cycle	Eine asynchrone Bearbeitung pro SafeLOGIC Zyklus <ul style="list-style-type: none"> neutrale Hochlaufzeiten neutraler Kommunikationsoverhead im Zyklus 	
5 per cycle	5 asynchrone Bearbeitungen je SafeLOGIC Zyklus <ul style="list-style-type: none"> 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 ein fehlendes Modul erkennt. <ul style="list-style-type: none"> Erlaubte Werte: 30 bis 3000 s Hinweise <ul style="list-style-type: none"> 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
Number_of_scans	Dieser Parameter definiert die Anzahl der Scans für die Modulsuche beim Hochlauf. Mit diesem Parameter lässt sich das Hochlaufverhalten des Systems optimieren, vor allem, wenn optionale Module konfiguriert sind, die nicht vorhanden sind. <ul style="list-style-type: none"> Erlaubte Werte: 1 bis 10 	5	-
ExternalMachineOptions (ab Release 1.4)	Aktivierung der externen Maschinenoptionen	No	-
	Parameter Wert	Beschreibung	
	Yes-ATTENTION	Externe Maschinenoptionen sind aktiviert	
No	Externe Maschinenoptionen sind deaktiviert		

Tabelle 23: Parameter SafeDESIGNER: Basic

Parameter	Beschreibung	Default Wert	Einheit						
ExternalStartupFlags (ab Release 1.4)	Aktivierung der externen Startup-Flags	No	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes-ATTENTION</td> <td>Externe Startup-Flags sind aktiviert</td> </tr> <tr> <td>No</td> <td>Externe Startup-Flags sind deaktiviert</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Yes-ATTENTION	Externe Startup-Flags sind aktiviert	No	Externe Startup-Flags sind deaktiviert
	Parameter Wert	Beschreibung							
	Yes-ATTENTION	Externe Startup-Flags sind aktiviert							
No	Externe Startup-Flags sind deaktiviert								
KeepRemanent	Automatisches Rücksetzen der remanenten Daten (siehe Automation Help der SafeDESIGNER Funktionsbausteine "SF_RemmanentData_SAFEDINT" oder "SF_RemmanentData_SAFEDWORD")	No	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes-ATTENTION</td> <td>Remanente Daten werden nicht automatisch rückgesetzt</td> </tr> <tr> <td>No</td> <td>Remanente Daten werden automatisch rückgesetzt, wenn ein geändertes SafeDESIGNER Projekt (CRC und/oder Timestamp geändert) auf die SafeLOGIC geladen wird.</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Yes-ATTENTION	Remanente Daten werden nicht automatisch rückgesetzt	No	Remanente Daten werden automatisch rückgesetzt, wenn ein geändertes SafeDESIGNER Projekt (CRC und/oder Timestamp geändert) auf die SafeLOGIC geladen wird.
	Parameter Wert	Beschreibung							
	Yes-ATTENTION	Remanente Daten werden nicht automatisch rückgesetzt							
No	Remanente Daten werden automatisch rückgesetzt, wenn ein geändertes SafeDESIGNER Projekt (CRC und/oder Timestamp geändert) auf die SafeLOGIC geladen wird.								

Tabelle 23: 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 als bzw. zu nahe an der notwendigen Bearbeitungszeit, so kann es zu einer Zykluszeitverletzung kommen.

Weitere Informationen hierzu finden Sie auch unter Abschnitt "[SafeLOGIC Info-Dialog im SafeDESIGNER](#)".

Gefahr!

Sofern einer der Parameter "ExternalMachineOptions" bzw. "ExternalStartupFlags" auf "Yes-ATTENTION" gesetzt wird und damit das Nutzen einer dieser Funktionen im SafeDESIGNER freigeschaltet wird, müssen unbedingt die damit verbundenen Hinweise im Kapitel "[Bedienung über AsSafety Bibliothek](#)" beachtet werden. Andernfalls kann es durch Fehlfunktionen zu gefahrbringenden Zuständen kommen.

Gefahr!

Falls der Parameter "KeepRemanent" auf "Yes-ATTENTION" konfiguriert ist, muss bei der Speicherung der Daten nach einem Projektdownload darauf geachtet werden, dass diese immer noch die gleiche Bedeutung im Anwendungsprogramm haben.

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 = No" gesetzt, so werden diese Default Werte verwendet.

Parameter	Beschreibung	Default Wert	Einheit						
Default_Synchronous_Network_Only	Dieser Parameter beschreibt die Synchronisationseigenschaften des zugrunde liegenden Netzwerks. Diese werden im Automation Studio / Automation Runtime festgelegt.	Yes	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes</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>No</td> <td>Keine Anforderung an die Synchronität der Netzwerke</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Yes	Für die Berechnung der sicheren Reaktionszeit werden ausschließlich synchrone Netzwerke mit gleichen Zykluszeiten oder ganzzahligen Verhältnissen der Zykluszeiten vorausgesetzt.	No	Keine Anforderung an die Synchronität der Netzwerke
	Parameter Wert	Beschreibung							
Yes	Für die Berechnung der sicheren Reaktionszeit werden ausschließlich synchrone Netzwerke mit gleichen Zykluszeiten oder ganzzahligen Verhältnissen der Zykluszeiten vorausgesetzt.								
No	Keine Anforderung an die Synchronität der Netzwerke								
Default_Max_X2X_CycleTime_us	Dieser Parameter gibt die max. X2X Zykluszeit für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 200 bis 30.000 µs (entspricht 0,2 bis 30 ms) 	5000	µs						
Default_Max_Powerlink_CycleTime_us	Dieser Parameter gibt die max. POWERLINK Zykluszeit für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 200 bis 30.000 µs (entspricht 0,2 bis 30 ms) 	5000	µs						
Default_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. <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 30.000 µs (entspricht 0 bis 30 ms) 	5000	µs						
Default_Min_X2X_CycleTime_us	Dieser Parameter gibt die min. X2X Zykluszeit für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 200 bis 30.000 µs (entspricht 0,2 bis 30 ms) 	200	µs						
Default_Min_Powerlink_CycleTime_us	Dieser Parameter gibt die min. POWERLINK Zykluszeit für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 200 bis 30.000 µs (entspricht 0,2 bis 30 ms) 	200	µs						
Default_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 Kopiertask berücksichtigt werden. <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 30.000 µs (entspricht 0 bis 30 ms) 	0	µs						
Default_Worst_Case_Response_Time_us	Dieser Parameter gibt den Grenzwert für die Überwachung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 3000 bis 500.000 µs (entspricht 3 bis 500 ms) 	50000	µs						
Default_Node_Guarding_Lifetime	Dieser Parameter gibt die max. Anzahl von Versuchen innerhalb der beim Parameter "Node_Guarding_Timeout_s" eingestellten Zeit an. Anhand dieser Versuche wird die Verfügbarkeit des Moduls sichergestellt. <ul style="list-style-type: none"> Erlaubte Werte: 1 bis 255 Hinweis <ul style="list-style-type: none"> Je größer der parametrisierte Wert, 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_us" bestimmt. 	5	-						

Tabelle 24: Parameter SafeDESIGNER: Safety_Response_Time_Defaults

5.3 Parameter im SafeDESIGNER - ab Release 1.10

Gruppe: Basic

Parameter	Beschreibung	Default Wert	Einheit										
Min required FW Rev	Dieser Parameter ist für zukünftige Funktionserweiterungen reserviert.	Basic Release	-										
SSDO Creation	Dieser Parameter definiert die Anzahl der asynchronen Bearbeitungen pro SafeLOGIC Zyklus. Mit diesem Parameter lässt sich das Hochlaufverhalten des Systems optimieren.	Time dependent	-										
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Time dependent</td> <td>Abhängig von der SafeLOGIC Zykluszeit <ul style="list-style-type: none"> bei Zykluszeiten ≤ 3 ms = 1 je 5 Zyklen bei Zykluszeiten > 3 ms = 1 je Zyklus </td> </tr> <tr> <td>1 per 5 cycles</td> <td>Eine asynchrone Bearbeitung wird auf 5 SafeLOGIC Zyklen verteilt <ul style="list-style-type: none"> kann zu langen Hochlaufzeiten führen geringster Kommunikationsoverhead im Zyklus </td> </tr> <tr> <td>1 per cycle</td> <td>Eine asynchrone Bearbeitung pro SafeLOGIC Zyklus <ul style="list-style-type: none"> neutrale Hochlaufzeiten neutraler Kommunikationsoverhead im Zyklus </td> </tr> <tr> <td>5 per cycle</td> <td>5 asynchrone Bearbeitungen je SafeLOGIC Zyklus <ul style="list-style-type: none"> minimale Hochlaufzeiten maximaler Kommunikationsoverhead im Zyklus </td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Time dependent	Abhängig von der SafeLOGIC Zykluszeit <ul style="list-style-type: none"> bei Zykluszeiten ≤ 3 ms = 1 je 5 Zyklen bei Zykluszeiten > 3 ms = 1 je Zyklus 	1 per 5 cycles	Eine asynchrone Bearbeitung wird auf 5 SafeLOGIC Zyklen verteilt <ul style="list-style-type: none"> kann zu langen Hochlaufzeiten führen geringster Kommunikationsoverhead im Zyklus 	1 per cycle	Eine asynchrone Bearbeitung pro SafeLOGIC Zyklus <ul style="list-style-type: none"> neutrale Hochlaufzeiten neutraler Kommunikationsoverhead im Zyklus 	5 per cycle	5 asynchrone Bearbeitungen je SafeLOGIC Zyklus <ul style="list-style-type: none"> minimale Hochlaufzeiten maximaler Kommunikationsoverhead im Zyklus
	Parameter Wert	Beschreibung											
	Time dependent	Abhängig von der SafeLOGIC Zykluszeit <ul style="list-style-type: none"> bei Zykluszeiten ≤ 3 ms = 1 je 5 Zyklen bei Zykluszeiten > 3 ms = 1 je Zyklus 											
	1 per 5 cycles	Eine asynchrone Bearbeitung wird auf 5 SafeLOGIC Zyklen verteilt <ul style="list-style-type: none"> kann zu langen Hochlaufzeiten führen geringster Kommunikationsoverhead im Zyklus 											
1 per cycle	Eine asynchrone Bearbeitung pro SafeLOGIC Zyklus <ul style="list-style-type: none"> neutrale Hochlaufzeiten neutraler Kommunikationsoverhead im Zyklus 												
5 per cycle	5 asynchrone Bearbeitungen je SafeLOGIC Zyklus <ul style="list-style-type: none"> minimale Hochlaufzeiten maximaler Kommunikationsoverhead im Zyklus 												
Node Guarding Timeout	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 ein fehlendes Modul erkennt. <ul style="list-style-type: none"> Erlaubte Werte: 30 bis 300 s Hinweise <ul style="list-style-type: none"> 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 bestimmt. 	60	s										
Number of scans	Dieser Parameter definiert die Anzahl der Scans für die Modulsuche beim Hochlauf. Mit diesem Parameter lässt sich das Hochlaufverhalten des Systems optimieren, vor allem, wenn optionale Module konfiguriert sind, die nicht vorhanden sind. <ul style="list-style-type: none"> Erlaubte Werte: 1 bis 10 	5; ab Hardware-Upgrade 1.10.1.0: 3	-										
Activate Setup Mode on empty SafeKEY (ab Hardware-Upgrade 1.10.2.x)	Dieser Parameter aktiviert den Setup-Modus nach einem Projekt-Download auf einen leeren SafeKEY.	No	-										
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes-ATTENTION</td> <td>Der Setup-Modus ist aktiviert.</td> </tr> <tr> <td>No</td> <td>Der Setup-Modus ist deaktiviert.</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Yes-ATTENTION	Der Setup-Modus ist aktiviert.	No	Der Setup-Modus ist deaktiviert.				
	Parameter Wert	Beschreibung											
Yes-ATTENTION	Der Setup-Modus ist aktiviert.												
No	Der Setup-Modus ist deaktiviert.												
Auto acknowledge firmware mismatch (ab Hardware-Upgrade 1.10.2.x)	Dieser Parameter aktiviert die automatische Quittierung eines Firmware-Tauschs (Quittierungsanforderung "Firmware Acknowledge").	No	-										
Auto acknowledge SafeKEY exchange (ab Hardware-Upgrade 1.10.2.x)	Dieser Parameter aktiviert die automatische Quittierung eines SafeKEY-Tauschs (Quittierungsanforderung "SafeKEY Exchange").	No	-										
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes-ATTENTION</td> <td>Die automatische Quittierung eines Firmware-Tauschs ist aktiviert.</td> </tr> <tr> <td>No</td> <td>Die automatische Quittierung eines Firmware-Tauschs ist nicht aktiviert.</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Yes-ATTENTION	Die automatische Quittierung eines Firmware-Tauschs ist aktiviert.	No	Die automatische Quittierung eines Firmware-Tauschs ist nicht aktiviert.				
	Parameter Wert	Beschreibung											
Yes-ATTENTION	Die automatische Quittierung eines Firmware-Tauschs ist aktiviert.												
No	Die automatische Quittierung eines Firmware-Tauschs ist nicht aktiviert.												
Process Data Transmission Rate (ab Hardware-Upgrade 1.10.5.x)	Dieser Parameter definiert die Basis-Übertragungsrate für Prozessdaten.	High	-										
<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>High</td> <td>Normale Übertragungsrate.</td> </tr> <tr> <td>Low</td> <td>Reduzierte Übertragungsrate, zur Unterstützung von Netzwerken mit niedrigen Übertragungsraten (Datenlaufzeit > 1 s).</td> </tr> </tbody> </table>				Parameter Wert	Beschreibung	High	Normale Übertragungsrate.	Low	Reduzierte Übertragungsrate, zur Unterstützung von Netzwerken mit niedrigen Übertragungsraten (Datenlaufzeit > 1 s).				
Parameter Wert	Beschreibung												
High	Normale Übertragungsrate.												
Low	Reduzierte Übertragungsrate, zur Unterstützung von Netzwerken mit niedrigen Übertragungsraten (Datenlaufzeit > 1 s).												

Tabelle 26: Parameter SafeDESIGNER: Basic

Information:

Die Hochlaufzeit wird auch von der asynchronen Bandbreite am POWERLINK beeinflusst. Optimierungsmöglichkeit siehe Automation Help unter Kommunikation -> POWERLINK -> Allgemeines -> Multiple Asynchronous Send.

Information:

Bei der Verwendung des Parameters "Activate Setup Mode on empty SafeKEY" sind die Hinweise in Abschnitt "Setup-Modus" auf Seite 70 zu beachten. Bei der Verwendung der Parameter "Auto acknowledge firmware mismatch" und "Auto acknowledge SafeKEY exchange" sind die Hinweise in Abschnitt "Automatische Quittierung" auf Seite 43 zu beachten.

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 = No" gesetzt, so werden diese Default Werte verwendet.

Parameter	Beschreibung	Default Wert	Einheit
Default Safe Data Duration	Dieser Parameter gibt die maximal erlaubte Datenlaufzeit zwischen der SafeLOGIC und dem SafeIO-Modul an. Weitere Informationen zur tatsächlichen Datenlaufzeit sind der Automation Help unter Diagnose und Service -> Diagnosewerkzeug -> Network Analyzer -> Editor -> Safety Laufzeitberechnung zu entnehmen. Zusätzlich ist die Zykluszeit der Sicherheitsapplikation zu addieren. <ul style="list-style-type: none"> Erlaubte Werte: 2000 bis 10.000.000 µs (entspricht 2 ms bis 10 s) 	20000	µs
Default Additional Tolerated Packet Loss	Dieser Parameter gibt die Anzahl der bei der Datenübertragung zusätzlich tolerierten Paketverluste an. <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 10 	0	Packets
Default Packets per Node Guarding	Dieser Parameter gibt die max. Anzahl von Paketen an, die für ein Nodeguarding verwendet werden. <ul style="list-style-type: none"> Erlaubte Werte: 1 bis 255 Hinweis <ul style="list-style-type: none"> Je größer der parametrisierte Wert, desto höher das asynchrone Datenaufkommen. Diese Einstellung ist nicht sicherheitskritisch - die Zeit für die sichere Abschaltung der Aktoren wird unabhängig davon bestimmt. 	5	Packets

Tabelle 27: Parameter SafeDESIGNER: Safety Response Time Defaults

Gruppe: Module Configuration

Parameter	Beschreibung	Default Wert	Einheit						
External Machine Options	Aktivierung der externen Maschinenoptionen	No	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes-ATTENTION</td> <td>Externe Maschinenoptionen sind aktiviert</td> </tr> <tr> <td>No</td> <td>Externe Maschinenoptionen sind deaktiviert</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Yes-ATTENTION	Externe Maschinenoptionen sind aktiviert	No	Externe Maschinenoptionen sind deaktiviert
	Parameter Wert	Beschreibung							
Yes-ATTENTION	Externe Maschinenoptionen sind aktiviert								
No	Externe Maschinenoptionen sind deaktiviert								
External Startup Flags	Aktivierung der externen Startup-Flags	No	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes-ATTENTION</td> <td>Externe Startup-Flags sind aktiviert</td> </tr> <tr> <td>No</td> <td>Externe Startup-Flags sind deaktiviert</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Yes-ATTENTION	Externe Startup-Flags sind aktiviert	No	Externe Startup-Flags sind deaktiviert
	Parameter Wert	Beschreibung							
Yes-ATTENTION	Externe Startup-Flags sind aktiviert								
No	Externe Startup-Flags sind deaktiviert								
Keep Remanent	Automatisches Rücksetzen der remanenten Daten (siehe Automation Help der SafeDESIGNER Funktionsbausteine "SF_RemmanentData_SAFEDINT" oder "SF_RemmanentData_SAFEDWORD")	No	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes-ATTENTION</td> <td>Remanente Daten werden nicht automatisch rückgesetzt</td> </tr> <tr> <td>No</td> <td>Remanente Daten werden automatisch rückgesetzt, wenn ein geändertes SafeDESIGNER Projekt (CRC und/oder Timestamp geändert) auf die SafeLOGIC geladen wird.</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Yes-ATTENTION	Remanente Daten werden nicht automatisch rückgesetzt	No	Remanente Daten werden automatisch rückgesetzt, wenn ein geändertes SafeDESIGNER Projekt (CRC und/oder Timestamp geändert) auf die SafeLOGIC geladen wird.
	Parameter Wert	Beschreibung							
Yes-ATTENTION	Remanente Daten werden nicht automatisch rückgesetzt								
No	Remanente Daten werden automatisch rückgesetzt, wenn ein geändertes SafeDESIGNER Projekt (CRC und/oder Timestamp geändert) auf die SafeLOGIC geladen wird.								
Cycle Time	Mit diesem Parameter wird die Zykluszeit der Sicherheitsapplikation festgelegt. <ul style="list-style-type: none"> Erlaubte Werte: 800 bis 20.000 µs (entspricht 0,8 bis 20 ms) Der eingestellte Wert wird intern auf das nächste ganzzahlige Vielfache der POWERLINK Zykluszeit aufgerundet.	2000	µs						
Cycle Time max (bis Hardware-Upgrade 1.10.1.0)	Parameter zur Kontrolle auf Überschreitung einer maximalen Zeit zwischen 2 SafeLOGIC Zyklen <ul style="list-style-type: none"> Erlaubte Werte: 800 bis 21.000 µs (entspricht 0,8 bis 21 ms) ACHTUNG: Der Wert sollte nicht genau gleich der tatsächlichen Zykluszeit sein. Eventuelle Netzwerkjitter müssen berücksichtigt werden. Die tatsächliche Zykluszeit wird durch den Parameter "Cycle Time" beeinflusst.	21000	µs						

Tabelle 28: Parameter SafeDESIGNER: Basic

Information:

Der Parameter "Cycle Time" 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" kleiner als bzw. zu nahe an der notwendigen Bearbeitungszeit, so kann es zu einer Zykluszeitverletzung kommen.

Weitere Informationen hierzu finden Sie auch unter Abschnitt "[SafeLOGIC Info-Dialog im SafeDESIGNER](#)".

Gefahr!

Sofern einer der Parameter "External Machine Options" bzw. "External Startup Flags" auf "Yes-ATTENTION" gesetzt wird und damit das Nutzen einer dieser Funktionen im SafeDESIGNER freigeschaltet wird, müssen unbedingt die damit verbundenen Hinweise im Kapitel "[Bedienung über AsSafety Bibliothek](#)" beachtet werden. Andernfalls kann es durch Fehlfunktionen zu gefahrbringenden Zuständen kommen.

Gefahr!

Falls der Parameter "Keep Remanent" auf "Yes-ATTENTION" konfiguriert ist, muss bei der Speicherung der Daten nach einem Projektdownload darauf geachtet werden, dass diese immer noch die gleiche Bedeutung im Anwendungsprogramm haben.

5.4 Kanalliste der SafeLOGIC

Kanalname	Zugriff über Automation Studio	Zugriff über SafeDESIGNER	Datentyp	Beschreibung
ModuleOk	Read	-	BOOL	Kenntnis ob Modul OK
SerialNumber	Read	-	UDINT	Serialnummer des Moduls
ModuleID	Read	-	UDINT	Modulkennung
HardwareVariant	Read	-	UDINT	Hardware-Variante
FirmwareVersion	Read	-	UDINT	Firmware-Version des Moduls
SafeFirmwareVersion	Read	-	UINT	Ab Hardware-Upgrade 1.10.1.4: Kanal zum Auslesen der Version der sicheren Firmware
UDID_low	Read	-	UDINT	UDID, unteren 4 Bytes
UDID_high	Read	-	UINT	UDID, oberen 2 Bytes
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
DINT1xx	Write	Read	DINT	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
DINT0xx	Read	Write	DINT	Kommunikationskanal SafeLOGIC zur CPU
UDINT0xx	Read	Write	UDINT	Kommunikationskanal SafeLOGIC zur CPU
SafeBOOLx	-	Write	SAFEBOOL	Kommunikationskanal SafeLOGIC zur SafeLOGIC
SafeMachineOptionxx	-	Read	SAFEBOOL	Interner Kanal für Maschinenoptionen
ExternalMachineOptionsBITxxx	-	Read	SAFEBOOL	Interne Kanäle für externe Maschinenoptionen
ExternalMachineOptionsINTxx	-	Read	SAFEINT	Interne Kanäle für externe Maschinenoptionen
ExternalMachineOptionsUINTxx	-	Read	SAFEWORD	Interne Kanäle für externe Maschinenoptionen
ExternalMachineOptionsDINTxx	-	Read	SAFEDINT	Interne Kanäle für externe Maschinenoptionen
ExternalMachineOptionsUDINTxx	-	Read	SAFEDWORD	Interne Kanäle für externe Maschinenoptionen

Tabelle 30: Kanalliste der SafeLOGIC

Information:

Kanäle für SafeLOGIC to SafeLOGIC communication: siehe [Darstellung im SafeDESIGNER](#)

Information:

An der X20SL8101 sowie an der X20SL8110 stehen zusätzliche Diagnosedatenpunkte zur Verfügung. Details dazu siehe Automation Help unter Kommunikation -> POWERLINK -> Diagnose -> Diagnosedatenpunkte -> Bus Controller.

Zusätzlich können folgende Daten über POWERLINK-Register ausgelesen werden:

Index:Subindex	Objektbezeichnung	Datentyp	Zugriff	Werte	Beschreibung
0x2000:0x04	SafetyFWversion1	UDINT	Read	-	Höherwertige 2 Bytes: Hardware-Variante des Moduls Niederwertige 2 Bytes: Firmware-Version Safety Prozessor 1
0x2000:0x05	SafetyFWversion2	UDINT	Read	-	Höherwertige 2 Bytes: Hardware-Variante des Moduls Niederwertige 2 Bytes: Firmware-Version Safety Prozessor 2
0x2000:0x08	Project_CRC	UDINT	Read	-	CRC des SafeDESIGNER Projekts
0x2000:0x09	Project_Time	DATE_AND_TIME	Read	-	Zeitstempel des SafeDESIGNER Projekts
0x2000:0x0C	Project_Name	STRING (ohne Nullterminierung)	Read	-	Projektname des SafeDESIGNER Projekts
0x2000:0x0D	Project_Author	STRING (ohne Nullterminierung)	Read	-	Name des Autors des SafeDESIGNER Projekts
0x2000:0x0E	SafeOS_RUN_STATE	BOOL	Read	0 1	SafeOS ist nicht in RUN (ident zu SafeOSstate!=0x66) SafeOS ist in RUN (ident zu SafeOSstate==0x66)
0x2000:0x0F	BOOT_STATE	UDINT	Read		Allgemeiner Hochlauf-Status der Firmware; Es wird empfohlen das aktualisierte Objekt "Bootstate" (0x2410:0x01) zu verwenden. 0x00 Hochlauf noch nicht begonnen 0x01 Initialisierung gestartet 0x10 Zyklische Hardware-Tests laufen 0x11 openSAFETY-Stack läuft 0x12 SafeOS läuft
0x2000:0x10	openSAFETYstate	UDINT	Read	0 1	PREOPERATIONAL State (alle zyklischen sicheren Daten werden gennullt) OPERATIONAL State
0x2000:0x11	SafeOsState	UDINT	Read		Status der Sicherheitsapplikation (entspricht der R/E-LED der SafeLOGIC); Details siehe " SafeLOGIC Info-Dialog im SafeDESIGNER " 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
0x2000:0x12	Temperature	INT	Read	-	Gemessene Temperatur in 0,1°C

Nachfolgende Objekte sind ab Hardware-Upgrade 1.10.4.0 verfügbar:

Index:Subindex	Datentyp	Zugriff	Werte	Beschreibung
0x2410:0x01	UDINT	Read		Bootstate; Hochlaufstatus der SafeLOGIC; Hinweise: <ul style="list-style-type: none"> Einige der Bootstates treten bei einem ordnungsgemäßen Hochlauf nicht auf oder werden so schnell durchlaufen, dass sie von außen nicht sichtbar sind. Üblicherweise werden die Bootstates in aufsteigender Reihenfolge durchlaufen. Es gibt aber auch Fälle, bei denen ein vorheriger Wert eingenommen wird.
			0x0003	Hochlauf Kommunikationsprozessor OK, keine Kommunikation zu den Sicherheitsprozessoren
			0x0008	SafeKEY Check (kein gültiger SafeKEY gesteckt)
			0x0010	FAILSAFE; Mindestens einer der Sicherheitsprozessoren befindet sich im sicheren Zustand.
			0x0020	Interne Kommunikation zu den Sicherheitsprozessoren gestartet
			0x0024	Firmware-Update der Sicherheitsprozessoren
			0x0030	Hochlauf der Sicherheitsprozessoren
			0x0040	Firmware der Sicherheitsprozessoren gestartet
			0x0440	Firmware der Sicherheitsprozessoren läuft
			0x0840	Laden der SafeDESIGNER-Applikation bzw. keine gültige SafeDESIGNER-Applikation vorhanden.
			0x1840	Warten auf Quittierungen (z. B. Modultausch)
			0x2040 ... 0x2A40	SCAN: Die verwendeten Safety-Module werden im Netzwerk gesucht und parametrierbar. Entsprechend dem SafeDESIGNER-Parameter "Number of Scans" werden mehrere SCAN-Läufe durchgeführt solange nicht alle Module gefunden wurden: 0x2040: Erster Durchlauf 0x2140: Zweiter Durchlauf 0x2240: Dritter Durchlauf ...
			0x3040	Fehlende Module; Der Hochlauf kann nicht fortgesetzt werden, da Module fehlen, welche mit "Optional = No" parametrierbar sind.
			0x3440	Parametrierung der vorhandenen Safety-Module abgeschlossen; Stabilisierung des zyklischen openSAFETY-Datenaustausches; Hinweis: Wenn der Bootstate hier verbleibt, sind die SafeDESIGNER-Parameter "(Default) Safe Data Duration", "(Default) Additional Tolerated Packet Loss" zu kontrollieren.

Index:Subindex	Datentyp	Zugriff	Werte	Beschreibung
0x2410:0x02	UDINT	Read	0x4040	RUN; finaler Status, Hochlauf abgeschlossen
0x2410:0x03	UDINT	Read	-	SCAN-Fortschritt (wie viele Module wurden im aktuell laufenden Scan bereits bearbeitet)
0x2410:0x04	UDINT	Read	-	Versorgungsspannung (in mV)
0x2410:0x05	UDINT	Read	-	CRC des Firmware-Headers auf Safety Prozessor 1
0x2410:0x06	UDINT	Read	-	CRC des Firmware-Headers auf Safety Prozessor 2
0x2410:0x07	UDINT	Read	-	Maximale Zykluszeit (Zeit von Zyklus-Start bis Zyklus-Ende)
0x2410:0x08	UDINT	Read	-	Zyklus-Start Intervall (Zeit von einem Zyklus-Start zum nächsten Zyklus-Start)
0x2410:0x09	UDINT	Read	-	SafeLOGIC Status Word
0x2410:0x0A	UDINT	Read	-	Anzahl fehlender Module
0x2410:0x0B	UDINT	Read	-	Anzahl UDID-Mismatches
0x2410:0x0C	UDINT	Read	-	Anzahl Firmware-Mismatches
0x2410:0x0D	UDINT	Read	-	Anzahl parametrierter Module
0x2410:0x0E	UDINT	Read	-	Fehlende nachladbare Dateien Flag: Bit 0: Maschinenoptionen fehlen in AUTOCNF.BIN Bit 1: Startup-Flags fehlen in AUTOCNF.BIN Bit 2: EMODATA1.BIN fehlt Bit 3: TABDATA1.BIN
0x2410:0x0F	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_SFS_LENGTH
0x2410:0x10	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_SFS_TOO_LONG
0x2410:0x11	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_SFS_FRM_ID
0x2410:0x12	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_SFS_SADR_INV
0x2410:0x13	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_SFS_SDN_INV
0x2410:0x14	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_SFS_TADR_INV
0x2410:0x15	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_SFS_CRC1
0x2410:0x16	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_SFS_CRC2
0x2410:0x17	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_SFS_DATA
0x2410:0x18	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_CYC_REJECT
0x2410:0x19	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_CYC_ERROR
0x2410:0x1A	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_ACYC_REJECT
0x2410:0x1B bis 0x2410:0x1F	UDINT	Read	-	openSAFETY Common Ereigniszähler SERR_k_ACYC_RETRY
0x2410:0x20	UDINT	Read	-	Reserviert für zukünftige openSAFETY Common Ereigniszähler
0x2410:0x21	UDINT	Read	-	Anzahl SCFM Fehler
0x2410:0x22	UDINT	Read	-	Anzahl SCM Fehler
0x2410:0x23	UDINT	Read	-	Anzahl SDN Fehler
0x2410:0x24	UDINT	Read	-	Anzahl SFS Fehler
0x2410:0x25	UDINT	Read	-	Anzahl SHNF Fehler
0x2410:0x26	UDINT	Read	-	Anzahl SNMTM Fehler
0x2410:0x27	UDINT	Read	-	Anzahl SNMTS Fehler
0x2410:0x28	UDINT	Read	-	Anzahl SOD Fehler
0x2410:0x29	UDINT	Read	-	Anzahl SPDO Fehler
0x2410:0x2A	UDINT	Read	-	Anzahl SSC Fehler
0x2410:0x2B	UDINT	Read	-	Anzahl SSDOC Fehler
0x2410:0x2C bis 0x2410:0xFE	UDINT	Read	-	Anzahl SSDOS Fehler
0x2424:0x01	UDINT	Read	-	Reserviert für zukünftige Erweiterungen
0x2424:0x02	UDINT	Read	-	AutoCnf.bin - Zeitstempel
0x2424:0x03	UDINT	Read	-	AutoCnf.bin - Anzahl der CRCs
0x2424:0x04 bis 0x2424:0x0A	UDINT	Read	-	AutoCnf.bin - Größe der Datei in Byte
0x2424:0x0B bis 0x2424:0xn	UDINT	Read	-	AutoCnf.bin - Reserviert für zukünftige Erweiterungen
0x2424:0xn+1 bis 0x2424:0xFE	UDINT	Read	-	AutoCnf.bin - CRC 1 bis N
0x2425:0x01	UDINT	Read	-	AutoCnf.bin - Reserviert für zukünftige Erweiterungen
0x2425:0x02	UDINT	Read	-	EmoData1.bin - Zeitstempel
0x2425:0x03	UDINT	Read	-	EmoData1.bin - Anzahl der CRCs
0x2425:0x04 bis 0x2425:0x0A	UDINT	Read	-	EmoData1.bin - Größe der Datei in Byte
0x2425:0x0B bis 0x2425:0xn	UDINT	Read	-	EmoData1.bin - Reserviert für zukünftige Erweiterungen
0x2425:0xn+1 bis 0x2425:0xFE	UDINT	Read	-	EmoData1.bin - CRC 1 bis N
0x2426:0x01	UDINT	Read	-	EmoData1.bin - Reserviert für zukünftige Erweiterungen
0x2426:0x02	UDINT	Read	-	TabData1.bin - Zeitstempel
0x2426:0x03	UDINT	Read	-	TabData1.bin - Anzahl der CRCs
0x2426:0x04 bis 0x2426:0x0A	UDINT	Read	-	TabData1.bin - Größe der Datei in Byte
0x2426:0x0B bis 0x2426:0xn	UDINT	Read	-	TabData1.bin - Reserviert für zukünftige Erweiterungen
0x2426:0xn+1 bis 0x2426:0xFE	UDINT	Read	-	TabData1.bin - CRC 1 bis N
0x2427:0x01	UDINT	Read	-	TabData1.bin - Reserviert für zukünftige Erweiterungen
0x2427:0x02	UDINT	Read	-	ParData1.bin - Zeitstempel
0x2427:0x02	UDINT	Read	-	ParData1.bin - Anzahl der CRCs

Index:Subindex	Datentyp	Zugriff	Werte	Beschreibung
0x2427:0x03	UDINT	Read	-	ParData1.bin - Größe der Datei in Byte
0x2427:0x04 bis 0x2427:0x0A	UDINT	Read	-	ParData1.bin - Reserviert für zukünftige Erweiterungen
0x2427:0x0B bis 0x2427:0xn	UDINT	Read	-	ParData1.bin - CRC 1 bis N
0x2427:0xn+1 bis 0x2427:0xFE	UDINT	Read	-	ParData1.bin - Reserviert für zukünftige Erweiterungen

Zusätzlich können im Objektbereich 0x2416 bis 0x2423 (Datentyp: UDINT, Zugriff: Read) zu jedem openSAFETY Node folgende Informationen abgerufen werden:

Parameter ID	Wert
0	SafeModule ID
1	Statuswort Bit 0: Fehlendes Modul Bit 1: Firmware-Mismatch des Moduls Bit 2: UDID-Mismatch des Moduls Bit 3: Reserviert Bit 4: Reserviert Bit 5: Connection Valid Bit des Moduls Bit 6 bis 31: Reserviert
2	Connection Valid Statistik (= Anzahl der negativen Flanken des Connection Valid Bits)
3	Propagation Delay Statistik (= Durchschnittswert der Datenlaufzeit); Einheit: 100 µs

Um den Index/Subindex zu ermitteln, sind folgende Formeln zu verwenden.

$$\text{Index} = \frac{\text{Modulnummer}}{23} + 0x2416$$

$$\text{Subindex} = \text{Parameter ID} + \{ [(\text{Modulnummer} - 1) \% 23] \times 11 \} \% 254 + 1$$

Modulnummer: Laufende Nummer des gewünschten Moduls

Parameter ID: Ist der vorherigen Tabelle zu entnehmen

5.5 Kanalliste des Einspeisemoduls - nur X20SL8101

Auf Station 1 am X2X Link ist bereits ein Einspeisemodul integriert.

Kanalname	Zugriff über Automation Studio	Zugriff über SafeDESIGNER	Datentyp	Beschreibung
ModuleOk	Read	-	BOOL	Kennung ob Modul OK
ModuleID	Read	-	UINT	Modulkennung
HardwareVariant	Read	-	UINT	Hardware-Variante
FirmwareVersion	Read	-	UINT	Firmware-Version des Moduls
StatusInput01	Read	-	BOOL	Warnung bei Überstrom (>2,3 A) oder Unterspannung (<4,7 V)
StatusInput02	Read	-	BOOL	I/O Versorgung unterhalb der Warnungsgrenze von 20,4 V
SupplyCurrent	Read	-	USINT	Busversorgungsstrom mit einer Auflösung von 0,1 A
SupplyVoltage	Read	-	USINT	Busversorgungsspannung mit einer Auflösung von 0,1 V

Tabelle 31: Kanalliste des Einspeisemoduls

5.6 SafeLOGIC Info-Dialog im SafeDESIGNER

Der Dialog 'Info Sicherheitssteuerung' erscheint, wenn die Schaltfläche 'Info' im Dialog 'Sicherheitssteuerung' (Kontrolldialog) oder im Dialog 'Debug' gedrückt wird.

Der Dialog zeigt Informationen zum aktuellen Projekt des sicheren Programmiersystems, zum auf der Sicherheitssteuerung gespeicherten/laufenden Projekt, zum aktuellen Status der Sicherheitssteuerung sowie Debug-Informationen usw.

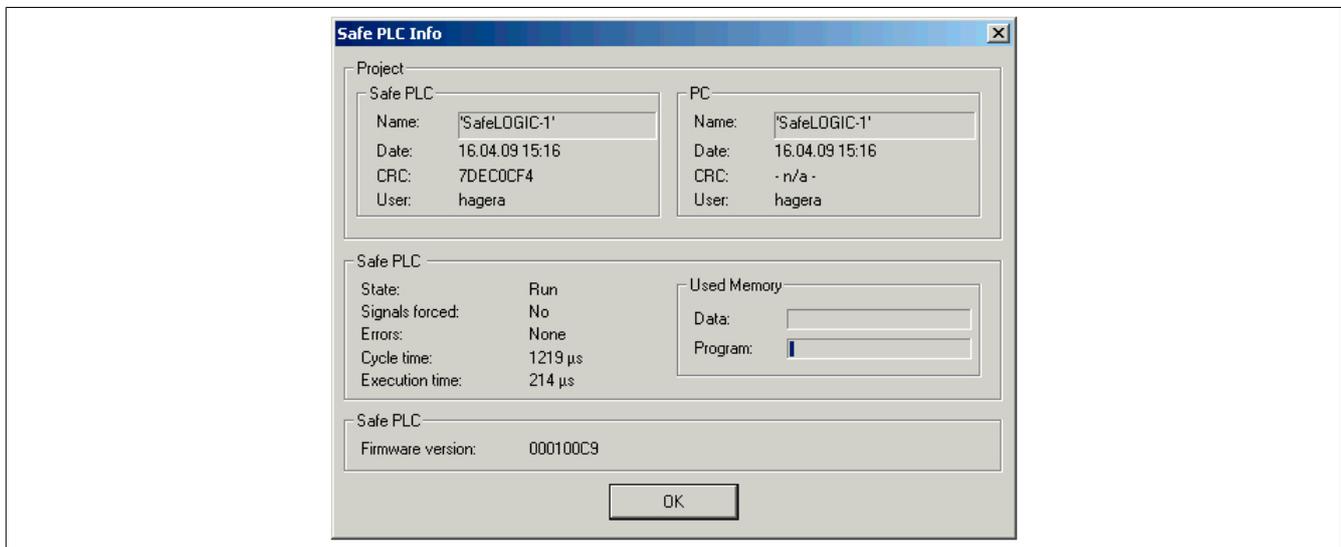


Abbildung 14: SafeLOGIC Info-Dialog

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 kompiliert ist
	User	Anwender der letzten Änderung
Safe PLC	Status und Informationen zur SafeLOGIC	
State	Zeigt den Betriebsstatus der Sicherheitssteuerung an.	
Signals forced	No	Es sind keine Variablen geforced.
	Yes	Es sind Variablen geforced.
Errors	Information bezüglich verfügbarer Fehlermeldungen im SafeDESIGNER Meldungsfenster	
Cycle time	Tatsächlich 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 Systemressourcen	
	Data	Datenspeicher der sicheren Applikation
	Program	Programmspeicher der sicheren Applikation
Firmware version	Firmware-Version	

6 Wartungsszenarien

Für die Bedienung der nachfolgenden Wartungsszenarien stehen einerseits die Bedienelemente an der SafeLOGIC (X20SL8xxx Serie) oder die Bedienelemente der "Remote Control" im SafeDESIGNER (X20SL8xxx Serie und X20SLXxxx Serie) zur Verfügung.

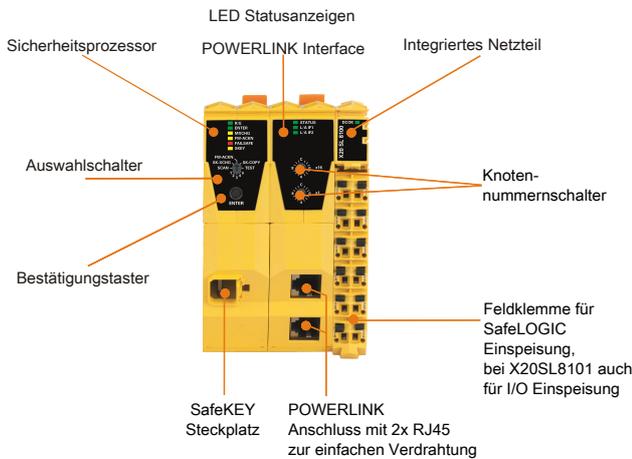


Abbildung 15: X20SL810x - Bedienelemente

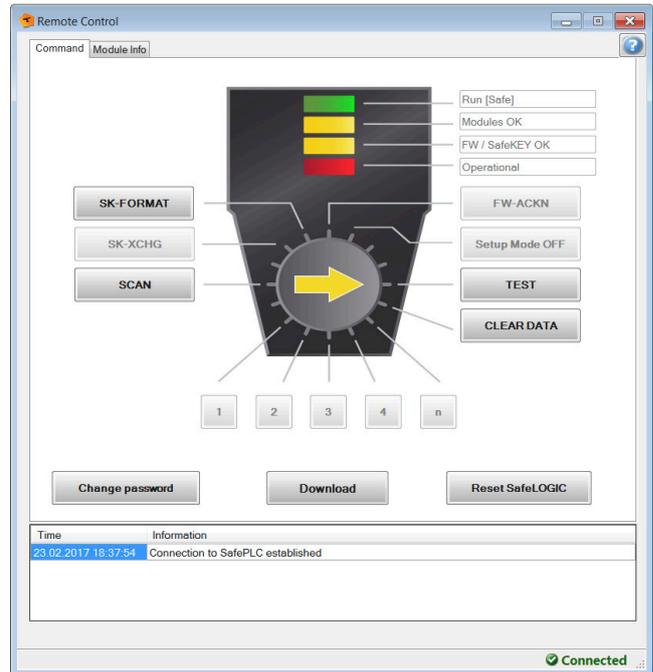


Abbildung 16: SafeDESIGNER - Bedienelemente "Remote Control"

Detaillierte Beschreibung der Bedienelemente siehe technisches Datenblatt der X20SL8xxx Serie, Kapitel Bedien- und Anschlusselemente.

Detaillierte Beschreibung der Bedienelemente siehe Automation Help SafeDESIGNER, Abschnitt Bedienelemente der Remote Control.

6.1 Tauschen von Modulen

Die SafeLOGIC erkennt selbstständig das Tauschen von sicheren Modulen. Das Gesamtsystem (SafeLOGIC, SafeLOGIC-X Systemkomponenten, 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

6.1.1 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!

6.1.2 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!**

6.1.3 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 bestätigen. Damit ist die Anzahl der vom Anwender getauschten Module und der vom System erkannten Vertauschungen verknüpft und zusätzliche Vertauschungen können erkannt werden.

Der Anwender wird mittels Status MXCHG über die Anzahl der erkannten Modulvertauschungen informiert. Dabei werden die am SafeKEY bzw. in der Safety Section der CompactFlash gespeicherten Kennungen der Module (UDID) gegen die UDIDs der Module im Netzwerk geprüft.

Bei 1, 2, 3 oder 4 unterschiedlichen UDIDs wird der Anwender über die genaue Anzahl der Unterschiede informiert. 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.

Bei mehr als 4 unterschiedlichen UDIDs wird pauschal ein Unterschied von mehr als 4 Modulen signalisiert. Der Anwender muss in diesem Fall einen vollständigen Verdrahtungstest aller Module durchführen.

Falls die Anzahl der signalisierten Module und der tatsächlich getauschten Module nicht übereinstimmt, 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!

6.1.4 Tauschen eines einzelnen Moduls

Wenn nur ein einzelnes Modul getauscht wurde (Status MXCHG signalisiert 1 getauschtes Modul) und an der Verdrahtung nichts geändert wurde, kann der Anwender entscheiden, den Verdrahtungstest entfallen zu lassen, da in diesem Fall die folgenden Fehler ausgeschlossen werden können:

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

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.

6.1.5 Modultausch bestätigen

Zur Bestätigung der Anzahl der getauschten Module muss die korrekte Modulanzahl angewählt 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 Modultauschs 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!

6.2 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 Hardware-Kennung hat oder sonstige Probleme am Modul vorliegen (z. B. falsche Parameter, aber die Parameter am Modul können von der SafeLOGIC nicht verändert werden), wird ein Fehler (Status "Missing Module") signalisiert. Dieser Zustand wird nur signalisiert, wenn kein Modultausch und kein Firmware-Tausch signalisiert wird. 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!

6.3 Bestätigung eines Firmware-Tauschs

Eine Änderung an der Firmware wird durch Status FW-ACKN angezeigt und muss durch die Aktion FW-ACKN bestätigt werden. Ein Firmware-Tausch 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 Firmware-Tauschs geschult sind.

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

Gefahr!

Verwenden Sie ausschließlich Firmware-Versionen, die in den FS-Zertifikaten der B&R-Sicherheitstechnik gelistet sind. Die FS-Zertifikate stehen auf der B&R Homepage <http://www.br-automation.com> zum Download zur Verfügung.

6.4 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 Modultauchs die Wartezeit, bis die SafeLOGIC das getauschte Modul erkennt, zu minimieren, kann diese Funktion auch manuell ausgelöst werden. Das Resultat des Scans wird unter folgenden Abschnitten beschrieben:

- "Tauschen von Modulen"
- "Sonstige Fehler in der Modulkonfiguration"
- "Bestätigung eines Firmware-Tauschs"

Der Vorgang selbst wird mit der Funktion SCAN gestartet und mit Status "Scanning" signalisiert. Erst nach Abschluss des Status "Scanning" werden die Resultate signalisiert (z. B. drei Module getauscht).

6.5 SafeKEY bzw. Safety Section der CompactFlash

Am SafeKEY (X20SL8xxx Serie) bzw. in der Safety Section der CompactFlash (X20SLXxxx Serie) werden folgende Daten gespeichert:

- SafeDESIGNER Applikation (Applikation und alle SafeDESIGNER Parameter der Module)
- Konfiguration (eindeutige Modulkennung - UDID, Firmware-Versionen der Module)
- Nachladbare Datenelemente (Maschinenoptionen, Tabellen, ...)

Größe der SafeDESIGNER-Applikation am SafeKEY

Die Größe der aktuellen Applikation am SafeKEY wird beim Kompilieren vom SafeDESIGNER berechnet und im Meldungsfenster ausgegeben (z. B. "Die Sicherheitsapplikation benötigt 0.688 MB (11 Sektoren) Speicher.").

Hinweise:

- Die Ausgabe berücksichtigt nur die Größe der SafeDESIGNER-Applikation. Speicher, welcher von der Firmware oder von nachladbaren Daten (Tabelle, Maschinenoptionen, usw.) benutzt wird, wird nicht berücksichtigt.
- Wird der Online-Projektvergleich (siehe Automation Help -> SafeDESIGNER) nicht benötigt, kann die Downloadgröße der Applikation durch Deaktivieren der folgenden Kommunikationseinstellung verringert werden: Online -> Kommunikationsparameter -> Download der Projektsourcen auf die SL

6.5.1 Ziehen eines SafeKEYs (nur X20SL8xxx Serie)

Das Ziehen eines SafeKEYs führt immer zu einem Wechsel in den BOOT Zustand 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.

6.5.2 Bestätigen eines SafeKEY Tauschs

Der Tausch eines SafeKEYs bzw. der Tausch der CompactFlash gegen eine CompactFlash mit veränderter Safety Section wird durch Status FW-ACKN signalisiert und muss mit der Funktion SK-XCHG quittiert werden. Anschließend ist ein vollständiger Funktionstest vorgeschrieben.

Information:

Ein SafeKEY Tausch kann nur bestätigt werden, wenn bereits ein gültiges SafeDESIGNER-Projekt auf den SafeKEY bzw. die CompactFlash übertragen wurde.

Gefahr!

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

Gefahr!

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

6.5.3 Austauschen der Applikation an der SafeLOGIC mittels SafeKEY Tausch (nur X20SL8xxx Serie)

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

- Auswahlschalter auf die Stellung SK-COPY stellen.
- Betätigen des Bestätigungstasters - 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 s vorgesehen. Die Blinkfrequenz der FW-ACKN LED wird nach 20 s erhöht, um das Ende der Tauschphase zu signalisieren.
- Nachdem der neue SafeKEY gesteckt wurde, muss erneut der Bestätigungstaster 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 des Bestätigungstasters - Aktion wird mit der ENTER LED quittiert.
- Durchführen eines vollständigen Funktionstests.

Information:

Wird nach 30 s 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 s. Wird nach 30 s kein SafeKEY gesteckt, geht die SafeLOGIC in den BOOT Zustand über.

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).

Information:

Es werden ausschließlich die maschinenbezogenen Daten kopiert und nicht die gesamten Daten der Sicherheitsapplikation.

6.6 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!

6.7 Autorisierung (nur X20SL8xxx Serie)

Folgende Funktionen können von der funktionalen CPU blockiert werden:

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

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	NumberOfEntries	USINT	R	0x22	Anzahl der Einträge auf diesem Index
0x2402:0x01	EnableAuthorization	UDINT	RW	"AENA", 0x41454E41	Aktivieren der Autorisierung
				"ADIS", 0x41444953	Deaktivieren der Autorisierung
0x2402:0x04	EnableModuleExchange	UDINT	RW	"UDID", 0x55444944	Autorisierung zur Bestätigung eines Modultauschs ist gegeben
				Alle anderen Werte	Autorisierung zur Bestätigung eines Modultauschs ist nicht gegeben
0x2402:0x05	EnableFWMismatch	UDINT	RW	"FWAC", 0x46574143	Autorisierung zur Bestätigung eines Firmware-Tauschs ist gegeben
				Alle anderen Werte	Autorisierung zur Bestätigung eines Firmware-Tauschs ist nicht gegeben
0x2402:0x06	EnableSKeyExchange	UDINT	RW	"SKEY", 0x534B4559	Autorisierung zur Bestätigung eines SafeKEY Tauschs ist gegeben
				Alle anderen Werte	Autorisierung zur Bestätigung eines SafeKEY Tauschs ist nicht gegeben

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

7 Softwarefunktionen

7.1 Bedienung über AsSafety Bibliothek

Informationen zur Bedienung über die AsSafety Bibliothek sind in der Automation Help unter Programmierung -> Bibliotheken -> Safety -> AsSafety verfügbar.

7.2 Automatische Quittierung

Das automatische Quittieren ist wie in den zuvor genannten Kapiteln üblicherweise nicht erlaubt. Unter der Voraussetzung, dass der Anwender ergänzende qualitätssichernde Maßnahmen bzw. Einschränkungen trifft, sind hiervon abweichend die nachfolgenden automatischen Quittierungen zulässig.

Gefahr!

Das automatische Quittieren von Quittierungsanforderungen der SafeLOGIC unter falschen Voraussetzungen ist nicht zulässig und kann zu gefährlichen Zuständen führen.

Abhängig von den Anforderungen der Sicherheitsanwendung können zusätzliche Maßnahmen notwendig sein, welche eigenverantwortlich durch den Anwender analysiert werden müssen.

7.2.1 Quittierungsanforderung "SafeKEY Exchange"

Die SafeDESIGNER-Anwendung und die Maschinenoption sind in der Safety Section der CompactFlash (X20SLXxxx Serie) bzw. am SafeKEY (X20SL8xxx Serie) gespeichert. Ein Tauschen der CompactFlash bzw. des SafeKEYs kann zu einem ungewollten Austausch dieser Daten führen. Die Quittierungsanforderung "SafeKEY Exchange" soll ein unbeabsichtigtes Austauschen dieser Daten verhindern.

Es muss sichergestellt werden, dass die bei einer automatischen Quittierung möglicherweise beteiligten CompactFlashes bzw. SafeKEYs die folgenden Kriterien erfüllen:

- Die SafeDESIGNER-Anwendung muss an einer Referenzmaschine vollständig validiert werden.
- Die Maschinenoptionsdatei muss an einer Referenzmaschine vollständig validiert werden.
- Es müssen ausreichend Maßnahmen installiert werden, um Verwechslungen der SafeDESIGNER-Anwendung bzw. der Maschinenoptionsdatei auf unterschiedlichen Maschinentypen zu vermeiden.
- Es dürfen keine Testversionen zur SafeDESIGNER-Anwendung oder zur Maschinenoptionsdatei vorhanden sein.

Unter den genannten Bedingungen darf auch ein automatisierter Update der SafeDESIGNER-Anwendung bzw. der Maschinenoptionsdatei auf die SafeLOGIC/SafeLOGIC-X implementiert werden.

7.2.2 Quittierungsanforderung "Firmware Acknowledge"

Das B&R Automation Runtime sorgt ohne Rückfrage dafür, dass die auf der CompactFlash gespeicherten Firmware-Versionen auf die Automatisierungskomponenten im Netzwerk übertragen werden. Dieser Mechanismus kann dazu führen, dass andere Firmware-Versionen im System aktiviert werden als jene, welche bei der Validierung der SafeDESIGNER-Anwendung aktiv waren. Ein Wechsel der Firmware der Safety-Module erfordert immer eine neuerliche Validierung der SafeDESIGNER-Anwendung. Die Quittierungsanforderung "Firmware Acknowledge" soll ein unbeabsichtigtes Austauschen der Firmware-Versionen verhindern.

Es muss sichergestellt werden, dass die bei einer automatischen Quittierung möglicherweise beteiligten CompactFlashes folgendes Kriterium erfüllen:

- Die installierten Firmware-Files der Safety-Module müssen zusammen mit der SafeDESIGNER-Anwendung an einer Referenzmaschine vollständig validiert werden.

7.2.3 Quittierungsanforderung "UDID Mismatch"

Die Anforderung "UDID Mismatch" tritt in folgenden Situationen auf:

- Beim Austausch von Modulen durch den Anwender (z. B. im Service-Fall); In diesem Fall kann es zu einem Vertauschen von Anschlussleitungen kommen.
- Durch Fehler in der funktionalen Applikation, welche zu einem Vertauschen von Modulen führen;

Um diese Vertauschungen auszuschließen muss nach der Quittierung einer "UDID Mismatch"-Anforderung ein Verdrahtungstest durchgeführt werden.

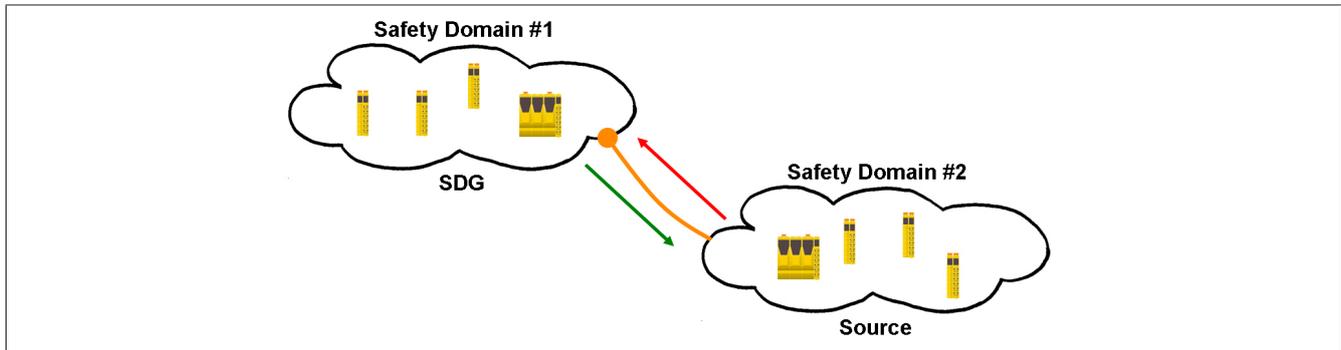
Die Quittierungsanforderung "UDID Mismatch" soll ein unbeabsichtigtes Vertauschen von Signalen (verursacht durch einen Modultausch oder durch Fehler in der funktionalen Applikation) verhindern.

- Das Servicepersonal ist anzuweisen, dass der beim Tauschen von Modulen zwingend notwendige Verdrahtungstest unabhängig von der automatischen Quittierung der "UDID Mismatch"-Anforderung durchgeführt werden muss.
- Weder in der Automation Studio Applikation noch in der SafeDESIGNER-Applikation dürfen mehr als 1 Modul pro Modultyp verwendet werden.

Sofern letztere Anforderung nicht erfüllt werden kann, darf eine Quittierungsanforderung von "UDID Mismatch" nicht automatisiert quittiert werden, da ein Vertauschen der Signale durch Fehler in der funktionalen Applikation nicht aufgedeckt werden würde.

7.3 SafeLOGIC to SafeLOGIC communication

Das Safety System bietet die Möglichkeit sichere Informationen zwischen zwei Sicherheitssteuerungen (SafeLOGIC) auszutauschen. Die SafeLOGIC to SafeLOGIC communication kann dazu verwendet werden um z. B. einen globalen Not-Aus in einem Maschinenverbund zu realisieren oder wenn eine Abhängigkeit zwischen den Sicherheitsapplikationen 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.



Information:

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

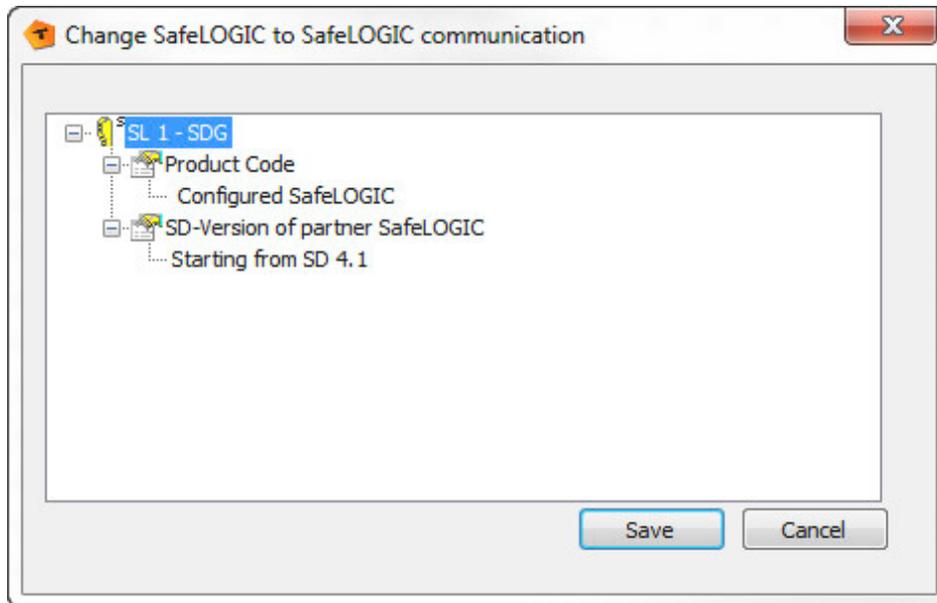
Zu diesem Zweck stellt eine SafeLOGIC ein Safety Domain Gateway (SDG) zur Verfügung an welches mehrere andere SafeLOGICen (Source) verbunden werden können. Über diese Gateway-Funktionalität ist es somit möglich zwischen mehreren Safety Domains zu kommunizieren. Die Verbindung zwischen Source SafeLOGIC 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 Male 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.

7.3.1 Systemvoraussetzungen

Für den sicheren Datenaustausch zwischen mindestens 2 SafeLOGICen sind folgende Punkte zu berücksichtigen:

- SafeDESIGNER <4.1: Es müssen die gleichen SafeDESIGNER-Versionen verwendet werden.
- SafeDESIGNER 4.1 bis 4.2.1: Die SafeDESIGNER-Versionen müssen sich innerhalb dieses Versionsbereichs befinden.
- SafeDESIGNER ab 4.2.2: Es dürfen SafeDESIGNER-Versionen ab 3.0 verwendet werden.
Um eine Verbindung mit der Gegenstelle herzustellen sind im folgenden Dialog die entsprechenden Parameter zu konfigurieren.



- Configured SafeLOGIC: Gegenstelle, mit welcher kommuniziert wird (z. B. X20SL8100)
- SD-Version of partner SafeLOGIC: Version, mit welcher die Applikation der Gegenstelle erstellt wurde

7.3.2 Möglichkeiten

Das System unterstützt verschiedene Möglichkeiten bei der Kommunikation. Die entsprechende Kommunikationsart wird über Parameter im Automation Studio festgelegt (siehe "[Gruppe: SafeLOGIC to SafeLOGIC communication](#)").

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
- Nicht verwendbar bei SafeLOGIC-X

Extended Kommunikation (ab Release 1.4 und Automation Studio 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

7.3.3 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 Konfiguration durchgeführt.

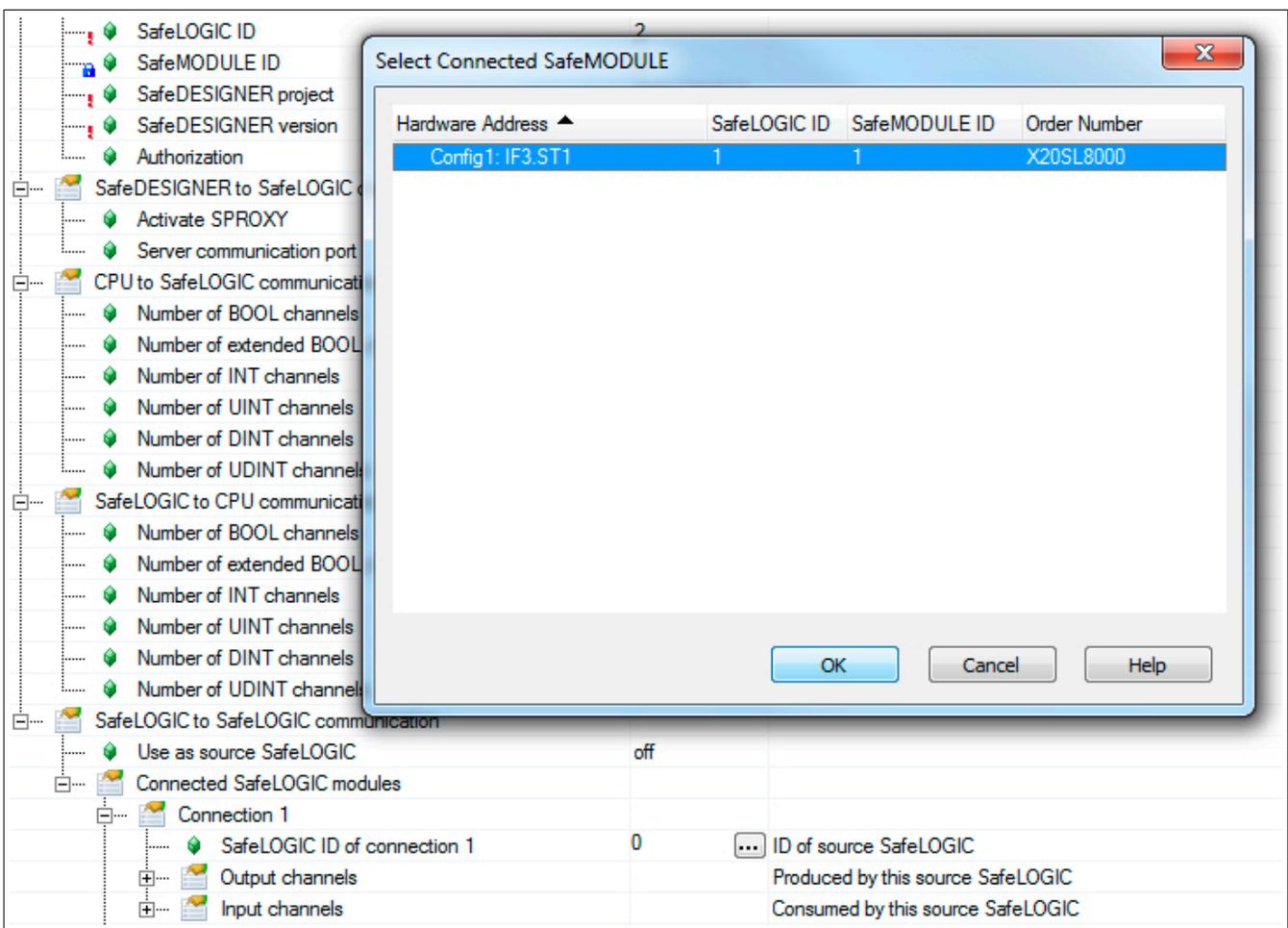


Zusätzlich kann nach dem Aktivieren des Parameters "Use as source SafeLOGIC" die Ausprägung - fix oder extended - der SafeLOGIC to SafeLOGIC communication konfiguriert werden. Ist der Parameter "Extended source SafeLOGIC communication" nicht aktiviert so wird die fixe Kommunikation verwendet.

Information:

Sollte zu einem späteren Zeitpunkt die Kommunikationsart - fix oder extended - geändert werden, kann dies zu Kanalüberschneidungen im SafeDESIGNER führen und die Kommunikationskanäle müssen neu verbunden werden.

Im nächsten Schritt wird die Source SL mit der SDG SL verbunden. Dazu gibt es im Automation Studio unter der I/O Konfiguration einer SafeLOGIC (X20SL80x1 und X20SL81xx) 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.

Connected SafeLOGIC modules		
Connection 1		
SafeLOGIC ID of connection 1	1	ID of source SafeLOGIC
Output channels		Produced by this source SafeLOGIC
Number of BOOL channels	8	
Number of INT channels	0	
Number of UINT channels	0	
Number of DINT channels	0	
Number of UDINT channels	0	
Input channels		Consumed by this source SafeLOGIC
Number of BOOL channels	8	
Number of INT channels	0	
Number of UINT channels	0	
Number of DINT channels	0	
Number of UDINT channels	0	

Soll eine SafeLOGIC to SafeLOGIC communication zwischen bestehenden oder getrennten Automation Studio Projekten erstellt werden, müssen einige Punkte in diesem Zusammenhang beachtet werden:

- SafeLOGIC IDs müssen eindeutig sein.
- Für die entsprechende Gegenstelle ist eine Dummy-Konfiguration mit allen Safety Komponenten anzulegen.
- Die Dummy-Konfiguration muss mit der realen Konfiguration übereinstimmen - wichtig sind hier die SafeMODULE IDs.
- Handelt es sich um Projekte mit mehreren iCNs (intelligent Controlled Nodes) so sind im iCN Projekt immer alle iCNs zu berücksichtigen.

7.3.4 Darstellung im SafeDESIGNER

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

Gefahr!

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

7.3.4.1 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.

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

Wird dieses Modul ausgewählt können dafür sicherheitstechnische Parameter eingestellt werden (siehe Abschnitt "Parameter für Verbindung - ab Release 1.10").

Fixe Kommunikation

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

Channel Name	Value	Slot	V...	CPU ...	Comment
SL1					SafeLOGIC ID 1
SL1.SM1.C1		IF3.ST1			X20SL8011 X20 SafeLOGIC, POWERLINK V2, SafeMC plus
SL2_SafeBOOL1					
SL2_SafeBOOL2					
SL2_SafeBOOL3					
SL2_SafeBOOL4					
SL2_SafeBOOL5					
SL2_SafeBOOL6					
SL2_SafeBOOL7					
SL2_SafeBOOL8					
SafeModuleOK					

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

Channel Name	Value	Slot	V...	CPU ...	Comment
SL2					SafeLOGIC ID 2
SL2.SM1		IF3.ST2			X20SL8000 X20 SafeLOGIC, POWERLINK V2, 24V
CPU_SafeLOGIC					
SafeLOGIC_SafeLOGIC					
SafeBOOL1					
SafeBOOL2					
SafeBOOL3					
SafeBOOL4					
SafeBOOL5					
SafeBOOL6					
SafeBOOL7					
SafeBOOL8					
external_MachineOptions					
SL2.SM2		IF6.ST3			X20SI2100 X20 Safe Digital In, 2xI, 24V

Extended Kommunikation

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

Channel Name	Value	Slot	V...	CPU ...	Comment
SL1					SafeLOGIC ID 1
SL1.SM1.C1		IF3.ST1			X20SL8011 X20 SafeLOGIC, POWERLINK V2, SafeMC plus
C01_SL2_SafeBOOL001					
C01_SL2_SafeBOOL002					
C01_SL2_SafeBOOL003					
C01_SL2_SafeBOOL004					
C01_SL2_SafeBOOL005					
C01_SL2_SafeBOOL006					
C01_SL2_SafeBOOL007					
C01_SL2_SafeBOOL008					
C01_SL2_SafeINT01					
C01_SL2_SafeUINT01					
C01_SL2_SafeDINT01					
C01_SL2_SafeUDINT01					
SafeModuleOK					
SL1_C01_SafeBOOL001					
SL1_C01_SafeBOOL002					
SL1_C01_SafeBOOL003					
SL1_C01_SafeBOOL004					
SL1_C01_SafeBOOL005					
SL1_C01_SafeBOOL006					
SL1_C01_SafeBOOL007					
SL1_C01_SafeBOOL008					
SL1_C01_SafeINT01					
SL1_C01_SafeUINT01					
SL1_C01_SafeDINT01					
SL1_C01_SafeUDINT01					

Weitere Verbindung

Sollte die Source SL ein weiteres Mal auf die gleiche SDG SL verbunden sein, 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, 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

7.3.4.2 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

Information:

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 Bit Information zum Zustand der Verbindung.

SL1.SM3		IF6.ST2			X20SO2120 X20 Safe Digital Out, 2xO, 24 V, 2A
SL2					SafeLOGIC ID 2
SL2.SM1.C1		IF3.ST2			X20SL8000
SafeBOOL1					
SafeBOOL2					
SafeBOOL3					
SafeBOOL4					
SafeBOOL5					
SafeBOOL6					
SafeBOOL7					
SafeBOOL8					
SafeModuleOK					
SL2_SafeBOOL1					
SL2_SafeBOOL2					
SL2_SafeBOOL3					
SL2_SafeBOOL4					
SL2_SafeBOOL5					
SL2_SafeBOOL6					
SL2_SafeBOOL7					
SL2_SafeBOOL8					

Extended Kommunikation

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

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
SL1_C01_SafeBOOL001					
SL1_C01_SafeBOOL002					
SL1_C01_SafeBOOL003					
SL1_C01_SafeBOOL004					
SL1_C01_SafeBOOL005					
SL1_C01_SafeBOOL006					
SL1_C01_SafeBOOL007					
SL1_C01_SafeBOOL008					
SL1_C01_SafeINT01					
SL1_C01_SafeUINT01					
SL1_C01_SafeDINT01					
SL1_C01_SafeUDINT01					
SafeModuleOK					
C01_SL2_SafeBOOL001					
C01_SL2_SafeBOOL002					
C01_SL2_SafeBOOL003					
C01_SL2_SafeBOOL004					
C01_SL2_SafeBOOL005					
C01_SL2_SafeBOOL006					
C01_SL2_SafeBOOL007					
C01_SL2_SafeBOOL008					
C01_SL2_SafeINT01					
C01_SL2_SafeUINT01					
C01_SL2_SafeDINT01					
C01_SL2_SafeUDINT01					

Weitere Verbindung

Sollte die Source SL ein weiteres Mal auf die SDG SL verbunden sein, 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

7.3.5 Parameter für Verbindung - bis Release 1.9

Ab Safety Release 1.4:

Für die Kommunikation stehen ebenfalls Zykluszeitparameter zur Verfügung um die "Worst_Case_Response_Time_us" 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.

Information:

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

Parameter	Beschreibung	Default Wert	Einheit										
Min_required_FW_Rev	Dieser Parameter ist für zukünftige Funktionserweiterungen reserviert.	Basic Release	-										
Optional	Mittels diesem Parameter kann das Modul "optional" parametrierbar 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.	No	-										
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>No</td> <td> <p>Das Modul ist für die Applikation zwingend erforderlich.</p> <p>Das Modul muss sich nach dem Hochlauf im OPERATIONAL Mode befinden und die sichere Kommunikation zur SafeLOGIC muss fehlerfrei aufgebaut sein ("SafeModuleOK = SAFETRUE"). Der Start der Abarbeitung der sicheren Applikation in der SafeLOGIC wird nach dem Hochlauf verzögert, bis dieser Zustand für alle Module mit "Optional = No" erreicht ist.</p> <p>Nach dem Hochlauf werden Modulprobleme mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt ein Eintrag ins Logbuch.</p> </td> </tr> <tr> <td>Yes</td> <td> <p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Yes" im OPERATIONAL Mode sind bzw. ob die sichere Kommunikation dieser Module zur SafeLOGIC korrekt aufgebaut ist oder nicht.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p> </td> </tr> <tr> <td>Startup</td> <td> <p>Das Modul ist optional. Während des Hochlaufs wird über das weitere Verhalten des Moduls entschieden.</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch vorhanden ist (unabhängig davon, ob es sich im Mode OPERATIONAL befindet oder nicht) so verhält sich das Modul wie bei "Optional = No".</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch nicht vorhanden ist, verhält sich das Modul wie bei "Optional = Yes".</p> </td> </tr> <tr> <td>Not_Present (ab Release 1.9)</td> <td> <p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Not_Present" physikalisch vorhanden sind.</p> <p>Zum Unterschied zur Parametrierung "Optional = Yes" wird bei "Optional = Not_Present" das Modul nicht gestartet und somit das Hochlaufverhalten des Systems optimiert.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p> </td> </tr> </tbody> </table>	Parameter Wert	Beschreibung	No	<p>Das Modul ist für die Applikation zwingend erforderlich.</p> <p>Das Modul muss sich nach dem Hochlauf im OPERATIONAL Mode befinden und die sichere Kommunikation zur SafeLOGIC muss fehlerfrei aufgebaut sein ("SafeModuleOK = SAFETRUE"). Der Start der Abarbeitung der sicheren Applikation in der SafeLOGIC wird nach dem Hochlauf verzögert, bis dieser Zustand für alle Module mit "Optional = No" erreicht ist.</p> <p>Nach dem Hochlauf werden Modulprobleme mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt ein Eintrag ins Logbuch.</p>	Yes	<p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Yes" im OPERATIONAL Mode sind bzw. ob die sichere Kommunikation dieser Module zur SafeLOGIC korrekt aufgebaut ist oder nicht.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p>	Startup	<p>Das Modul ist optional. Während des Hochlaufs wird über das weitere Verhalten des Moduls entschieden.</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch vorhanden ist (unabhängig davon, ob es sich im Mode OPERATIONAL befindet oder nicht) so verhält sich das Modul wie bei "Optional = No".</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch nicht vorhanden ist, verhält sich das Modul wie bei "Optional = Yes".</p>	Not_Present (ab Release 1.9)	<p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Not_Present" physikalisch vorhanden sind.</p> <p>Zum Unterschied zur Parametrierung "Optional = Yes" wird bei "Optional = Not_Present" das Modul nicht gestartet und somit das Hochlaufverhalten des Systems optimiert.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p>		
Parameter Wert	Beschreibung												
No	<p>Das Modul ist für die Applikation zwingend erforderlich.</p> <p>Das Modul muss sich nach dem Hochlauf im OPERATIONAL Mode befinden und die sichere Kommunikation zur SafeLOGIC muss fehlerfrei aufgebaut sein ("SafeModuleOK = SAFETRUE"). Der Start der Abarbeitung der sicheren Applikation in der SafeLOGIC wird nach dem Hochlauf verzögert, bis dieser Zustand für alle Module mit "Optional = No" erreicht ist.</p> <p>Nach dem Hochlauf werden Modulprobleme mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt ein Eintrag ins Logbuch.</p>												
Yes	<p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Yes" im OPERATIONAL Mode sind bzw. ob die sichere Kommunikation dieser Module zur SafeLOGIC korrekt aufgebaut ist oder nicht.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p>												
Startup	<p>Das Modul ist optional. Während des Hochlaufs wird über das weitere Verhalten des Moduls entschieden.</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch vorhanden ist (unabhängig davon, ob es sich im Mode OPERATIONAL befindet oder nicht) so verhält sich das Modul wie bei "Optional = No".</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch nicht vorhanden ist, verhält sich das Modul wie bei "Optional = Yes".</p>												
Not_Present (ab Release 1.9)	<p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Not_Present" physikalisch vorhanden sind.</p> <p>Zum Unterschied zur Parametrierung "Optional = Yes" wird bei "Optional = Not_Present" das Modul nicht gestartet und somit das Hochlaufverhalten des Systems optimiert.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p>												
External_UDID	Dieser Parameter aktiviert zum Modul die Möglichkeit, die erwartete UDID extern von der CPU vorgeben zu lassen.	No	-										
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes-ATTENTION</td> <td>Die UDID wird von der CPU vorgegeben. Bei einer Änderung der UDID ist ein Neustart der SafeLOGIC notwendig.</td> </tr> <tr> <td>No</td> <td>Die UDID wird mittels eines Teach-In-Verfahrens während der Inbetriebnahme vorgegeben.</td> </tr> </tbody> </table>	Parameter Wert	Beschreibung	Yes-ATTENTION	Die UDID wird von der CPU vorgegeben. Bei einer Änderung der UDID ist ein Neustart der SafeLOGIC notwendig.	No	Die UDID wird mittels eines Teach-In-Verfahrens während der Inbetriebnahme vorgegeben.						
Parameter Wert	Beschreibung												
Yes-ATTENTION	Die UDID wird von der CPU vorgegeben. Bei einer Änderung der UDID ist ein Neustart der SafeLOGIC notwendig.												
No	Die UDID wird mittels eines Teach-In-Verfahrens während der Inbetriebnahme vorgegeben.												

Tabelle 32: Parameter SafeDESIGNER: Basic

Gefahr!

Falls die Funktion "External_UDID = Yes-ATTENTION" benutzt wird, können durch falsche Vorgaben von der CPU sicherheitskritische Situationen entstehen.

Führen Sie deshalb eine FMEA (Failure Mode and Effects Analysis) durch um diese Situationen zu erkennen und mittels zusätzlicher, sicherheitstechnischer Maßnahmen abzusichern.

Gruppe: Safety_Response_Time

Parameter	Beschreibung	Default Wert	Einheit						
Synchronous_Network_Only	Dieser Parameter beschreibt die Synchronisationseigenschaften des zugrunde liegenden Netzwerks. Diese werden im Automation Studio / Automation Runtime festgelegt.	Yes	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes</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>No</td> <td>Keine Anforderung an die Synchronität der Netzwerke</td> </tr> </tbody> </table>	Parameter Wert	Beschreibung	Yes	Für die Berechnung der sicheren Reaktionszeit werden ausschließlich synchrone Netzwerke mit gleichen Zykluszeiten oder ganzzahligen Verhältnissen der Zykluszeiten vorausgesetzt.	No	Keine Anforderung an die Synchronität der Netzwerke		
Parameter Wert	Beschreibung								
Yes	Für die Berechnung der sicheren Reaktionszeit werden ausschließlich synchrone Netzwerke mit gleichen Zykluszeiten oder ganzzahligen Verhältnissen der Zykluszeiten vorausgesetzt.								
No	Keine Anforderung an die Synchronität der Netzwerke								
Max_SDG_Powerlink_CycleTime_us	Dieser Parameter gibt die max. Zykluszeit des POWERLINK-Netzwerkes an, in dem die andere SafeLOGIC betrieben wird. <ul style="list-style-type: none"> Erlaubte Werte: 200 bis 30.000 µs (entspricht 0,2 bis 30 ms) 	5000	µs						
Max_Powerlink_CycleTime_us	Dieser Parameter gibt die max. POWERLINK Zykluszeit für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 200 bis 30.000 µs (entspricht 0,2 bis 30 ms) 	5000	µs						
Max_CPU_CrossLinkTask_CycleTime_us	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 dem selben POWERLINK-Netzwerk befinden. <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 3.000.000 µs (entspricht 0 bis 3 s) 	5000	µs						
Min_SDG_Powerlink_CycleTime_us	Dieser Parameter gibt die min. Zykluszeit des POWERLINK-Netzwerkes an, in dem die andere SafeLOGIC betrieben wird. <ul style="list-style-type: none"> Erlaubte Werte: 200 bis 30.000 µs (entspricht 0,2 bis 30 ms) 	200	µs						
Min_Powerlink_CycleTime_us	Dieser Parameter gibt die min. POWERLINK Zykluszeit für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 200 bis 30.000 µs (entspricht 0,2 bis 30 ms) 	200	µs						
Min_CPU_CrossLinkTask_CycleTime_us	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 dem selben POWERLINK-Netzwerk befinden. <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 3.000.000 µs (entspricht 0 bis 3 s) 	0	µs						
Worst_Case_Response_Time_us	Dieser Parameter gibt den Grenzwert für die Überwachung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 3000 bis 12.500.000 µs (entspricht 3 ms bis 12,5 s) Hinweis: Bei großen Werten auch den Parameter "Slow_Connection" beachten!	100000	µs						
Node_Guarding_Lifetime	Dieser Parameter gibt die max. Anzahl von Versuchen innerhalb der beim Parameter "Node_Guarding_Timeout_s" eingestellten Zeit an. Anhand dieser Versuche wird die Verfügbarkeit des Moduls sichergestellt. <ul style="list-style-type: none"> Erlaubte Werte: 1 bis 255 Hinweis <ul style="list-style-type: none"> Je größer der parametrisierte Wert, 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_us" bestimmt. 	5	-						
Max_SDG_Cycle_Time_us	Dieser Parameter gibt die max. Zykluszeit der anderen SafeLOGIC für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 800 bis 20.000 µs (entspricht 0,8 bis 20 ms) 	5000	µs						
Min_SDG_Cycle_Time_us	Dieser Parameter gibt die min. Zykluszeit der anderen SafeLOGIC für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 800 bis 20.000 µs (entspricht 0,8 bis 20 ms) 	1600	µs						
Slow_Connection	Dieser Parameter gibt an, ob es sich bei dieser Verbindung um eine langsame Verbindung handelt.	No	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes</td> <td>Es handelt sich um eine Verbindung mit großem Verhältnis zwischen SafeLOGIC Zykluszeit und Telegrammlaufzeit (wirkt sich intern auf die Parameterberechnung aus). Faustregel: "Yes" ab Verhältnis 50:1 (Telegrammlaufzeit : SafeLOGIC Zykluszeit)</td> </tr> <tr> <td>No</td> <td>Standard-Verbindung; Parameterberechnung unverändert</td> </tr> </tbody> </table>	Parameter Wert	Beschreibung	Yes	Es handelt sich um eine Verbindung mit großem Verhältnis zwischen SafeLOGIC Zykluszeit und Telegrammlaufzeit (wirkt sich intern auf die Parameterberechnung aus). Faustregel: "Yes" ab Verhältnis 50:1 (Telegrammlaufzeit : SafeLOGIC Zykluszeit)	No	Standard-Verbindung; Parameterberechnung unverändert		
Parameter Wert	Beschreibung								
Yes	Es handelt sich um eine Verbindung mit großem Verhältnis zwischen SafeLOGIC Zykluszeit und Telegrammlaufzeit (wirkt sich intern auf die Parameterberechnung aus). Faustregel: "Yes" ab Verhältnis 50:1 (Telegrammlaufzeit : SafeLOGIC Zykluszeit)								
No	Standard-Verbindung; Parameterberechnung unverändert								

Tabelle 33: Parameter SafeDESIGNER: Safety_Response_Time

Information:

Der Parameter "CPU_CrossLinkTask_CycleTime_us" wird benötigt wenn sich Source SL und SDG SL in unterschiedlichen Netzwerken oder auf unterschiedlichen Steuerungen befinden. Wenn dies nicht der Fall 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 Kopierzeiten zwischen den beteiligten Schnittstellen.

Information:

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, muss der Parameter aktiviert werden ("Slow_Connection = Yes").

7.3.6 Parameter für Verbindung - ab Release 1.10

Für die Kommunikation stehen ebenfalls Zykluszeitparameter zur Verfügung um die maximale Datenlaufzeit 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.

Information:

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.

Materialnummer: X20SL8100		
Description: X20 SafeLOGIC, POWERLINK V2, 24V, univ.		
SafeMODULE ID: 3		
Import file: -		
Parameter	Value	Unit
Basic		
Min required FW Rev	Basic Release	
Optional	No	
External UDID	No	
Safety Response Time		
Synchronous Network Only	Yes	
Safe Data Duration	20000	us
Additional Tolerated Packed Loss	0	packets
Slow Connection	No	
Node Guarding Lifetime	5	iterations
Max SDG Cycle Time	5000	us
Min SDG Cycle Time	1600	us

Gruppe: Basic

Parameter	Beschreibung	Default Wert	Einheit										
Min required FW Rev	Dieser Parameter ist für zukünftige Funktionserweiterungen reserviert.	Basic Release	-										
Optional	Mittels diesem Parameter kann das Modul "optional" parametrierbar 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.	No	-										
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>No</td> <td> <p>Das Modul ist für die Applikation zwingend erforderlich.</p> <p>Das Modul muss sich nach dem Hochlauf im OPERATIONAL Mode befinden und die sichere Kommunikation zur SafeLOGIC muss fehlerfrei aufgebaut sein ("SafeModuleOK = SAFETRUE"). Der Start der Abarbeitung der sicheren Applikation in der SafeLOGIC wird nach dem Hochlauf verzögert, bis dieser Zustand für alle Module mit "Optional = No" erreicht ist.</p> <p>Nach dem Hochlauf werden Modulprobleme mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt ein Eintrag ins Logbuch.</p> </td> </tr> <tr> <td>Yes</td> <td> <p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Yes" im OPERATIONAL Mode sind bzw. ob die sichere Kommunikation dieser Module zur SafeLOGIC korrekt aufgebaut ist oder nicht.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p> </td> </tr> <tr> <td>Startup</td> <td> <p>Das Modul ist optional. Während des Hochlaufs wird über das weitere Verhalten des Moduls entschieden.</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch vorhanden ist (unabhängig davon, ob es sich im Mode OPERATIONAL befindet oder nicht) so verhält sich das Modul wie bei "Optional = No".</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch nicht vorhanden ist, verhält sich das Modul wie bei "Optional = Yes".</p> </td> </tr> <tr> <td>NotPresent</td> <td> <p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = NotPresent" physikalisch vorhanden sind.</p> <p>Zum Unterschied zur Parametrierung "Optional = Yes" wird bei "Optional = NotPresent" das Modul nicht gestartet und somit das Hochlaufverhalten des Systems optimiert.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p> </td> </tr> </tbody> </table>	Parameter Wert	Beschreibung	No	<p>Das Modul ist für die Applikation zwingend erforderlich.</p> <p>Das Modul muss sich nach dem Hochlauf im OPERATIONAL Mode befinden und die sichere Kommunikation zur SafeLOGIC muss fehlerfrei aufgebaut sein ("SafeModuleOK = SAFETRUE"). Der Start der Abarbeitung der sicheren Applikation in der SafeLOGIC wird nach dem Hochlauf verzögert, bis dieser Zustand für alle Module mit "Optional = No" erreicht ist.</p> <p>Nach dem Hochlauf werden Modulprobleme mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt ein Eintrag ins Logbuch.</p>	Yes	<p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Yes" im OPERATIONAL Mode sind bzw. ob die sichere Kommunikation dieser Module zur SafeLOGIC korrekt aufgebaut ist oder nicht.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p>	Startup	<p>Das Modul ist optional. Während des Hochlaufs wird über das weitere Verhalten des Moduls entschieden.</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch vorhanden ist (unabhängig davon, ob es sich im Mode OPERATIONAL befindet oder nicht) so verhält sich das Modul wie bei "Optional = No".</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch nicht vorhanden ist, verhält sich das Modul wie bei "Optional = Yes".</p>	NotPresent	<p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = NotPresent" physikalisch vorhanden sind.</p> <p>Zum Unterschied zur Parametrierung "Optional = Yes" wird bei "Optional = NotPresent" das Modul nicht gestartet und somit das Hochlaufverhalten des Systems optimiert.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p>		
Parameter Wert	Beschreibung												
No	<p>Das Modul ist für die Applikation zwingend erforderlich.</p> <p>Das Modul muss sich nach dem Hochlauf im OPERATIONAL Mode befinden und die sichere Kommunikation zur SafeLOGIC muss fehlerfrei aufgebaut sein ("SafeModuleOK = SAFETRUE"). Der Start der Abarbeitung der sicheren Applikation in der SafeLOGIC wird nach dem Hochlauf verzögert, bis dieser Zustand für alle Module mit "Optional = No" erreicht ist.</p> <p>Nach dem Hochlauf werden Modulprobleme mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt ein Eintrag ins Logbuch.</p>												
Yes	<p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = Yes" im OPERATIONAL Mode sind bzw. ob die sichere Kommunikation dieser Module zur SafeLOGIC korrekt aufgebaut ist oder nicht.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p>												
Startup	<p>Das Modul ist optional. Während des Hochlaufs wird über das weitere Verhalten des Moduls entschieden.</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch vorhanden ist (unabhängig davon, ob es sich im Mode OPERATIONAL befindet oder nicht) so verhält sich das Modul wie bei "Optional = No".</p> <p>Wird während des Hochlaufs erkannt, dass das Modul physikalisch nicht vorhanden ist, verhält sich das Modul wie bei "Optional = Yes".</p>												
NotPresent	<p>Das Modul ist für die Applikation nicht erforderlich.</p> <p>Das Modul wird beim Hochlauf nicht betrachtet, d. h. die sichere Applikation wird gestartet unabhängig davon, ob Module mit "Optional = NotPresent" physikalisch vorhanden sind.</p> <p>Zum Unterschied zur Parametrierung "Optional = Yes" wird bei "Optional = NotPresent" das Modul nicht gestartet und somit das Hochlaufverhalten des Systems optimiert.</p> <p>Nach dem Hochlauf werden Modulprobleme NICHT mittels schnell blinkender "MXCHG" LED an der SafeLOGIC signalisiert. Außerdem erfolgt KEIN Eintrag ins Logbuch.</p>												
External UDID	Dieser Parameter aktiviert zum Modul die Möglichkeit, die erwartete UDID extern von der CPU vorgeben zu lassen.	No	-										
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes-ATTENTION</td> <td>Die UDID wird von der CPU vorgegeben. Bei einer Änderung der UDID ist ein Neustart der SafeLOGIC notwendig.</td> </tr> <tr> <td>No</td> <td>Die UDID wird mittels eines Teach-In-Verfahrens während der Inbetriebnahme vorgegeben.</td> </tr> </tbody> </table>	Parameter Wert	Beschreibung	Yes-ATTENTION	Die UDID wird von der CPU vorgegeben. Bei einer Änderung der UDID ist ein Neustart der SafeLOGIC notwendig.	No	Die UDID wird mittels eines Teach-In-Verfahrens während der Inbetriebnahme vorgegeben.						
Parameter Wert	Beschreibung												
Yes-ATTENTION	Die UDID wird von der CPU vorgegeben. Bei einer Änderung der UDID ist ein Neustart der SafeLOGIC notwendig.												
No	Die UDID wird mittels eines Teach-In-Verfahrens während der Inbetriebnahme vorgegeben.												

Tabelle 34: Parameter SafeDESIGNER: Basic

Gefahr!

Falls die Funktion "External UDID = Yes-ATTENTION" benutzt wird, können durch falsche Vorgaben von der CPU sicherheitskritische Situationen entstehen.

Führen Sie deshalb eine FMEA (Failure Mode and Effects Analysis) durch um diese Situationen zu erkennen und mittels zusätzlicher, sicherheitstechnischer Maßnahmen abzusichern.

Gruppe: Safety Response Time

Parameter	Beschreibung	Default Wert	Einheit						
Safe Data Duration	Dieser Parameter gibt die maximal erlaubte Datenlaufzeit zwischen der SafeLOGIC und dem SafeIO-Modul an. Weitere Informationen zur tatsächlichen Datenlaufzeit sind der Automation Help unter Diagnose und Service -> Diagnosewerkzeug -> Network Analyzer -> Editor -> Safety Laufzeitberechnung zu entnehmen. Zusätzlich ist die Zykluszeit der Sicherheitsapplikation zu addieren. <ul style="list-style-type: none"> Erlaubte Werte: 2000 bis 10.000.000 µs (entspricht 2 ms bis 10 s) 	20000	µs						
Additional Tolerated Packet Loss	Dieser Parameter gibt die Anzahl der bei der Datenübertragung zusätzlich tolerierten Paketverluste an. <ul style="list-style-type: none"> Erlaubte Werte: 0 bis 10 	0	Packets						
Slow Connection	Dieser Parameter gibt an, ob es sich bei dieser Verbindung um eine langsame Verbindung handelt.	No	-						
	<table border="1"> <thead> <tr> <th>Parameter Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Yes</td> <td>Es handelt sich um eine Verbindung mit großem Verhältnis zwischen SafeLOGIC Zykluszeit und Telegrammlaufzeit (wirkt sich intern auf die Parameterberechnung aus). Faustregel: "Yes" ab Verhältnis 50:1 (Telegrammlaufzeit : SafeLOGIC Zykluszeit)</td> </tr> <tr> <td>No</td> <td>Standard-Verbindung; Parameterberechnung unverändert</td> </tr> </tbody> </table>			Parameter Wert	Beschreibung	Yes	Es handelt sich um eine Verbindung mit großem Verhältnis zwischen SafeLOGIC Zykluszeit und Telegrammlaufzeit (wirkt sich intern auf die Parameterberechnung aus). Faustregel: "Yes" ab Verhältnis 50:1 (Telegrammlaufzeit : SafeLOGIC Zykluszeit)	No	Standard-Verbindung; Parameterberechnung unverändert
	Parameter Wert	Beschreibung							
Yes	Es handelt sich um eine Verbindung mit großem Verhältnis zwischen SafeLOGIC Zykluszeit und Telegrammlaufzeit (wirkt sich intern auf die Parameterberechnung aus). Faustregel: "Yes" ab Verhältnis 50:1 (Telegrammlaufzeit : SafeLOGIC Zykluszeit)								
No	Standard-Verbindung; Parameterberechnung unverändert								
Packets per Node Guarding	Dieser Parameter gibt die max. Anzahl von Paketen an, die für ein Node Guarding verwendet werden. <ul style="list-style-type: none"> Erlaubte Werte: 1 bis 255 Hinweis <ul style="list-style-type: none"> Je größer der parametrisierte Wert, desto höher das asynchrone Datenaufkommen. Diese Einstellung ist nicht sicherheitskritisch - die Zeit für die sichere Abschaltung der Aktoren wird unabhängig davon bestimmt. 	5	Packets						
Max SDG Cycletime	Dieser Parameter gibt die max. Zykluszeit der anderen SafeLOGIC für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 800 bis 20.000 µs (entspricht 0,8 bis 20 ms) 	5000	µs						
Min SDG Cycletime	Dieser Parameter gibt die min. Zykluszeit der anderen SafeLOGIC für die Berechnung der sicheren Reaktionszeit an. <ul style="list-style-type: none"> Erlaubte Werte: 800 bis 20.000 µs (entspricht 0,8 bis 20 ms) 	1600	µs						

Tabelle 35: Parameter SafeDESIGNER: Safety Response Time

Information:

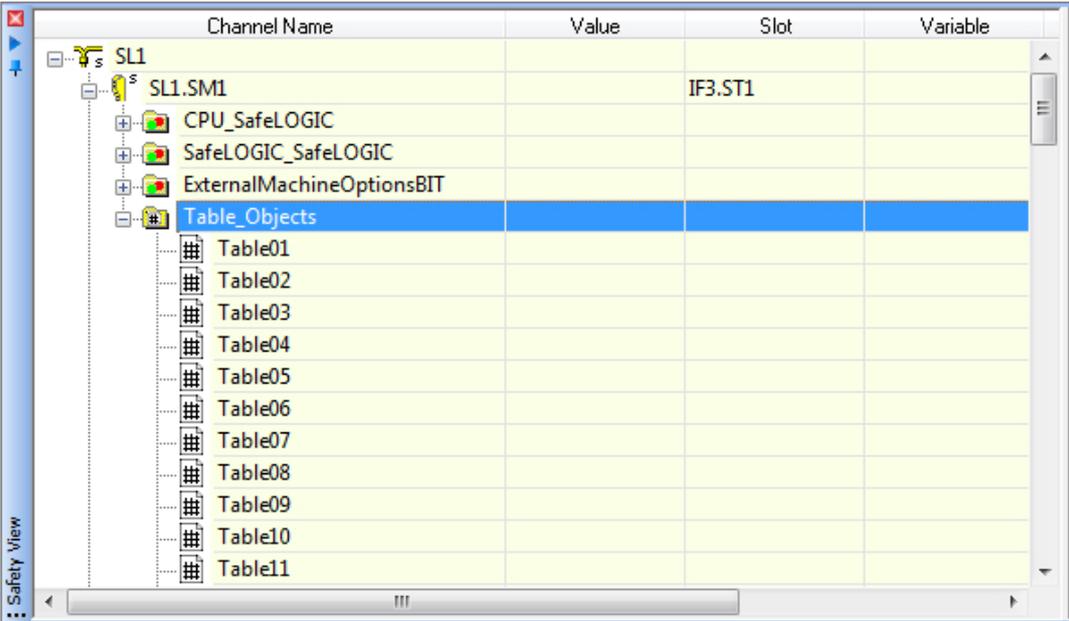
Über den Parameter "Slow Connection" kann zusätzlich noch angegeben werden, dass es sich bei der Verbindung zwischen Source SL und SDG SL um eine langsame Verbindung handelt. Wird für das Timeout der Verbindung ein Wert von einigen Sekunden benötigt, muss der Parameter aktiviert werden ("Slow Connection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

7.4 Tabellenobjekte

Unter einem Tabellenobjekt versteht sich eine CSV-Datei mit einer gewissen Struktur sowie Daten. Im SafeDESIGNER stehen unter der SafeLOGIC bis zu 99 sogenannte Tabellenobjekte zur Verfügung. Jedes Objekt stellt die Verbindung zu einer CSV-Datei mit den entsprechenden Daten dar. Zusätzlich gibt es im SafeDESIGNER die Bibliothek "Table_SF" für die Auswertung der verschiedenen Tabellenobjekte. Die Funktionsbausteine dieser Bibliothek müssen mit einem Tabellenobjekt verknüpft werden.

Information:

Die im SafeDESIGNER implementierten Prüfungs- und Lock-Funktionen, zusammen mit der Validierung der Tabellendaten durch den Anwender, erlauben die Verwendung von COTS (Commercial off-the-shelf) Editoren für Tabellendaten.



Channel Name	Value	Slot	Variable
SL1			
SL1.SM1		IF3.ST1	
CPU_SafeLOGIC			
SafeLOGIC_SafeLOGIC			
ExternalMachineOptionsBIT			
Table_Objects			
Table01			
Table02			
Table03			
Table04			
Table05			
Table06			
Table07			
Table08			
Table09			
Table10			
Table11			

Die nötigen Einstellungen für die Tabellenobjekte werden über Parameter der SafeLOGIC gesteuert. Hier gibt es einen eigenen Reiter "Tables". Für jedes Tabellenobjekt können folgende Einstellungen getroffen werden:

- TableSource → woher kommen die Tabellendaten
 - NOT used → Tabellenobjekt wird nicht verwendet
 - SafeDESIGNER download → Daten werden mit der Applikation übertragen
 - Remote download → Daten werden nicht mit der Applikation übertragen. Diese müssen nachträglich über die AsSafety Bibliothek übertragen werden.
- TableType → um welchen Tabellentyp handelt es sich
 - A - Q
 - R - Z → Tabellentypen für SafeROBOTIC

Model no.:	X20SL8010
Description:	X20 SafeLOGIC, POWERLINK V2, SafeMC
SafeMODULE ID:	1
Import file:	

Parameter	Value
Tables	
TableSource_01	SafeDESIGNER download
TableType_01	A
TableSource_02	NOT used
TableType_02	A
TableSource_03	NOT used
TableType_03	A
TableSource_04	NOT used
TableType_04	R
TableSource_05	NOT used
TableType_05	A
TableSource_06	NOT used
TableType_06	A
TableSource_07	NOT used

Navigation: Basic | Safety_Response_Time_Defaults | **Tables** | ALL

Information:

Details zum Aufbau der Tabellenobjekte bzw. der Daten finden sich in der Hilfe des zu verwendenden Funktionsbausteins.

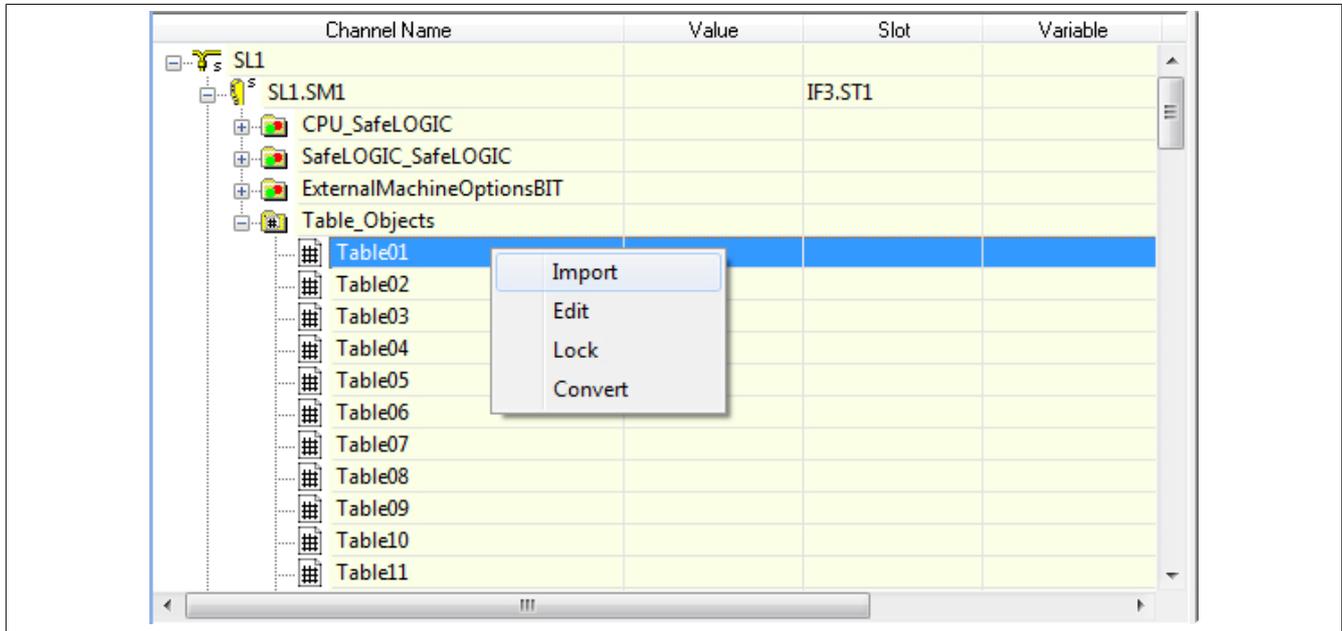
7.4.1 Ablauf

Zu Beginn muss für jedes Tabellenobjekt der richtige Typ sowie die Source eingestellt werden.

Information:

Wird ein Tabellenobjekt in der Applikation verwendet und ist jedoch der "TableSource" Parameter auf "NOT used" eingestellt, führt dies beim Kompilieren zu einer Fehlermeldung.

Über das Kontextmenü (Rechtsklick auf ein Tabellenobjekt) können verschiedene Aktionen ausgeführt werden.



7.4.1.1 Import

Über diesen Menüpunkt kann eine bestehende CSV-Datei mit entsprechenden Daten, die passend zum ausgewählten Tabellentyp sind, importiert werden.

Information:

Wird eine Datei importiert, welche nicht zum Tabellentyp passt, führt dies beim Kompilieren zu einer Fehlermeldung.

7.4.1.2 Edit

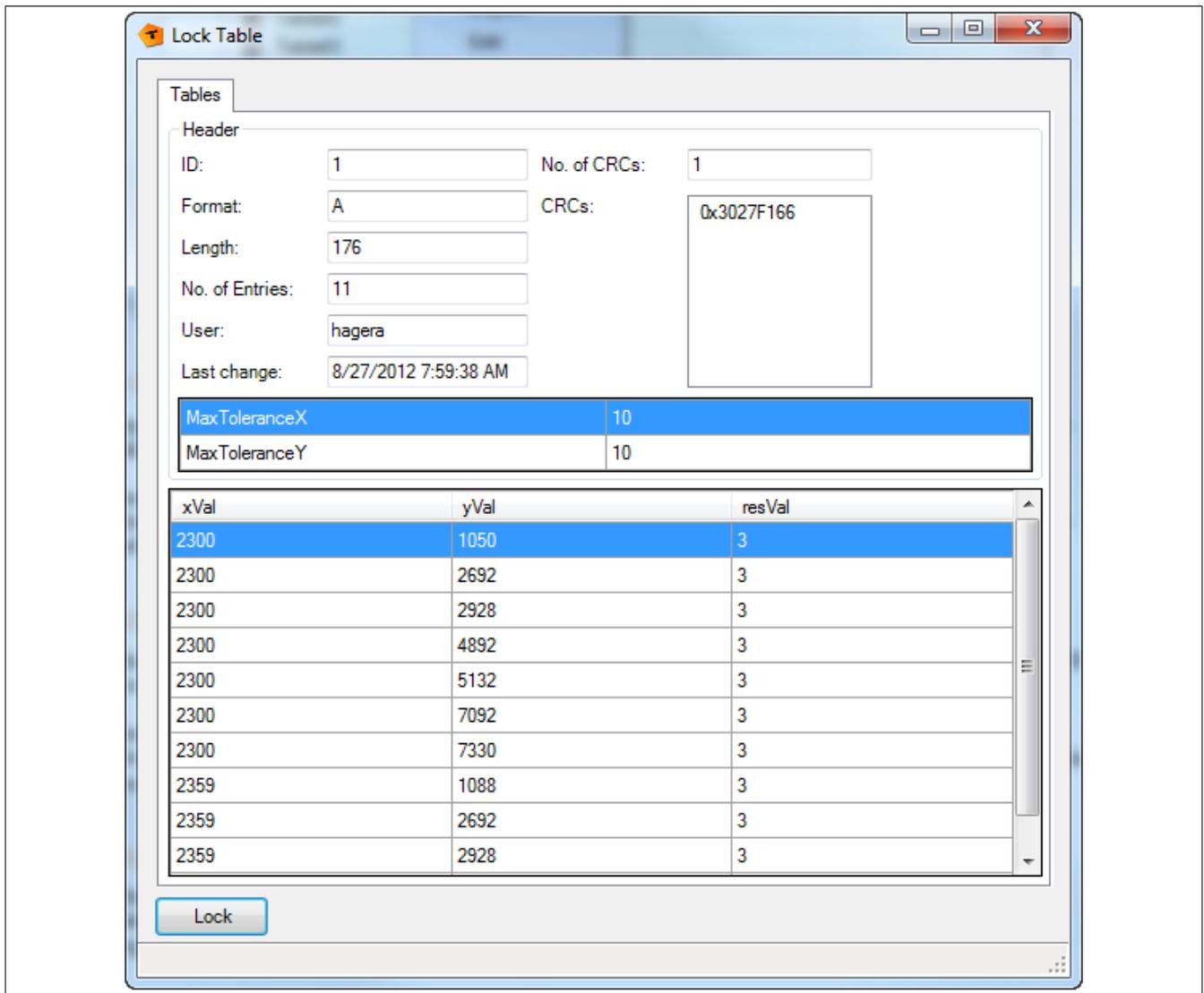
Über diesen Menüpunkt kann die Datei mit dem eingestellten Standardprogramm für CSV-Dateien (z. B. Excel) editiert werden.

Information:

Wird eine Datei bearbeitet ist es zwingend erforderlich diese Datei wieder zu sperren - über "Lock" - da ansonsten die CRC der Datei nicht passt.

7.4.1.3 Lock

Über diesen Menüpunkt wird die Datei gesperrt und über den aktuellen Inhalt eine CRC gerechnet. Gleichzeitig werden die Daten passend zum ausgewählten Tabellentyp im Fenster noch einmal angezeigt.

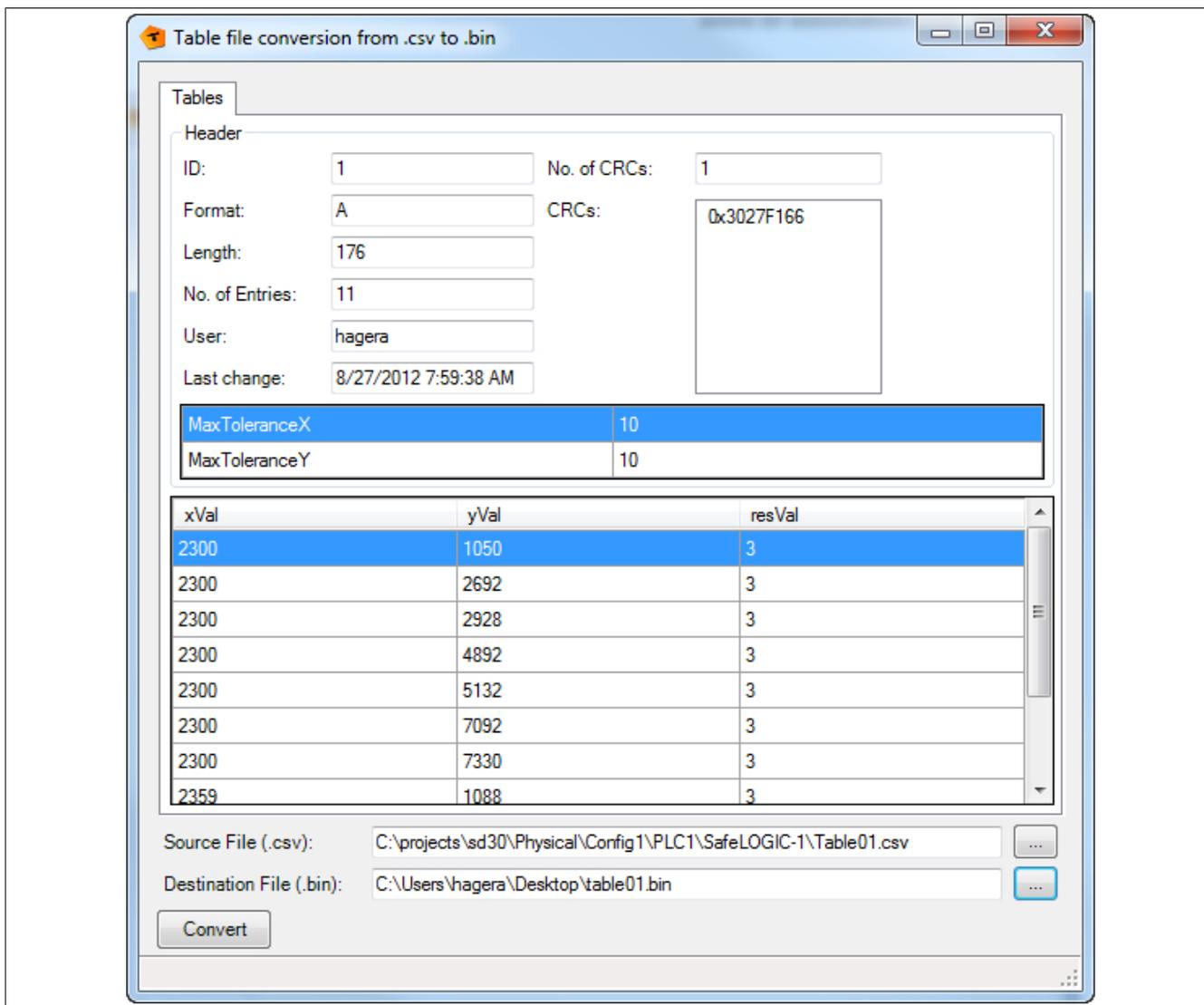


Information:

Sollte es Probleme mit der Datei geben, werden in diesem Fenster auch Fehlermeldungen ausgegeben (z. B. Format passt nicht, Datei konnte nicht geöffnet werden, etc.).

7.4.1.4 Convert

Über diesen Menüpunkt kann eine Konvertierung der Datei ins Binärformat für die SafeLOGIC vorgenommen werden. Es muss der entsprechende Pfad für das Ablegen der Binärdatei angegeben werden.



Information:

Diese Binärdatei kann dann für den Download über die funktionale CPU verwendet werden.

7.4.2 Verwendung in der Applikation

Für die Verwendung der Tabellenobjekte muss zu Beginn ein zugehöriger Funktionsbaustein in der Applikation verwendet werden (siehe dazu auch Bibliothek "Table_SF").

Der Eingang "S_TableID" muss mit einem Tabellenobjekt verknüpft werden. Dazu wird in der Safety View das Tabellenobjekt markiert und mit gedrückter linker Maustaste in die Applikation gezogen - optional kann für die Verbindung ein aussagekräftiger Name vergeben werden.

Information:

Im Falle eines Problems oder eines Fehlers wird beim Kompilieren eine Fehlermeldung ausgegeben.

7.5 Blackout-Modus

Der Blackout-Modus ermöglicht es Anwendern, nach dem Ausfall von Teilen eines B&R Systems die Abarbeitung der Applikation in untergeordneten Teilsystemen aufrecht zu erhalten. Das B&R System bietet damit - unabhängig vom Einsatz von Redundanztechnologien - die Möglichkeit, auf systemkritische Situationen anwendungsspezifisch zu reagieren.

Der Einsatz Blackout-fähiger Module ist bei folgenden Anforderungen empfehlenswert:

- Exit-Routinen bei Systemausfall, z. B. um das Öffnen einer Presse bei Systemausfall zu ermöglichen.
- Halten bzw. kontrolliertes Setzen eines Ausgangs bei Systemausfall, z. B. automatisches Schließen von Zuflussventilen.
- Verzögerungssequenzen bei Systemausfall, z. B. Reduzieren von Motorgeschwindigkeiten vor dem Senden eines Stoppbefehls.

Bei entsprechender Parametrierung der Blackout-fähigen Module wird der Blackout-Modus ausgeführt, wenn die Netzwerkverbindung zum übergeordneten Controller bzw. zur übergeordneter CPU unterbrochen wird.

Sobald die Störung des Netzwerkes behoben wurde, wird der Blackout-Modus selbstständig von den Modulen beendet und stoßfrei mit dem Netzwerk synchronisiert.

Voraussetzungen zum Betrieb

Um den Blackout-Modus benutzen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Das verwendete Modul muss den Blackout-Modus unterstützen.
- Im Automation Studio muss der Parameter "Blackout mode" aktiviert sein.

7.5.1 Anwendungsbereiche

Durch den Einsatz von Blackout-fähigen Modulen kann ein Teil der Steuerung auch funktionsfähig bleiben, wenn die Netzwerk- oder X2X Link Verbindung zwischen den Modulen gestört wird.

7.5.1.1 Verlust der POWERLINK-Verbindung

Ausgangssituation

In einer Anwendung sind mehrere Stationen mittels Netzkabel mit der CPU verbunden. Durch einen Störfall wird die Datenübertragung zwischen der CPU und den Stationen unterbrochen.

Auswirkung

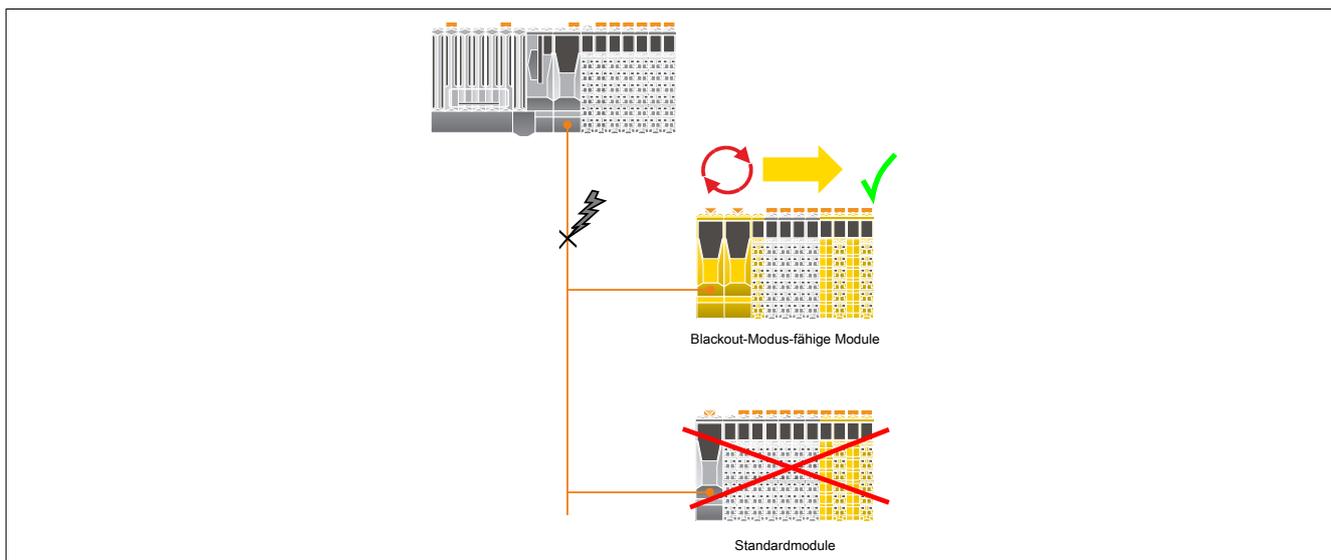
Nicht Blackout-fähige Module werden zurückgesetzt und im Standardverhalten betrieben.

Blackout-fähige Module zeigen folgendes Verhalten:

- Die programmierte Funktion wird weiter ausgeführt.
- Untergeordnete Netzwerke funktionieren weiterhin.
- Daten von der CPU werden mit "0" initialisiert.
- Das Modul fügt sich nach dem Beheben der Störung wieder stoßfrei in das übergeordnete Netzwerk ein.

Warnung!

Der Blackout-Modus führt zu einer Initialisierung der Daten von der CPU mit "0". Wird der Blackout-Modus in Kombination mit "Ausgangsinvertierung" verwendet, kann dies zu einem ungewolltem Setzen von Ausgängen führen.



7.5.1.2 Verlust der X2X Link Verbindung

Ausgangssituation

In einer Anwendung sind Module mittels X2X Link Kabel mit dem Netzwerk verbunden. Durch einen Defekt des X2X Link Kabels wird die Datenübertragung zwischen der CPU und den Modulen unterbrochen.

Auswirkung

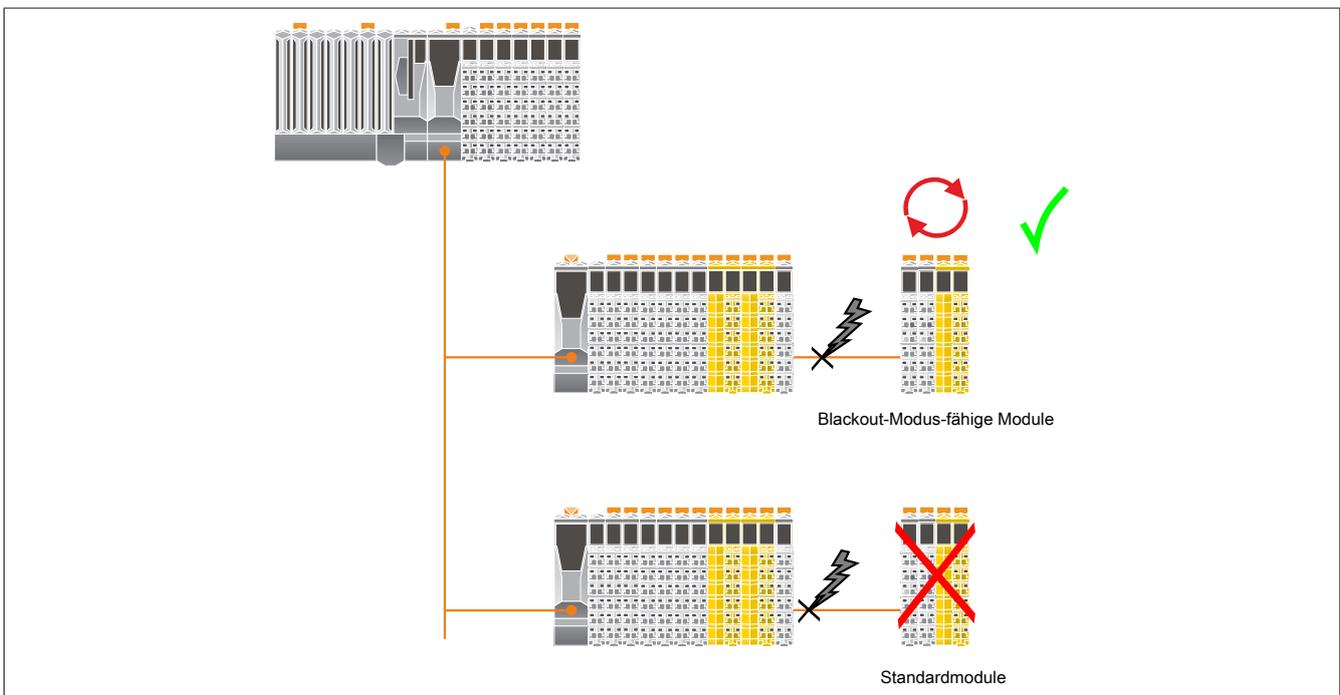
Nicht Blackout-fähige Module werden zurückgesetzt und im Standardverhalten betrieben.

Blackout-fähige Module zeigen folgendes Verhalten:

- Die programmierte Funktion wird weiter ausgeführt.
- Untergeordnete Netzwerke funktionieren weiterhin.
- Daten von der CPU werden mit "0" initialisiert.
- Das Modul fügt sich nach dem Beheben der Störung wieder stoßfrei in das übergeordnete Netzwerk ein.

Warnung!

Der Blackout-Modus führt zu einer Initialisierung der Daten von der CPU mit "0". Wird der Blackout-Modus in Kombination mit "Ausgangsinvertierung" verwendet, kann dies zu einem ungewolltem Setzen von Ausgängen führen.



7.5.2 Programmierung des Blackout-Modus

Der Blackout-Modus kann von den Blackout-fähigen Modulen selbst nicht erkannt werden. Falls es in einer Applikation notwendig ist, ein spezielles Blackout-Verhalten zu programmieren, muss deshalb ein indirektes Verfahren gewählt werden.

Eine Möglichkeit ist, in der dem Blackout-fähigen Modul übergeordneten CPU einen Zähler zu implementieren und diesen zyklisch abzufragen. Der Blackout-Modus würde sich in diesem Fall durch einen sich nicht mehr ändernden Zählerwert oder durch einen Nullwert im Zähler bemerkbar machen.

Die Blackout-fähigen Module selbst lassen sich in 2 Kategorien einteilen:

- **Programmierbare Module**
Die Blackout-Funktion wird auf der Basis bestehender Funktionsbausteine programmiert, das heißt, es werden die bestehenden Technologien der Applikationsprogrammierung oder der reACTION Technology verwendet.
Die Blackout-Funktion wird dabei weitgehend unabhängig von anderen Systemkomponenten abgearbeitet.
- **Standardfunktionsmodule**
Diese Module sind nicht programmierbar, sondern behalten im Falle des Blackout-Modus ihr Standardverhalten bei.

7.5.3 Standalone-Funktion

Die Standalone-Funktion ist eine Erweiterung des Blackout-Modus. Nach dem Einschalten der Stromversorgung wird unabhängig von einer bestehenden Netzwerkverbindung sofort der Blackout-Modus aktiviert. Das heißt, nach dem Einschalten der Stromversorgung beginnt das Modul die zuletzt abgespeicherte Konfiguration bzw. Applikation abzuarbeiten, ohne auf eine Aktivität bzw. einen Abgleich mit einer übergeordneten CPU bzw. SafeLOGIC zu warten.

Sobald das Netzwerk aktiv wird, synchronisiert sich das Modul stoßfrei auf das bestehende Netzwerk auf.

Warnung!

Standalone-Module verhalten sich während des Hochfahrens des Systems und bis zum Aufbau der Netzwerkverbindung identisch zum Blackout-Modus. Daher ist ihr Einsatz mit besonderer Sorgfalt durchzuführen!

Voraussetzungen zum Betrieb

Um die Standalone-Funktion benutzen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Das verwendete Modul muss die Standalone-Funktion unterstützen.
- Im Automation Studio muss der Parameter "Standalone mode" aktiviert sein.
- Für die Standalone-Funktion am Bus Controller (z. B. X20SL8101) ist der Blackout-Modus für mindestens 1 Modul am lokalen X2X Link aktiviert.
- Das Modul muss zuvor mindestens einmal mit einer CPU betrieben worden sein, damit eine gültige Konfiguration vorliegt.

Information:

Die Verwendung der Standalone-Funktion ist in Verbindung mit DNA nicht zulässig. Es müssen fest eingestellte Adressen verwendet werden.

Warnung!

Folgende Aspekte sind besonders zu berücksichtigen:

- **Das Modul muss (dauerhaft) eindeutig gekennzeichnet sein, um sein vom Standard abweichendes Verhalten zu markieren.**
- **Wartungstechniker müssen mit dem besonderen Verhalten dieser Module vertraut sein.**
- **Vor dem Stecken der Feldklemme auf ein Modul mit aktivierter Standalone-Funktion muss zumindest eine der folgenden Bedingungen erfüllt sein:**
 - **Es muss sichergestellt sein, dass das Modul wirklich mit der Standalone-Funktion betrieben werden soll und die korrekte Version der Parametrierung am Modul geprüft wurde.**
 - **Die Blinksequenz des Moduls zeigt den "normalen, netzwerkgebundenen operational State" des Moduls an.**

7.5.3.1 Anwendungsbereich

Ausgangssituation

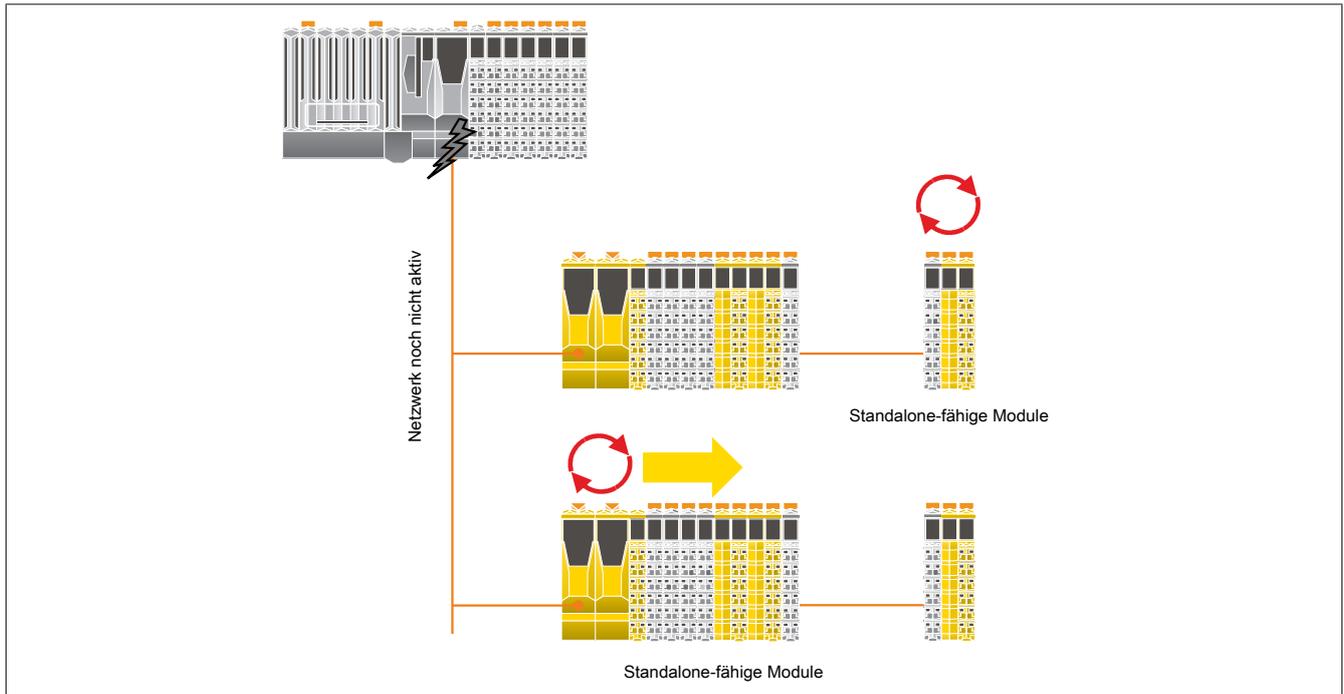
In einer Anwendung sind mehrere Stationen mittels Netzkabel mit der CPU verbunden. Nach dem Aus- und Einschalten des gesamten Systems kommt es durch einen Störfall nicht zum Aufbau der Netzwerkverbindung.

Auswirkung

Nicht Standalone-fähige Module werden erst nach Hochlauf der Anwendung in den aktiven Zustand versetzt.

Standalone-fähige Module zeigen folgendes Verhalten:

- Der Boot-Vorgang startet, ohne auf ein übergeordnetes Netzwerk zu warten.
- Das Modul verhält sich Identisch zum Blackout-Modus.
- Sobald das Netzwerk aktiv wird, fügt es sich stoßfrei in das übergeordnete Netzwerk ein.



7.6 Setup-Modus

Der Setup-Modus unterstützt den Anwender bei der Inbetriebnahme.

Der Setup-Modus wird ab Hardware-Upgrade 1.10.2.x unterstützt.

Für die Verwendung des Setup-Modus ist Automation Runtime B4.26 oder höher erforderlich.

Der aktive Setup-Modus wird sowohl über die FAILSAFE-LED (X20SL81xx-Serie) bzw. über die SE-LED (X20SLXxxx-Serie) als auch einen Eintrag im Logbuch signalisiert.

Bei aktivem Setup-Modus sind die Quittierungsanforderungen "SafeKEY Exchange", "Firmware Acknowledge" und "UDID Mismatch" nicht mehr notwendig.

Der Setup-Modus kann sowohl über die Bedienelemente der "Remote Control" im SafeDESIGNER (X20SL81xx-Serie und X20SLXxxx-Serie) als auch über den Auswahlschalter und Bestätigungstaster (X20SL81xx-Serie) aktiviert und deaktiviert werden.

Gefahr!

**Der Setup-Modus darf nur während der Inbetriebnahme der Maschine/Anlage aktiviert sein.
Im laufenden Betrieb muss der Setup-Modus deaktiviert sein.**

Gefahr!

Nach Beendigung des Setup-Modus muss ein Funktionstest inklusive Verdrahtungstest durchgeführt werden.

Wenn während aktivem Setup-Modus ein SafeKEY-Tausch oder ein SafeLOGIC-Tausch erfolgt, wird der Setup-Modus deaktiviert.

Auch in diesem Fall muss ein Funktionstest durchgeführt werden.

Der Funktionstest darf nur von Personen durchgeführt werden, welche mit der Sicherheitsapplikation und deren Funktionen vertraut sind.

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

8 Sichere Reaktionszeit

Als sichere Reaktionszeit wird die Zeit zwischen Eintreffen des Signals am Eingangskanal und Ausgabe des Abschaltsignals am Ausgang bezeichnet.

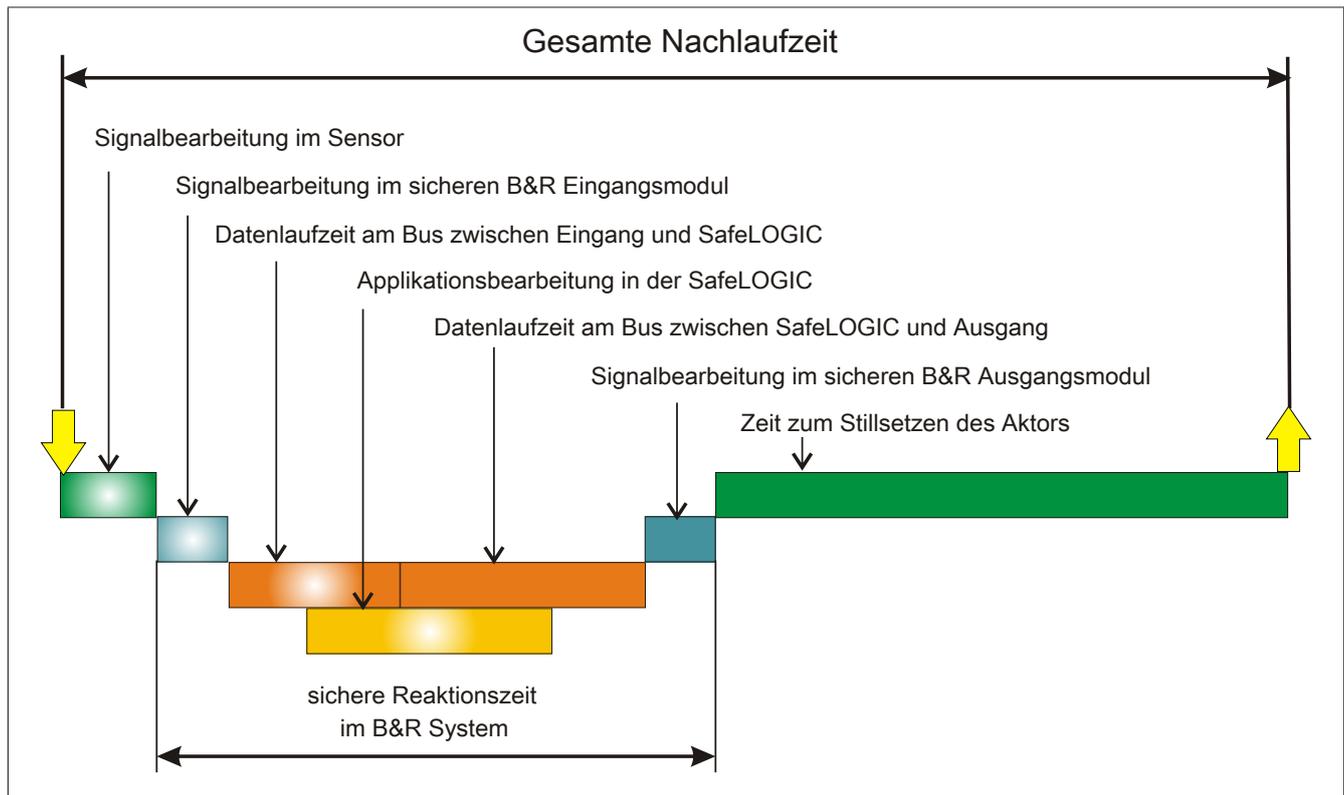


Abbildung 17: Gesamte Nachlaufzeit

Wie in der Abbildung ersichtlich setzt sich die sichere Reaktionszeit im B&R System aus folgenden Teil-Reaktionszeiten zusammen:

- Signalbearbeitung im sicheren B&R Eingangsmodul
- Datenlaufzeit am Bus zwischen Eingang und SafeLOGIC
- Datenlaufzeit am Bus zwischen SafeLOGIC und Ausgang
- Signalbearbeitung im sicheren B&R Ausgangsmodul

Gefahr!

Die folgenden Kapitel berücksichtigen ausschließlich die sichere Reaktionszeit im B&R System. Für die Betrachtung der gesamten sicherheitstechnischen Reaktionszeit muss der Anwender zwingend die Signalbearbeitung im Sensor sowie die Zeit zum Stillsetzen des Aktors mit berücksichtigen.

Führen Sie in jedem Fall eine Validierung der gesamten Nachlaufzeit an der Anlage durch!

Information:

Die sichere Reaktionszeit im B&R System beinhaltet bereits alle Verzögerungen, die durch das Sampling der Eingangsdaten verursacht werden (Abtasttheorem).

8.1 Signalbearbeitung im sicheren B&R Eingangsmodul

Für die Signalbearbeitung im sicheren B&R Eingangsmodul muss die maximale I/O-Updatezeit im Kapitel "I/O-Updatezeit" des entsprechenden Moduls beachtet werden.

8.2 Datenlaufzeit am Bus

Für die Datenlaufzeiten am Bus muss folgender Zusammenhang betrachtet werden:

- Die Datenlaufzeit vom Eingang zur SafeLOGIC bzw. zum Ausgang ergibt sich aus der Summe der an der Übertragungsstrecke beteiligten Zykluszeiten bzw. CPU-Kopierzeiten.
- Für das tatsächliche Zeitverhalten am Bus sind die Einstellungen im POWERLINK MN (Managing Node, funktionale CPU) entscheidend, jedoch sind diese Einstellungen sicherheitstechnisch nicht anwendbar, da diese Werte jederzeit im Zuge von Modifikationen außerhalb der Sicherheitsapplikation geändert werden können.
- In der SafeLOGIC werden über die Services von openSAFETY die Datenlaufzeiten am Bus überwacht. In dieser Prüfung ist systembedingt die Zeit für die Abarbeitung der Applikation in der SafeLOGIC eingerechnet. Die Überwachung wird dabei von den Parametern der Parametergruppe "Safety Response Time" im SafeDESIGNER definiert.

Information:

Kommt es auf Grund veränderter Parameter im POWERLINK MN zu veränderten Datenlaufzeiten am Bus, die außerhalb der im SafeDESIGNER in der Parametergruppe "Safety Response Time" festgelegten Parameter liegen, so kann es in diesem Netzwerksegment zur Abschaltung von Sicherheitskomponenten durch die SafeLOGIC kommen.

Information:

Kommt es auf Grund von EMV Störungen zu Datenausfällen, die außerhalb der im SafeDESIGNER in der Parametergruppe "Safety Response Time" festgelegten Parameter liegen, so kann es in diesem Netzwerksegment zur Abschaltung von Sicherheitskomponenten durch die SafeLOGIC kommen.

Berechnung der maximalen Datenlaufzeit - bis Release 1.9:

- Die gesamte max. Datenlaufzeit am Bus ergibt sich aus der Addition des Parameters "Worst_Case_Response_Time_us" des sicheren Eingangsmoduls und des Parameters "Worst_Case_Response_Time_us" des sicheren Ausgangsmoduls. Dabei ist der Parameter "Manual_Configuration" zu beachten. Ist der Parameter "Manual_Configuration" auf "No" konfiguriert, so wird der beim Parameter "Default_Worst_Case_Response_Time_us" eingestellte Wert verwendet.
- **Sonderfall: Lokale Eingänge am X20SLX Modul:**
Die gesamte max. Datenlaufzeit am Bus ergibt sich aus der Addition des Parameters "Cycle_Time_max_us" + 2000 µs und des Parameters "Worst_Case_Response_Time_us" des sicheren Ausgangsmoduls. Dabei ist der Parameter "Manual_Configuration" zu beachten. Ist der Parameter "Manual_Configuration" auf "No" konfiguriert, so wird der beim Parameter "Default_Worst_Case_Response_Time_us" eingestellte Wert verwendet.

Berechnung der maximalen Datenlaufzeit - ab Release 1.10:

Für die Berechnung der Datenlaufzeit zwischen sicherem Eingangsmodul und sicherem Ausgangsmodul sind folgende Parameter relevant, wobei der Parameter "Manual Configuration" zu beachten ist.

- Relevante Parameter bei "Manual Configuration = No":
 - "PacketLoss1": Parameter "Default Additional Tolerated Packet Loss" der Gruppe "Safety Response Time Defaults" der SafeLOGIC
 - "DataDuration1": Parameter "Default Safe Data Duration" der Gruppe "Safety Response Time Defaults" der SafeLOGIC
 - "NetworkSyncCompensation1": 12 ms
 - "PacketLoss2": identisch zu "PacketLoss1"
 - "DataDuration2": identisch zu "DataDuration1"
 - "NetworkSyncCompensation2": identisch zu "NetworkSyncCompensation1"
- Relevante Parameter bei "Manual Configuration = Yes":
 - "PacketLoss1": Parameter "Additional Tolerated Packet Loss" der Gruppe "Safety Response Time" des sicheren Eingangsmoduls
 - "DataDuration1": Parameter "Safe Data Duration" der Gruppe "Safety Response Time" des sicheren Eingangsmoduls
 - "NetworkSyncCompensation1": 12 ms
 - "PacketLoss2": Parameter "Additional Tolerated Packet Loss" der Gruppe "Safety Response Time" des sicheren Ausgangsmoduls
 - "DataDuration2": Parameter "Safe Data Duration" der Gruppe "Safety Response Time" des sicheren Ausgangsmoduls
 - "NetworkSyncCompensation2": identisch zu "NetworkSyncCompensation1"
- **Sonderfall: Lokale Eingänge am X20SLX-Modul:**
 - "PacketLoss1": 0
 - "DataDuration1": Parameter "Cycle Time max" der Gruppe "Module Configuration" der X20SLX + 2000 µs
 - "NetworkSyncCompensation1": 0 ms
- **Sonderfall: Lokale Ausgänge am X20SLX-Modul:**
 - "PacketLoss2": 0
 - "DataDuration2": Parameter "Cycle Time max" der Gruppe "Module Configuration" der X20SLX + 2000 µs
 - "NetworkSyncCompensation2": 0 ms
- **Sonderfall: Verknüpfung lokaler Eingänge mit lokalen Ausgängen am X20SRT-Modul:**
 - "PacketLoss1": 0
 - "PacketLoss2": 0
 - "DataDuration1": Parameter "Cycle time" der Gruppe "General"
 - "DataDuration2": Parameter "Cycle time" der Gruppe "General"
 - "NetworkSyncCompensation1": 0 ms
 - "NetworkSyncCompensation2": 0 ms

Die maximale Datenlaufzeit zwischen sicherem Eingangsmodul und sicherem Ausgangsmodul ergibt sich aus folgender Rechnung:

Maximale Datenlaufzeit = (PacketLoss1+1)* DataDuration1 + NetworkSyncCompensation1 + (PacketLoss2+1)* DataDuration2 + NetworkSyncCompensation2

Information:

Zusätzlich zur Datenlaufzeit am Bus ist die Zeit für die Signalbearbeitung im sicheren B&R Ein- und Ausgangsmodul (siehe Abschnitt 8 "[Sichere Reaktionszeit](#)") zu berücksichtigen.

Information:

Weitere Informationen zur tatsächlichen Datenlaufzeit sind der Automation Help unter Diagnose und Service -> Diagnosewerkzeug -> Network Analyzer -> Editor -> Safety Laufzeitberechnung zu entnehmen. Zusätzlich ist die Zykluszeit der Sicherheitsapplikation zu addieren.

8.3 Signalbearbeitung im sicheren B&R Ausgangsmodul

Für die Signalbearbeitung im sicheren B&R Ausgangsmodul muss die maximale I/O-Updatezeit im Kapitel "I/O-Updatezeit" des entsprechenden Moduls beachtet werden.

8.4 Minimale Signallängen

Die Parameter der Parametergruppe "Safety Response Time" im SafeDESIGNER beeinflussen die max. Anzahl der Datenpakete, welche ausfallen dürfen, ohne dass eine sicherheitstechnische Reaktion ausgelöst wird. Somit wirken diese Parameter wie ein Ausschaltfilter. Bei einem Verlust mehrerer Datenpakete innerhalb der tolerierten Anzahl kann es daher zu einem Nicht-Erkennen sicherheitstechnischer Signale kommen, wenn deren Low-Phase kürzer ist, als die ermittelte Datenlaufzeit.

Gefahr!

Der Verlust von Signalen kann zu schwerwiegenden, sicherheitstechnischen Problemen führen. Prüfen Sie bei allen Signalen die mögliche minimale Impulslänge und stellen Sie sicher, dass diese größer ist als die ermittelte Datenlaufzeit.

Lösungsvorschlag:

- Beim Eingangsmodul kann mit dem Einschaltfilter die Low-Phase eines Signals verlängert werden.
- Low-Phasen von Signalen der SafeLOGIC können mit den Funktionen der Wiederanlaufsperrern oder mit Timer Bausteinen verlängert werden.

9 Bestimmungsgemäße Verwendung

Gefahr!

Gefährdung durch falsche Anwendung der sicherheitstechnischen Produkte/Funktionen

Nur wenn die Produkte/Funktionen gemäß ihrer bestimmungsgemäßen Verwendung, von qualifiziertem Personal und unter Berücksichtigung der angeführten Sicherheitshinweise eingesetzt werden, ist die ordnungsgemäße Funktion gegeben. Die genannten Bedingungen sind einzuhalten oder eigenverantwortlich mit ergänzenden Maßnahmen abzudecken um die spezifizierten Schutzfunktionen sicherzustellen.

9.1 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.

9.2 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-Halt 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.

9.3 Security Konzept

B&R Produkte kommunizieren über eine Netzwerkschnittstelle und wurden für die Einbindung in ein sicheres Netzwerk entwickelt. Auf das Netzwerk und die B&R-Produkte wirken unter anderem folgende Gefahren ein:

- Unautorisierter Zugriff
- Digitaler Einbruch (intrusion)
- Datenpannen (data leakage)
- Datendiebstahl
- Eine Vielzahl anderer Arten von IT-Sicherheitsverstößen (IT security breaches)

Es obliegt dem Betreiber, eine sichere Verbindung zwischen B&R-Produkten und dem internen Netzwerk, gegebenenfalls auch anderen Netzwerken wie dem Internet, bereitzustellen und aufrecht zu erhalten. Hierfür sind unter anderem folgende Maßnahmen bzw. Sicherheitslösungen geeignet:

- Segmentieren des Netzwerks (z. B. Trennung des IT- und OT -Netzwerks)
- Firewalls für die sichere Verbindung der Netzwerksegmente
- Umsetzung eines sicherheitsoptimierten Benutzerkonten- und Passwort-Konzeptes
- Intrusion Prevention- und Authentifizierungs-Systeme
- Endpoint Security-Lösungen mit Modulen wie Anti-Malware, Data Leakage Prevention, etc.
- Datenverschlüsselung

Es liegt in der Verantwortung des Betreibers, geeignete Maßnahmen zu ergreifen und wirksame Sicherheitslösungen einzusetzen.

Die B&R Industrial Automation GmbH und ihre Tochtergesellschaften haften nicht für Schäden und/oder Verluste, die beispielweise aus IT-Sicherheitsverstößen, unautorisiertem Zugriff, digitalem Einbruch, Datenpannen und/oder Datendiebstahl resultieren.

Bevor B&R Produkte oder Updates freigibt, werden diese entsprechenden Funktionstests unterzogen. Unabhängig davon wird die Entwicklung eigener Testprozesse empfohlen, um Auswirkungen von Änderungen vorab überprüfen zu können. Zu solchen Änderungen zählen:

- Installation von Produkt-Updates
- Nennenswerte System-Modifikationen wie Konfigurations-Änderungen
- Einspielen von Updates oder Patches für Dritt-Software (non-B&R Software)
- Austausch von Hardware

Diese Tests sollen sicherstellen, dass implementierte Sicherheitsmaßnahmen wirksam bleiben und dass sich die Systeme wie erwartet verhalten.

9.4 Haftungsausschluss Sicherheitstechnik

Der fachgerechte Einsatz aller B&R Produkte ist vom Kunden durch geeignete Schulungs-, Instruktionen- und Dokumentationsmaßnahmen sicherzustellen. Zu beachten sind dabei die in den Handbüchern der Systeme festgelegten Richtlinien. B&R trifft keinerlei Prüf- und/oder Warnpflicht bezüglich des vom Kunden beabsichtigten Einsatzzwecks des gelieferten Produktes.

Beim Einsatz von sicherheitstechnischen Komponenten dürfen keine Änderungen an den Geräten vorgenommen werden. Es dürfen ausschließlich zertifizierte Produkte verwendet werden. Die jeweils aktuellen, gültigen Produktversionen sind in den entsprechenden Zertifikaten gelistet. Die aktuellen Zertifikate sind auf der B&R Homepage (www.br-automation.com) im Download-Bereich der jeweiligen Produkte verfügbar. Der Einsatz von nicht zugelassenen Produkten oder Produktversionen ist nicht zulässig.

Vor der Anwendung sicherheitstechnischer Produkte sind unbedingt alle relevanten Informationen in den jeweils aktuellsten Versionen der Datenblätter der verwendeten Produkte zu lesen und die entsprechenden Sicherheitshinweise zu beachten. Die zertifizierten Datenblätter sind auf der B&R Homepage (www.br-automation.com) im Download-Bereich der jeweiligen Produkte verfügbar.

B&R schließt für sich und seine Mitarbeiter jede Haftung für Schäden und Aufwände aus, welche durch eine Falschanwendung der Produkte verursacht werden. Das gilt auch für Falschanwendungen, welche durch B&R eigene Angaben und Hinweise beispielsweise im Zuge von Vertriebs-, Support oder Applikationstätigkeiten verursacht werden. Es liegt in der alleinigen Verantwortung des Anwenders, die von B&R übermittelten Angaben und Hinweise auf ihre sicherheitstechnisch korrekte Anwendbarkeit zu prüfen. Darüber hinaus liegt die gesamte Verantwortung für die sicherheitstechnisch ordnungsgemäße Ausführung der Sicherheitsfunktion ausschließlich beim Anwender.

9.5 X20 Systemeigenschaften

Aufgrund der nahtlosen Integration aller X20 Safety Produkte in das B&R Basis-System sind die Systemeigenschaften und Anwenderhinweise aus dem X20 System Anwenderhandbuch auch für die X20 Safety Produkte gültig.

Warnung!

Mögliches Versagen der Sicherheitsfunktion

Fehlfunktion des Moduls wegen unspezifizierter Betriebsbedingung

Die in den mitgeltenden Dokumenten angeführten Hinweise zur Installation und zum Betrieb der Module sind zu berücksichtigen.

In diesem Sinne sind für die X20 Safety Produkte die Inhalte und Anwenderhinweise in den folgenden, mitgeltenden Dokumentationen zu beachten:

- X20 System Anwenderhandbuch
- Installations- / EMV-Guide

9.6 Installationshinweise X20-Module

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 unbeschichteter Module in kondensierender Luftfeuchtigkeit und bei Temperaturen unter 0°C NICHT erlaubt ist.

Der Betrieb beschichteter (coated) Module ist in kondensierender Luftfeuchtigkeit erlaubt.

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. Das gilt auch für alle digitalen Signalquellen, welche an die Module angeschlossen werden.

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

Die Versorgung von X20 Potenzialgruppen muss generell mit einer Sicherung mit maximal 10 A abgesichert werden.

Weitergehende Informationen dazu können Kapitel "Mechanische und elektrische Konfiguration" des X20 bzw. X67 System Anwenderhandbuchs entnommen werden.

9.7 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!

Anwendungen in denen der sichere Zustand das aktive Einschalten eines Aktors bewirken muss, können mit diesem Modul nicht umgesetzt werden. In diesen Fällen müssen andere Maßnahmen diese sicherheitstechnische Anforderung erfüllen (z. B. mechanische Bremsen bei hängender Last, welche bei Spannungsausfall einfallen).

9.8 Gebrauchsdauer

Alle Safety Module sind wartungsfrei ausgeführt. An den Safety Modulen dürfen keine Reparaturen vorgenommen werden.

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.

10 Releaseinformation

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

Handbuchversion	gültig für		
V1.141			
V1.140			
V1.131	Version	ab	bis
V1.130	Produktset	Release 1.2	Release 1.10
V1.123	SafeDESIGNER	2.70	4.9
V1.122	Firmware	270	399
V1.121	Upgrades	1.2.0.0	1.10.999.999
V1.120			
V1.111			
V1.110			
V1.103			
V1.102			
V1.101			
V1.100			
V1.92			
V1.91			
V1.90			
V1.80			
V1.71			
V1.70			
V1.64			
V1.63.2			
V1.63.1			
V1.63			
V1.62			
V1.61			
V1.60			
V1.52.1			
V1.52			
V1.51			
V1.50.1			
V1.50			
V1.42			
V1.41			
V1.40			
V1.20			
V1.10			
V1.02			
V1.01	Version	ab	bis
V1.00	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 36: Releaseinformation

11 Versionshistorie

Version	Datum	Kommentar
1.141	April 2019	<ul style="list-style-type: none"> • Kapitel 3 "Technische Daten": Normen aktualisiert • Kapitel 9.3 "Security Konzept" aktualisiert • Kapitel 9.6 "Installationshinweise X20-Module" aktualisiert
1.140	Februar 2019	<ul style="list-style-type: none"> • Kapitel 3 "Technische Daten": <ul style="list-style-type: none"> – Max. Anzahl openSAFETY Nodes aktualisiert – Aufstellungshöhe auf 2000 m beschränkt – Coated Modul: Temperaturbereich erweitert • Kapitel 5.3 "Parameter im SafeDESIGNER - ab Release 1.10": Parameter "Process Data Transmission Rate" aufgenommen • Kapitel 8.2 "Datenlaufzeit am Bus": Berechnung der maximalen Datenlaufzeit aktualisiert • Kapitel 9 "Bestimmungsgemäße Verwendung": Gefahrenhinweis aufgenommen • Kapitel "Security-Hinweise" aufgenommen • Kapitel 9.5 "X20 Systemeigenschaften": Warnhinweis aufgenommen • Normen aktualisiert • Redaktionelle Änderungen
1.120	November 2017	<ul style="list-style-type: none"> • Kapitel 3 "Technische Daten": <ul style="list-style-type: none"> – Normen und sicherheitstechnische Kennwerte aktualisiert – Zeitliche Genauigkeit aufgenommen – max. Anzahl openSAFETY Nodes aktualisiert – max. Anzahl Variablen im Variablen-Status aufgenommen • Kapitel 5.1 "Parameter in der I/O Konfiguration": Gruppe "POWERLINK parameters" aktualisiert und Information aufgenommen • Kapitel 5.3 "Parameter im SafeDESIGNER - ab Release 1.10": Gruppe "Safety Response Time Defaults": Parameter "Default Safe Data Duration" aktualisiert • Kapitel 5.4 "Kanalliste der SafeLOGIC": Neue Objekte ab Hardware-Upgrade 1.10.4.0 aufgenommen • Kapitel 6.5 "SafeKEY bzw. Safety Section der CompactFlash": Beschreibung erweitert • Kapitel 7.3 "SafeLOGIC to SafeLOGIC communication": Systemvoraussetzungen aufgenommen • Kapitel 7.3.6 "Parameter für Verbindung - ab Release 1.10": Gruppe "Safety Response Time": Parameter "Safe Data Duration" aktualisiert • Kapitel 7.5 "Blackout-Modus": Voraussetzungen zum Betrieb aktualisiert • Kapitel 8.2 "Datenlaufzeit am Bus": Beschreibung erweitert und Information aufgenommen • Kapitel 9.6 "Installationshinweise X20-Module": Gefahrenhinweis erweitert • Redaktionelle Änderungen
1.111	Februar 2017	<ul style="list-style-type: none"> • Kapitel 5.1 "Parameter in der I/O Konfiguration": Parameter "Interface Slot Enable" und "Standalone mode" aufgenommen • Kapitel 5.3 "Parameter im SafeDESIGNER - ab Release 1.10": Parameter "Activate Setup Mode on empty SafeKEY", "Auto acknowledge firmware mismatch" und "Auto acknowledge SafeKEY exchange" aufgenommen • Kapitel 5.4 "Kanalliste der SafeLOGIC": Kanal "SafeFirmwareVersion" aufgenommen • Kapitel 7.2 "Automatische Quittierung": aufgenommen
1.110	Januar 2017	<ul style="list-style-type: none"> • Kapitel 1.1 "Funktion": um Blackout-Modus erweitert • Kapitel 3 "Technische Daten": Normen und sicherheitstechnische Kennwerte aktualisiert, Information aufgenommen • Kapitel 4.1.3 "Auswahlschalter und Bestätigungstaster": neue Schalterpositionen ergänzt • Kapitel 5.3 "Parameter im SafeDESIGNER - ab Release 1.10": Gruppe Basic: Information aufgenommen • Kapitel 6.5.2 "Bestätigen eines SafeKEY Tauschs": Information aufgenommen • Kapitel 7.1 "Bedienung über AsSafety Bibliothek": Inhalt entfernt, dafür Verweis auf Automation Help • Kapitel 7.5 "Blackout-Modus": neu aufgenommen • Kapitel 7.6 "Setup-Modus": neu aufgenommen • Kapitel 8.2 "Datenlaufzeit am Bus": Information zur Datenlaufzeit aufgenommen
1.102	Juni 2016	<p>Dokumentation umbenannt von X20SL810x auf X20SL81xx Modul X20SL8110 aufgenommen</p> <ul style="list-style-type: none"> • Kapitel 3 "Technische Daten": <ul style="list-style-type: none"> – Normen aktualisiert – Technische Daten aktualisiert

Tabelle 37: Versionshistorie

Version	Datum	Kommentar
1.101	März 2016	<ul style="list-style-type: none"> • Kapitel 8 "Sichere Reaktionszeit": Information aufgenommen
1.100	Januar 2016	<p>Zusammenführung coated / uncoated Dokumentation umbenannt von X20SL8100 auf X20SL810x Modul X20SL8101 aufgenommen</p> <ul style="list-style-type: none"> • Kapitel 1 "Allgemeines": neu aufgenommen • Kapitel 3 "Technische Daten": <ul style="list-style-type: none"> – Normen aktualisiert – Temperaturbereich erweitert – Technische Daten aktualisiert • Kapitel 4.3.2 "LED "STATUS"": überarbeitet • Kapitel 4.3.4 "RJ45 Ports": überarbeitet • Kapitel 5.2 "Parameter im SafeDESIGNER - bis Release 1.9": Parameter "KeepRemanent" aufgenommen • Kapitel 5.3 "Parameter im SafeDESIGNER - ab Release 1.10": neu aufgenommen • Kapitel 5.4 "Kanalliste der SafeLOGIC": Zusätzliche Registerbeschreibung aufgenommen • Kapitel "Überprüfen der verwendeten Library Version" neu aufgenommen • Kapitel 7.2 "Automatische Quittierung": neu aufgenommen • Kapitel 7.3.6 "Parameter für Verbindung - ab Release 1.10": neu aufgenommen • Kapitel 8.1 "Signalbearbeitung im sicheren B&R Eingangsmodul": Beschreibung aktualisiert • Kapitel 8.2 "Datenlaufzeit am Bus": Beschreibung um "ab Release 1.10" erweitert • Kapitel 8.3 "Signalbearbeitung im sicheren B&R Ausgangsmodul": Beschreibung aktualisiert • Kapitel 8.4 "Minimale Signallängen": Beschreibung aktualisiert • Kapitel 9.4 "Haftungsausschluss Sicherheitstechnik": überarbeitet • Kapitel 10 "Releaseinformation": aktualisiert
1.71	Juni 2014	<ul style="list-style-type: none"> • Kapitel 3 "Technische Daten": <ul style="list-style-type: none"> – "Sicherheitstechnische Kennwerte" aufgenommen, dafür Kapitel "Sicherheitstechnische Kennwerte" gelöscht – "Funktionalität": Folgende Punkte neu aufgenommen: <ul style="list-style-type: none"> - "max. Anzahl der openSAFETY Nodes" - "max. Anzahl der POWERLINK Controlled Nodes" - "Datenaustausch zwischen CPU und SL" - "Datenaustausch zwischen SL und SL" – "Grenzwerte für SafeDESIGNER Applikation" neu aufgenommen • Kapitel 5.2 "Parameter im SafeDESIGNER - bis Release 1.9": Gruppe "Safety_Response_Time_Defaults": Parameter "Default_Node_Guarding_Lifetime" neu aufgenommen • Kapitel 7.3.5 "Parameter für Verbindung - bis Release 1.9": Gruppe "Safety_Response_Time": Parameter "Node_Guarding_Lifetime" neu aufgenommen • Kapitel 8.2 "Datenlaufzeit am Bus": Beschreibung erweitert • Kapitel 9.6 "Installationshinweise X20-Module": Abbildung "Absicherung verschiedener Potenzialgruppen" entfernt, dafür Beschreibung aktualisiert • Kapitel 10 "Releaseinformation": aktualisiert
1.70	Oktober 2013	Erste Ausgabe als produktspezifisches Handbuch

Tabelle 37: Versionshistorie

12 EG-Konformitätserklärung

Das vorliegende Dokument wurde in deutscher Sprache erstellt. Die deutsche Ausgabe stellt daher die Originalbetriebsanleitung im Sinne der Maschinenrichtlinie 2006/42/EG dar. Dokumente in anderen Sprachen sind als Übersetzung der Originalbetriebsanleitung zu interpretieren.

Hersteller des Produkts:

B&R Industrial Automation GmbH

B&R Straße 1

5142 Eggelsberg

Österreich

Telefon: +43 7748 6586-0

Fax: +43 7748 6586-26

office@br-automation.com

Gerichtsstand gemäß Art. 17 EuGVÜ ist A-4910

Ried im Innkreis Firmenbuchgericht: Ried im Innkreis

Firmenbuchnummer: FN 111651 v.

Erfüllungsort gemäß Art. 5 EuGVÜ ist A-5142 Eggelsberg

UST-ID: ATU62367156

Die EG-Konformitätserklärungen der B&R Produkte sind auf der B&R Homepage www.br-automation.com als Download verfügbar.