X20(c)SL81xx

Information:

B&R makes every effort to keep data sheets as current as possible. From a safety point of view, however, the current version of the data sheet must always be used.

The certified, currently valid data sheet can be downloaded from the B&R website www.br-automation.com.

Organization of notices

Safety notices

Contain **only** information that warns of dangerous functions or situations.

Signal word	Description
Danger!	Failure to observe these safety guidelines and notices will result in death, severe injury or substantial damage to property.
Warning!	Failure to observe these safety guidelines and notices can result in death, severe injury or substantial damage to property.
Caution!	Failure to observe these safety guidelines and notices can result in minor injury or damage to property.
Notice!	Failure to observe these safety guidelines and notices can result in damage to property.

Table 1: Organization of safety notices

General notices

Contain **useful** information for users and instructions for avoiding malfunctions.

Signal word	Description
Information:	Useful information, application tips and instructions for avoiding malfunctions.

Table 2: Organization of general notices

1 General information

The modules are equipped with SafeLOGIC functionality that allows them to safely execute applications designed in SafeDESIGNER. The modules can be used in safety applications up to PL e or SIL 3.

The SafeLOGIC controller coordinates the safety-related communication of all modules involved in the application. In this context, the SafeLOGIC controller also monitors the configuration of these modules and autonomously carries out parameter downloads to the modules if necessary. This guarantees a consistent and correct module configuration in the network from a safety point of view in all scenarios involving module replacement and service. For SafeLOGIC products, these services are executed by the SafeLOGIC controller. For SafeLOGIC-X products, these services are executed on the standard CPU in interaction with Automation Runtime. The safety-related characteristics up to PL e or SIL 3 for applications are provided in both variants, however.
In addition, SafeLOGIC-X products have the same I/O properties as the associated SafeIO products.

- openSAFETY manager for up to 10 / 20 / 100 / 280 SafeNODES
- Flexibly programmable using Automation Studio / SafeDESIGNER
- Innovative management of safe machine options (SafeOPTION)
- Parameter and configuration management

1.1 Function

SafeLOGIC function

The module is equipped with SafeLOGIC functionality that allows it to safely execute applications designed in SafeDESIGNER. The module can be used in safety-related applications up to PL e or SIL 3.

In addition, the module coordinates the safety-related communication of all modules involved in the application. In this context, the module also monitors the configuration of these modules and autonomously carries out parameter downloads to the modules if necessary. This guarantees a consistent and correct module configuration in the network from a safety point of view in all scenarios involving module replacement and service. For SafeLOGIC products, these services are executed by the SafeLOGIC controller. For SafeLOGIC-X products, these services are executed on the standard CPU in interaction with Automation Runtime. The safety-related characteristics up to PL e or SIL 3 for applications are provided with both variants, however.

Blackout mode

In blackout mode, module functionality persists even if the network fails. Without this function, the safe state would always be initiated on the affected module if the network fails. In addition, blackout mode can allow partial operation to resume or coordinated shutdown scenarios to be initiated. This mode also makes it possible to boot a module without a network based on a configuration saved on the module beforehand.

openSAFETY

This module uses the protective mechanisms of openSAFETY when transferring data to the various bus systems. Because the data is encapsulated in the openSAFETY container in a fail-safe manner, the components on the network that are involved in the transfer do not require any additional safety-related features. At this point, only the safety-related characteristic values specified for openSAFETY in the technical data are to be consulted. The data in the openSAFETY container undergoes safety-related processing only when received by the remote station; for this reason, only this component is involved from a safety point of view. Read access to the data in the openSAFETY container for applications without safety-related characteristics is permitted at any point in the network without affecting the safety-related characteristics of openSAFETY.

open SAFETY

1.2 Coated modules

Coated modules are X20 modules with a protective coating for the electronics component. This coating protects X20c modules from condensation.
The modules' electronics are fully compatible with the corresponding X20 modules.

Information:

For simplification purposes, only images and module IDs of uncoated modules are used in this data sheet.

The coating has been certified according to the following standards:

- Condensation: BMW GS 95011-4, 2x 1 cycle
- Corrosive gas: EN 60068-2-60, Method 4, exposure 21 days

Contrary to the specifications for X20 system modules without safety certification and despite the tests performed, X20 safety modules are **NOT suited for applications with corrosive gases (EN 60068-2-60)!**

2 Order data

X20SL8100

X20SL8101

X20SL8110

Model number	Short description
	CPUs
X20SL8100	X20 SafeLOGIC, safety controller, openSAFETY gateway, removable application memory: SafeKEY, 1 POWERLINK interface, controlled node, integrated 2-port hub, including power supply module, 1x terminal block X20TB52 and X20 end cover plate X20AC0SR1 (right) included, order SafeKEY and SafeLOGIC range of functions using the X20MK configurator!
X20cSL8100	X20 SafeLOGIC, coated, safety controller, openSAFETY gateway, removable application memory: SafeKEY, 1 POWERLINK interface, controlled node, integrated 2-port hub, including power supply module, 1x terminal block X20TB52 and X20 end cover plate X20AC0SR1 (right) included, order SafeKEY and SafeLOGIC range of functions using the X20MK configurator!
X20SL8101	X20 SafeLOGIC with X20 bus controller, safety controller, openSAFETY gateway, removable application memory: SafeKEY, 1 POWERLINK interface, controlled node, integrated 2-port hub, including power supply module for internal I/O power supply and X2X Link power supply, 1x terminal block X20TB52 and X20 end cover plate X20AC0SR1 (right) included, order SafeKEY and SafeLOGIC range of functions using the X20MK configurator!
X20cSL8101	X20 SafeLOGIC with X20 bus controller, coated, safety controller, openSAFETY gateway, removable application memory: SafeKEY, 1 POWERLINK interface, controlled node, integrated 2-port hub, including power supply module for internal I/O power supply and X2X Link power supply, 1x terminal block X20TB52 and X20 end cover plate X20AC0SR1 (right) included, order SafeKEY and SafeLOGIC range of functions using the X20MK configurator!
X20SL8110	X20 SafeLOGIC, safety controller, openSAFETY gateway, removable application memory: SafeKEY, 1 POWERLINK interface, 1 slot for X20 interface module, controlled node, integrated 2-port hub, including power supply module, 1x terminal block X20TB52 and X20 end cover plate X20AC0SR1 (right) included, order SafeKEY and SafeLOGIC range of functions using the X20MK configurator!
	Required accessories
	Accessories
X20MKXXXX.XXX.XXX	"Safety Technology Guarding" defines the range of functions available for applications using X20SL81xx- or X20cSL81xx-series SafeLOGIC controllers. Licenses are stored on a SafeKEY dongle. The functions required for the application must be put together in the X20MK configurator by selecting a SafeKEY with a sufficient amount of memory, a coated/non-coated variant and the necessary technology functions. Each solution is delivered exclusively as a set consisting of the SafeKEY and the activated licenses for the selected technology functions.

Table 3: X20SL8100, X20cSL8100, X20SL8101, X20cSL8101, X20SL8110 - Order data

3 Technical data

Model number	X20SL8100	X20cSL8100	X20SL8101	X20cSL8101	X20SL8110
Short description					
Interfaces	POWERLINK				
System module	CPU				
General information					
Cooling	Fanless				
B&R ID code	0xDD61	0xE287	0xE649	0xE926	0xE64A
System requirements					
Automation Studio	4.0.16 or later		4.1.6 or later		V4.2.5 or later
Automation Runtime	V3.08 or later (for AsSafety library F4.06 or later)		F4.09 or later, F4.10 or later, A4.23 or later		B4.25 or later
SafeDESIGNER	3.1.0 or later		4.1.0 or later		V4.2 or later
Safety Release	1.7 or later				1.10 or later
Status indicators	CPU function, POWERLINK, SafeKEY				
Diagnostics					
CPU function	Yes, using status LED				
POWERLINK	Yes, using status LED				
SafeKEY	Yes, using status LED				
Power consumption	4.3 W		5.3 W		3.9 W [1]
Blackout mode					
Scope	-		Network segment		-
Function	-		Programmable		-
Standalone mode	-		Yes		-
Power consumption for X2X Link power supply	-		1.42 W [2]		-
Power consumption					
Internal I/O	-		0.6 W [2]		-
Electrical isolation					
Fieldbus - X2X Link	-		Yes		-
Fieldbus - I/O	-		Yes		-
Certifications					
CE	Yes				
EAC	Yes				
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 (see X20 user's manual) 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 preparation
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				
Safety characteristics					
EN ISO 13849-1:2015					
Category	Cat. 4				
PL	PL e				
DC	>94%				
MTTFD	2500 years				
Mission time	Max. 20 years				
IEC 61508:2010, IEC 61511:2004, EN 62061:2013					
SIL CL	SIL 3				
SFF	>90%				
PFH / PFH_d					
Module	$<1*10^{-10}$				
openSAFETY wired	Negligible				
openSAFETY wireless	$<1*10^{-14}$ * Number of openSAFETY packets per hour				
PFD	$<2*10^{-5}$				
Proof test interval (PT)	20 years				

Table 4: X20SL8100, X20cSL8100, X20SL8101, X20cSL8101, X20SL8110 - Technical data

Model number	X20SL8100	X20cSL8100	X20SL8101	X20cSL8101	X20SL8110
Functionality					
Communication with each other	Yes				
Support for machine options					
BOOL	512				
INT	64				
UINT	64				
DINT	64				
UDINT	64				
SafeMOTION support	Yes, depends on the number of available operating licenses on the SafeKEY				
Timing precision	Time * 0.05 + Cycle time of the safety application				
Shortest task class cycle time	1 ms				
Max. number of openSAFETY nodes	100, depends on the number of available operating licenses on the SafeKEY		280, depends on the number of available operating licenses on the SafeKEY and available resources		
Max. number of POWERLINK controlled nodes	50		100		
Data exchange between CPU and SL					
Max. total data width for each direction	128 bytes				
Max. number of data points for each direction					
BOOL	352 (96 + 256 extended)				
INT	30				
UINT	30				
DINT	15				
UDINT	15				
Data exchange between SL and SL					
Max. total number of data points for each direction [3]	16				
Max. number of data points for each direction					
BOOL	128				
INT	16				
UINT	16				
DINT	16				
UDINT	16				
Limit values for SafeDESIGNER application					
Max. resources available for SafeDESIGNER info window entries [4]					
FB instances	4096				
Marker memory	131,072 bytes				
Stack memory	32,768 bytes				
Memory for safe input data	2048 bytes				
Memory for safe output data	2048 bytes				
Memory for standard input data	1024 bytes				
Memory for standard output data	1024 bytes				
Marker count	8192				
Additional SafeDESIGNER limit values					
Max. number of function block types	512				
Max. number of force variables	64				
Max. number of variable with variable status	1023				
Input SL / BC / X2X Link power supply					
Input voltage	24 VDC -15% / +20%				
Input current	Max. 0.25 A		Max. 0.9 A		Max. 0.25 A
Fuse	-		Integrated, cannot be replaced		-
Reverse polarity protection	Yes				
Output SL / BC / X2X Link power supply					
Nominal output power	-		7 W		-
Parallel connection	-		Yes [5]		-
Redundant operation	-		Yes		-
Overload characteristics	-		Short-circuit proof, temporary overload		-
Input I/O power supply					
Input voltage	-		24 VDC -15% / +20%		-
Fuse	-		Required line fuse: Max. 10 A, slow-blow		-
Reverse polarity protection	-		Yes		-
Output I/O power supply					
Nominal output voltage	-		24 VDC		-
Behavior on short circuit	-		Required line fuse		-
Permissible contact load	-		10 A		-
Interfaces					
Fieldbus	POWERLINK controlled node				
Type	Type 3 [6]				
Variant	2x shielded RJ45 port (hub)				

Table 4: X20SL8100, X20cSL8100, X20SL8101, X20cSL8101, X20SL8110 - Technical data

Model number	X20SL8100	X20cSL8100	X20SL8101	X20cSL8101	X20SL8110
Line length	Max. 100 m between 2 nodes (segment length)				
Transfer rate	100 Mbit/s				
Transfer					
Physical layer	100BASE-TX				
Half-duplex	Yes				
Full-duplex	No				
Autonegotiation	Yes				
Auto-MDI / MDIX	Yes				
Min. cycle time 7)					
Fieldbus	200 µs				
X2X Link	-		200 µs		-
Synchronization between bus systems possible	-		Yes		-
Operating conditions					
Mounting orientation					
Horizontal	Yes				
Vertical	Yes				
Installation elevation above sea level	0 to 2000 m, no limitation				
Degree of protection per EN 60529	IP20				
Ambient conditions					
Temperature					
Operation					
Horizontal mounting orientation	0 to 60°C	-40 to 60°C 8)	0 to 60°C	-40 to 60°C 9)	0 to 60°C
Vertical mounting orientation	0 to 45°C	-40 to 45°C 10)	0 to 45°C	-40 to 45°C 11)	0 to 45°C
Derating	-		See section "Derating".		-
Storage	-40 to 85°C				
Transport	-40 to 85°C				
Relative humidity					
Operation	5 to 95%, non-condensing	Up to 100%, condensing	5 to 95%, non-condensing	Up to 100%, condensing	5 to 95%, non-condensing
Storage	5 to 95%, non-condensing				
Transport	5 to 95%, non-condensing				
Mechanical properties					
Note	Order SafeKEY and SafeLOGIC range of functions using the X20MK configurator. X20 end cover plate (right) included in delivery. 12-pin X20 terminal block, safety-keyed, included in delivery. SafeKEY cover included in delivery.				
Dimensions					
Width	62.5$^{+0.2}$ mm				
Height	99 mm				
Depth	75 mm				
Weight	190 g				

Table 4: X20SL8100, X20cSL8100, X20SL8101, X20cSL8101, X20SL8110 - Technical data

1) Power consumption without interface module
2) The specified values are maximum values. For examples of the exact calculation, see section "Mechanical and electrical configuration" of the X20 system user's manual.
3) Keep in mind that 8 BOOL count as 1 data point.
4) For a parameter description, see section "Message window" of the SafeDESIGNER documentation.
5) In parallel operation, it is only permitted to expect 75% of the nominal power. It is important to make sure that all power supplies operated in parallel are switched on and off at the same time.
6) See Automation Help under "Communication / POWERLINK / General information / Hardware - CN" for more information. It is important to note, however, that the SafeLOGIC controller does not support "early writing of output data". The use of "poll-response chaining" is not recommended for controlled nodes in the same POWERLINK line.
7) The minimum cycle time specifies the time up to which the bus cycle can be reduced without communication errors occurring.
8) Up to hardware upgrade <1.10.5.0 and hardware revision <F0: -25 to 60°C
9) Up to hardware upgrade <1.10.5.0 and hardware revision <E0: -25 to 60°C
10) Up to hardware upgrade <1.10.5.0 and hardware revision <F0: -25 to 45°C
11) Up to hardware upgrade <1.10.5.0 and hardware revision <E0: -25 to 45°C

Danger!

Operation outside the technical data is not permitted and can result in dangerous states.

Information:

For detailed information about installation, see chapter "Installation notes for X20 modules" on page 78.

X20SL8101: Derating for SafeLOGIC / Bus controller / X2X Link power supply

The nominal output power for the X2X Link power supply is 7 W.
The nominal output power depends on the operating temperature and the mounting orientation. The resulting nominal output power can be looked up in the following table.

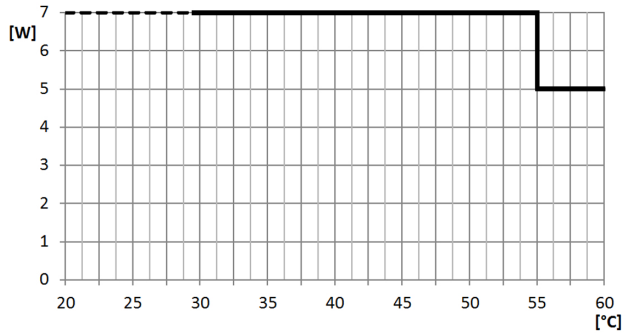
Horizontal (0 to 60°C, coated: -40 to 60°C)	Vertical (0 to 45°C, coated: -40 to 45°C)
	No derating

Table 5: Derating for SafeLOGIC / Bus controller / X2X Link power supply

Information:

Regardless of the values specified in the derating curve, the module cannot be operated above the values specified in the technical data.

4 Operating and connection elements

LEDs and buttons/switches are provided for operating the SafeLOGIC. These elements can be used to perform the following actions:

- Module exchange, including a test of the complete module configuration (section "Module replacement")
- Firmware replacement (section "Acknowledging a firmware modification")
- SafeKEY replacement, including possible transfer of module configuration from the old SafeKEY (section "Changing the application on the SafeLOGIC controller by replacing the SafeKEY (X20SL8xxx series only)")
- and SafeLOGIC controller replacement (section "Replacing a SafeLOGIC controller")

The AsSafety library (chapter "Operation via the AsSafety library") can also be used to operate the SafeLOGIC controller using the HMI application.

SafeLOGIC has the following operating and connection elements:

X20SL810x

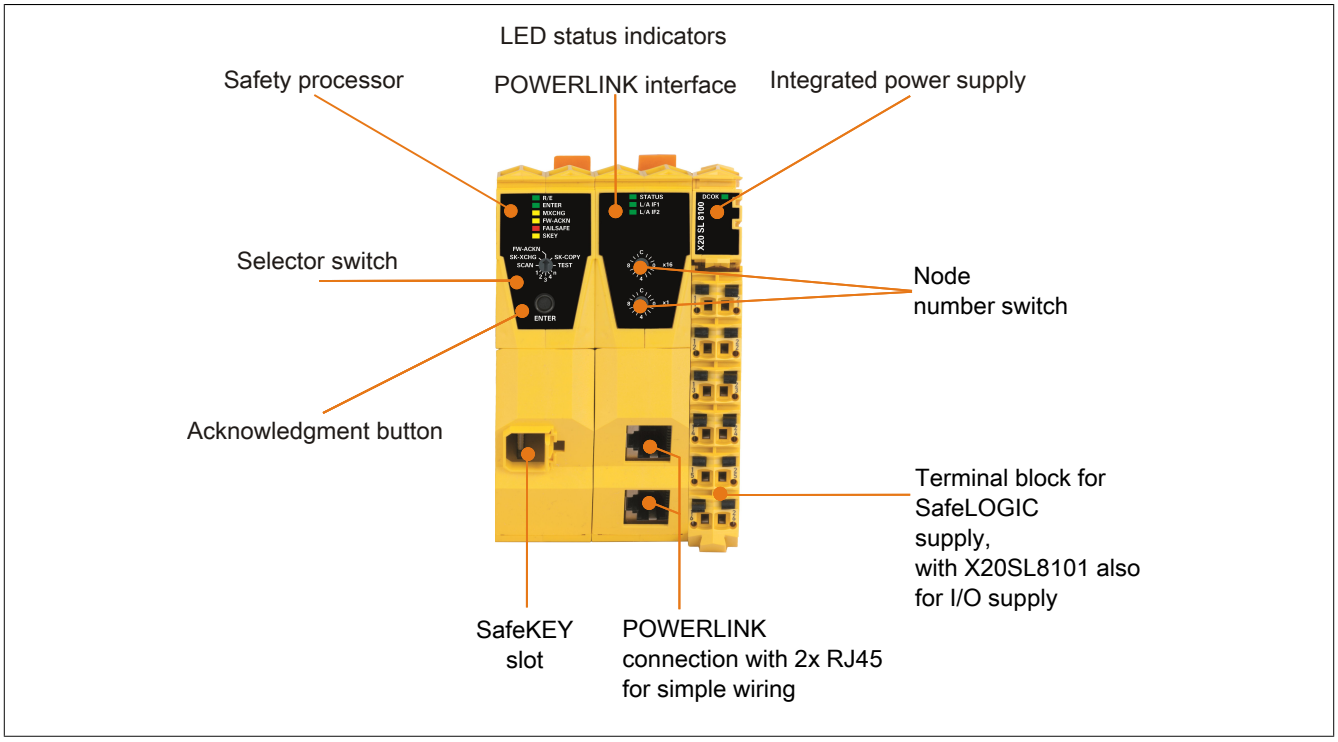


Figure 1: X20SL810x - Operating elements

X20SL8110

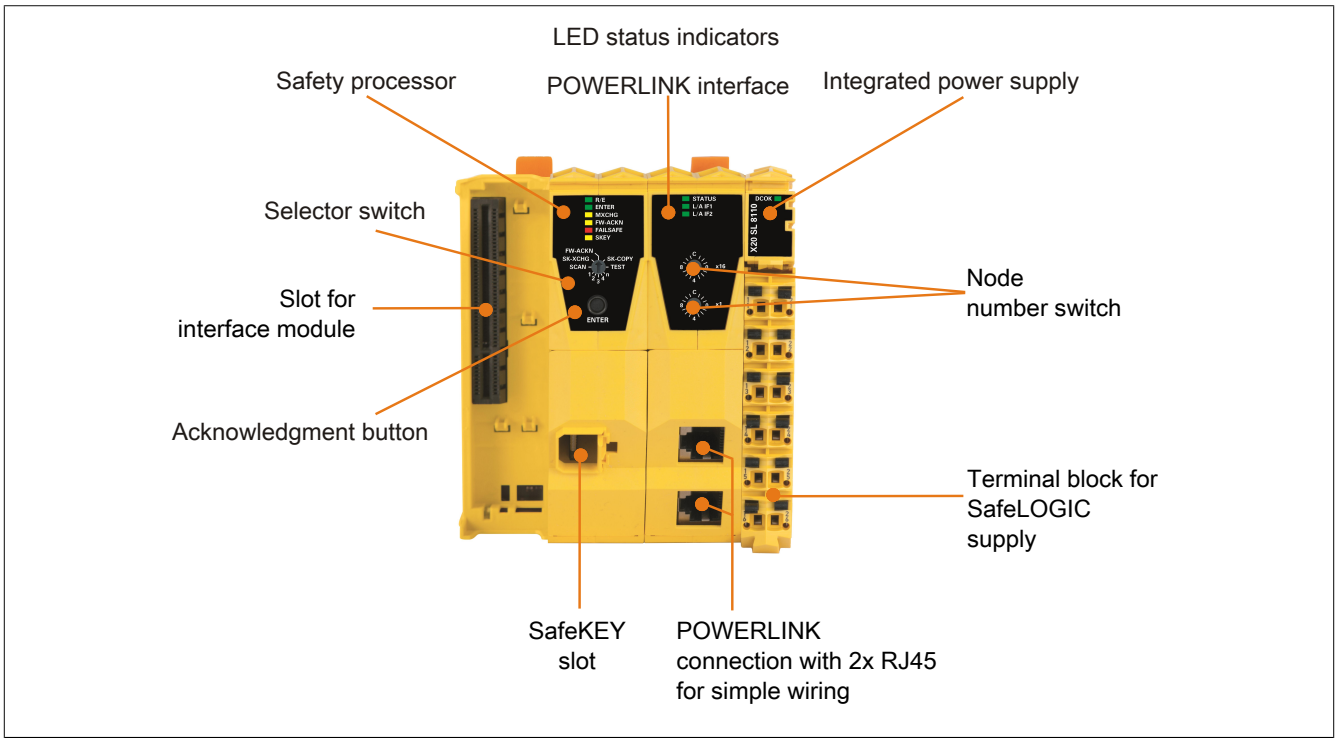


Figure 2: X20SL8110 - Operating elements

Slot for interface modules

The X20SL8110 SafeLOGIC controller is equipped with a slot for interface modules.

Various bus and network systems can easily be integrated into the X20 system by selecting the corresponding interface module.

The following interface modules can be used in the X20SL8110 SafeLOGIC controller:

Module	Description
X20IF10E3-1	X20 interface module for DTM configuration, 1 PROFINET RT device (slave) interface, electrically isolated

4.1 Safety processor

4.1.1 LED status indicators of the safety processor

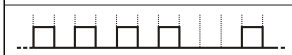
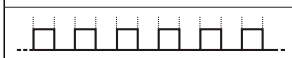
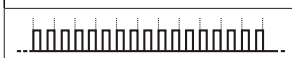
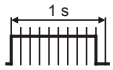
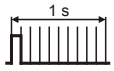
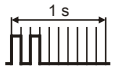
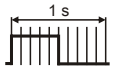
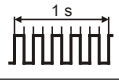
LED	Color	Status	Description
R/E		Off	Boot phase
	Green	On	Application exists and is being executed
		Blinking	Application exists but is not being executed (in the download dialog box for the SafeDESIGNER, "Automatic start" was not selected OR boot phase, i.e. not all necessary safe modules on the network were configured correctly.) In addition, boot states 0x1840 to 0x3440 under index:subindex 0x2410:0x01 must be checked in section "SafeLOGIC - Channel list".
	Orange	On	SafeDESIGNER in "Debug" mode
		Blinks at 0.5 Hz	SafeDESIGNER in "Debug" mode, application in "Stop"
		Blinks at 1 Hz	No application on SafeKEY
ENTER	Green	On	Missing authorization, see "Authorization (X20SL8xxx series only)".
		Blinks 1x for 0.8 s	Confirmation of correct entry
		Blinks (1 Hz) for 5 s	Faulty operation
MXCHG	Orange	Off	Module configuration OK
			Replacement of 1 module detected
			Replacement of 2 modules detected
			Replacement of 3 modules detected
			Replacement of 4 modules detected
			Replacement of more than 4 modules detected
			Missing module detected
FW-ACKN	Orange	Off	Firmware configuration OK
		Blinking	Firmware update carried out
		On	SafeKEY was replaced
ENTER MXCHG FW-ACKN	Green Orange Orange	Running sequence	Performing module scan or boot phase (beginning with Release 1.5 - Note: Check STATUS LED, see section "LED status indicators for the POWERLINK interface"!)
FAILSAFE	Red		The FAILSAFE LED indicates the boot behavior or state "FailSafe" for the entire module after booting.
		Off	Safety firmware OPERATIONAL state
			Boot phase
			Safety firmware PRE_OPERATIONAL state or "SafeOSstate!=RUN"
			Safe communication channel not OK, openSAFETY connection valid problem or "SafeOSstate!=RUN" If the SafeLOGIC controller remains in this state for a longer time, parameter "Default Safe Data Duration" of the "Group: Safety Response Time Defaults" must be checked.
			Boot phase, faulty firmware, setup mode active (hardware upgrade 1.10.2.x and later) For details about setup mode, see section "Setup mode".
			Test/Pilot firmware or safety application created with test/pilot version of SafeDESIGNER

Table 6: Safety processor status indicators

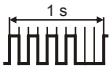
			SafeDESIGNER in "Debug" mode
		On	Safety state active for the entire module (= state "FailSafe")
SKEY	Orange	Off	No access to the SafeKEY
		Blinking	Access to the SafeKEY

Table 6: Safety processor status indicators

Danger!

A constantly lit FAILSAFE LED indicates a possible safety-related system error.
It is your responsibility to ensure that all necessary repair measures are initiated after an error occurs since subsequent errors can result in dangerous situations!

4.1.2 LED test

The functionality of the LEDs can be tested using the following sequence:

- Move the selector switch to TEST.
- Press the ENTER confirmation button.
- All of the safety processor LEDs will turn on (left module of the SafeLOGIC controller) for the exact duration that the confirmation button is pressed.

4.1.3 Selector switch and confirmation button

If configuration confirmations are required for the user, they can be generated by pre-selecting the desired function via the selector switch and then pressing the ENTER confirmation button.

Figure 3: Selector switch and confirmation button

Switch position	Functionality	Description
FW-ACKN	Firmware acknowledgment	Acknowledges a firmware change on one or more modules[1)]
Unlabeled position between FW-ACKN and SK-COPY (=0xD)	Setup mode (hardware upgrade 1.10.2.x or later)	Enables/Disables setup mode For details about setup mode, see section "Setup mode".
SK-COPY	SafeKEY copy	Copy of the configuration data from the SafeKEY[2)]
TEST	Test	Performs an LED test
Unlabeled position between TEST and n	CLEAR DATA	Deletes the following "user data": • Remanent data • Configuration file from the standard application • Extended machine options • Table objects • Subsequently loadable parameter file - firmware version V322 or later
1,2,3,4,n	Replacing a module	Confirm the replacement of 1, 2, 3, 4 or more than 4 modules
SCAN	Scan	Triggers a module scan
SK-XCHG	SafeKEY exchange	Confirmation of SafeKEY exchange[1)]
Unlabeled position between FW-ACKN and SK-XCHG	Format SafeKEY	Formatting SafeKEY (Release 1.4 and later)[2)]

Table 7: Confirmation modes

1) Triggers a restart in firmware versions ≤ V322.
2) Triggers an automatic restart.

Confirmation (all functions except for "Format SafeKEY")

The confirmation button must be pressed for 0.5 to 5 s to receive confirmation. After 0.5 s, the LED ENTER (see chapter "LED status indicators of the safety processor") begins to light. After releasing the confirmation button, the ENTER LED remains illuminated for an extra 0.8 s. This sequence indicates a correct entry.

- If the confirmation button is released before 0.5 s, it has no effect.
- If the confirmation button is pressed for longer than 5 s, then the ENTER LED blinks for 5 s to display an error.

Another possible reason for an error is an improper placement of the selector switch. If the user wants to confirm a module replacement for one specific module, for example, then the selector switch must be at position "1" (see section "Replacing an individual module"). In this case, if a placement other than "1" is confirmed with the confirmation button, it is considered an error and the ENTER LED blinks for 5 s.

Confirmation of "Format SafeKEY"

The confirmation button must be pressed for 20 to 30 s to receive a confirmation for "Format SafeKEY". After 20 s, the ENTER LED is illuminated. After releasing the confirmation button, the ENTER LED remains illuminated for an extra 0.8 s. This sequence indicates a correct entry.

- If the confirmation button is released before 20 s, it has no effect.
- If the confirmation button is pressed for longer than 30 s, then the ENTER LED blinks for 5 s to display an error.

All data will be deleted (including password), which is why going online with SafeDESIGNER and assigning a new password is recommended.

4.2 Slot for application memory (SafeKEY)

In order to operate the SafeLOGIC controller, application memory (SafeKEY) is required to save the program, the parameters and the system configuration.

The SafeKEY is equipped with a mechanical locking mechanism to make it more difficult to inadvertently remove during operation.

Figure 4: SafeKEY unlocked

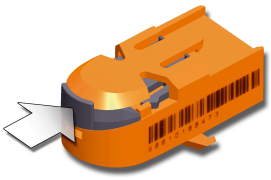


Figure 5: SafeKEY locked

Information:

Removing a SafeKEY during operation causes the SafeLOGIC controller to be restarted and all safety-related actuators to be cut off.

Removing a SafeKEY during operation can destroy the data on the SafeKEY.

Removing a SafeKEY during operation must therefore be avoided at all cost.

The "Backing up the SafeKEY" sequence is not affected by this general rule.

Information:

Note that modules operated on the local X2X bus of the X20SL8101 are only correctly configured if a valid safety project exists on the SafeKEY. Otherwise, "ModuleOk" in Automation Studio remains set to FALSE.

4.3 POWERLINK interface

4.3.1 LED status indicators for the POWERLINK interface

Figure	LED	Color	Status	Description
	STATUS[1)]	Green/Red		Status/Error LED, The LED states are described in section 4.3.2 "LED "STATUS"".
	L/A IFx	Green	On	A link to the peer station has been established.
			Blinking	A link to the peer station has been established. Indicates Ethernet activity is taking place on the bus.

Table 8: POWERLINK interface status indicators

1) The Status/Error LED is a green/red dual LED.

4.3.2 LED "STATUS"

LED "Status/Error" is a green and red dual LED. The color green (status) is superimposed on the color red (error).

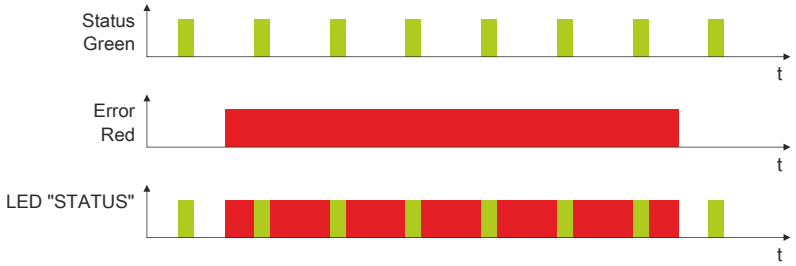
Red - Error	Description
On	The controlled node (CN) is in an error state (failed Ethernet frames, increased number of collisions on the network, etc.). If an error occurs in the following states, then the green LED blinks over the red LED: • PRE_OPERATIONAL_1 • PRE_OPERATIONAL_2 • READY_TO_OPERATE  Note: • Several red blinking signals are displayed immediately after the device is switched on. This is not an error, however. • The LED is lit red for CNs with set physical node number 0 to which no node number has yet been assigned by dynamic node allocation (DNA).

Table 9: Status/Error LED lit red: LED indicating error

Green - Status	Description
Off	No power supply or mode NOT_ACTIVE. The controlled node (CN) is either not supplied with power, or it is in state NOT_ACTIVE. The CN waits in this state for about 5 seconds after a restart. Communication is not possible with the CN. If no POWERLINK communication is detected during these 5 seconds, the CN enters state BASIC_ETHERNET (flickering). If POWERLINK communication is detected before this time expires, however, the CN immediately enters state PRE_OPERATIONAL_1.
Flickering green (approx. 10 Hz)	Mode BASIC_ETHERNET. The CN has not detected any POWERLINK communication. In this state, it is possible to communicate directly with the CN (e.g. with UDP, IP, etc.) If POWERLINK communication is detected while in this state, the CN enters state PRE_OPERATIONAL_1.
Single flash (approx. 1 Hz)	Mode PRE_OPERATIONAL_1. The CN waits until it receives an SoC frame and then switches to state PRE_OPERATIONAL_2.
Double flash (approx. 1 Hz)	Mode PRE_OPERATIONAL_2. The CN is normally configured by the manager in this state. A command then switches the CN to the READY_TO_OPERATE state.
Triple flash (approx. 1 Hz)	Mode READY_TO_OPERATE. The manager switches the CN via command to the OPERATIONAL state.
On	Mode OPERATIONAL. The PDO mapping is active and cyclic data is evaluated.
Blinking (approx. 2.5 Hz)	Mode STOPPED. Output data is not being output, and no input data is being provided. It is only possible to switch to or leave this state after the manager has given the appropriate command.

Table 10: Status/Error LED lit green: LED indicating operating state

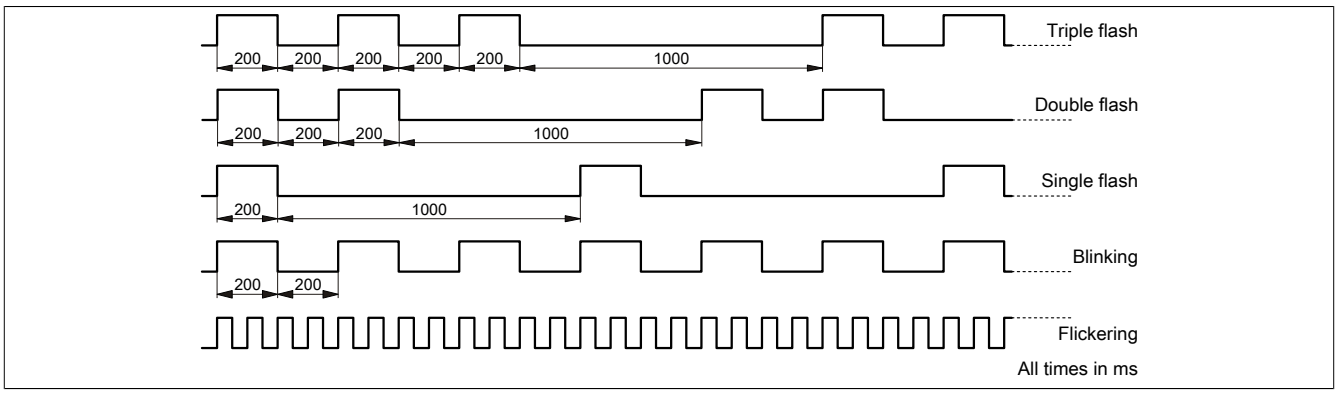


Figure 6: LED status indicators - Blink times

4.3.3 POWERLINK station number

Figure 7: POWERLINK station number switches

The station number of the POWERLINK station is set using the two number switches. Station numbers between 0x01 and 0xEF are permitted.

Switch position	Description
0x00	Reserved, switch position not permitted.
0x01 to 0xEF	Station number of the POWERLINK station, operation as controlled node (CN)
0xF0 to 0xFF	Reserved, switch position not permitted.

Table 11: POWERLINK station number

4.3.4 RJ45 ports

For information about wiring X20 modules with an Ethernet interface, see section "Mechanical and electrical configuration - Cabling guidelines for X20 modules with an Ethernet cable" of the X20 user's manual.

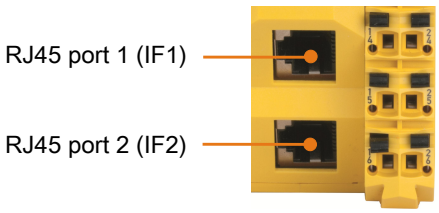


Figure 8: RJ45 ports

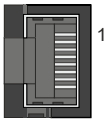
Interface	Pinout		
	Pin	Ethernet	
 1 Shielded RJ45 port	1	RXD	Receive data
	2	RXD\	Receive data\
	3	TXD	Transmit data
	4	Termination	
	5	Termination	
	6	TXD\	Transmit data\
	7	Termination	
	8	Termination	

Table 12: Pinout for RJ45 port

4.4 SG support

SG3 / SGC

The SafeLOGIC controller is not currently supported on SG3 and SGC target systems.

SG4

The SafeLOGIC controller comes with preinstalled firmware. In addition, the firmware version appropriate to the Safety Release will also be saved to the standard CPU when the Automation Studio project is downloaded.

If a different firmware version is being used, then the firmware saved on the standard CPU will automatically be loaded to the module.

When changing the safety-related firmware on the SafeLOGIC controller, the measures listed in section "Acknowledging a firmware modification" must be taken.

4.5 Integrated power supply

A power supply is integrated in the SafeLOGIC controller.

4.5.1 LED status indicators for the integrated power supply

X20SL81x0

Figure	LED	Color	Status	Description
	DCOK	Green	On	Voltage applied to module
			Off	Voltage not applied to module

Table 13: X20SL81x0 - LED status indicators for the integrated power supply

X20SL8101

Figure	LED	Color	Status	Description
	r	Green	Off	No power to module
			Single flash	RESET mode
			Blinking	PREOPERATIONAL mode
			On	RUN mode
	e	Red	Off	No power to module or everything OK
			Double flash	LED indicates one of the following states: • The SafeLOGIC controller / bus controller / X2X Link power supply for the power supply is overloaded • I/O power supply too low • Input voltage for the SafeLOGIC controller / bus controller / X2X Link power supply is too low
	e + r	Solid red / Single green flash		Invalid firmware
	l	Red	Off	The SafeLOGIC controller / bus controller / X2X Link power supply is in the valid range.
			On	The SafeLOGIC controller / bus controller / X2X Link power supply for the power supply is overloaded.

Table 14: X20SL8101 - LED status indicators for the integrated power supply

4.5.2 Pinout for the integrated power supply

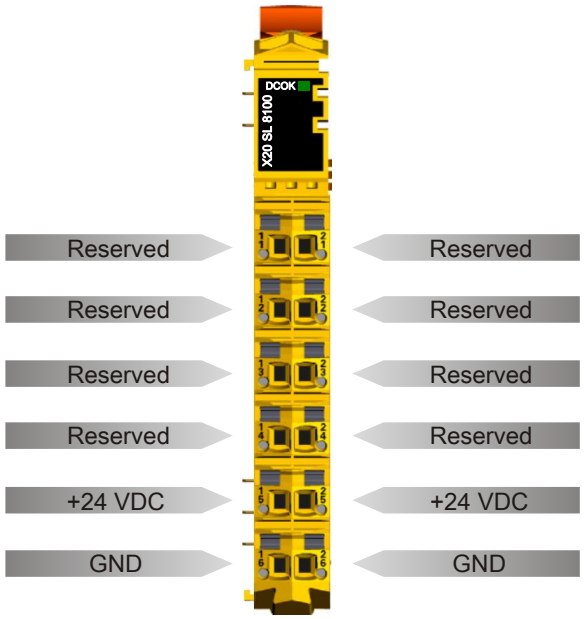


Figure 9: X20SL81x0 - Pinout of the integrated power supply

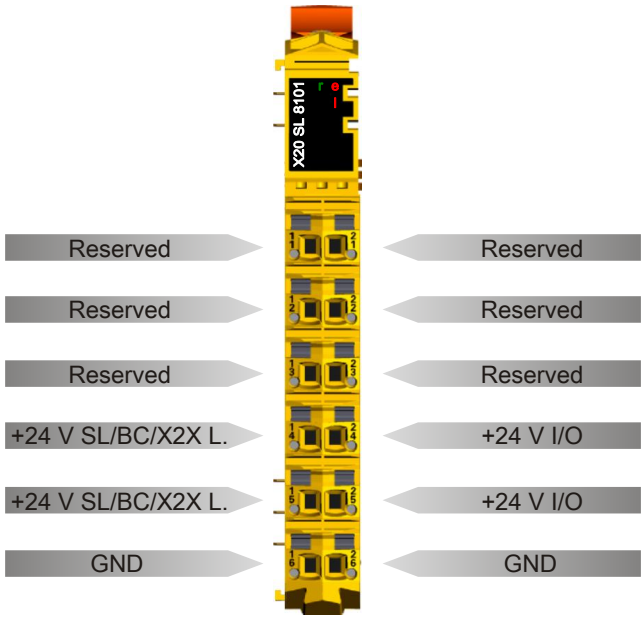


Figure 10: X20SL8101 - Pinout of the integrated power supply

4.5.3 Connection examples

X20SL81x0

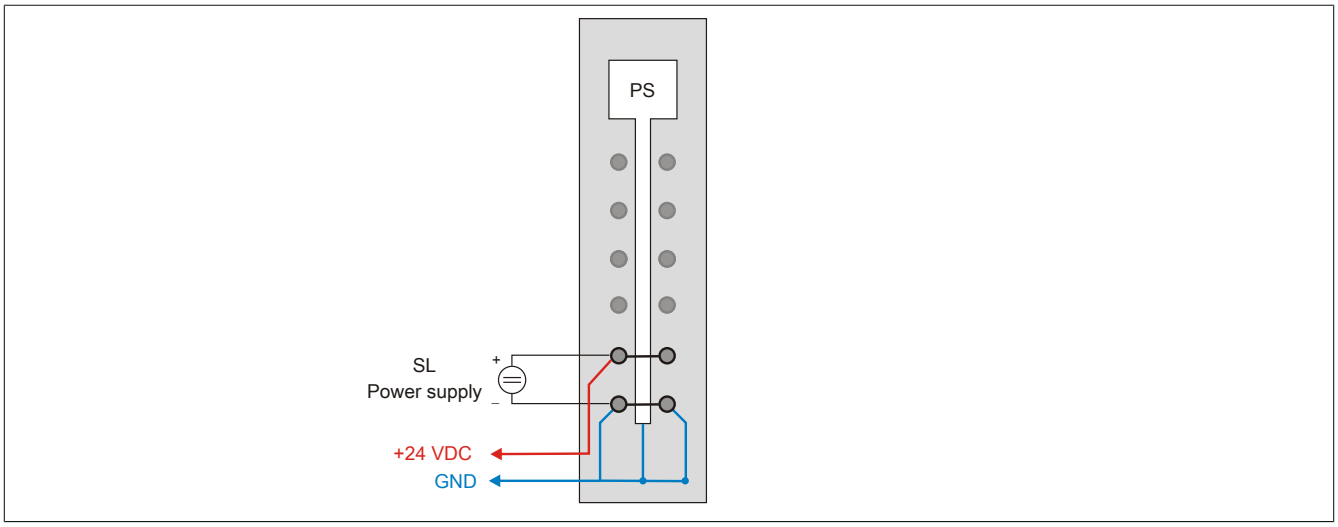


Figure 11: X20SL81x0 - Connection example

X20SL8101 - Connection example with 2 isolated power supplies

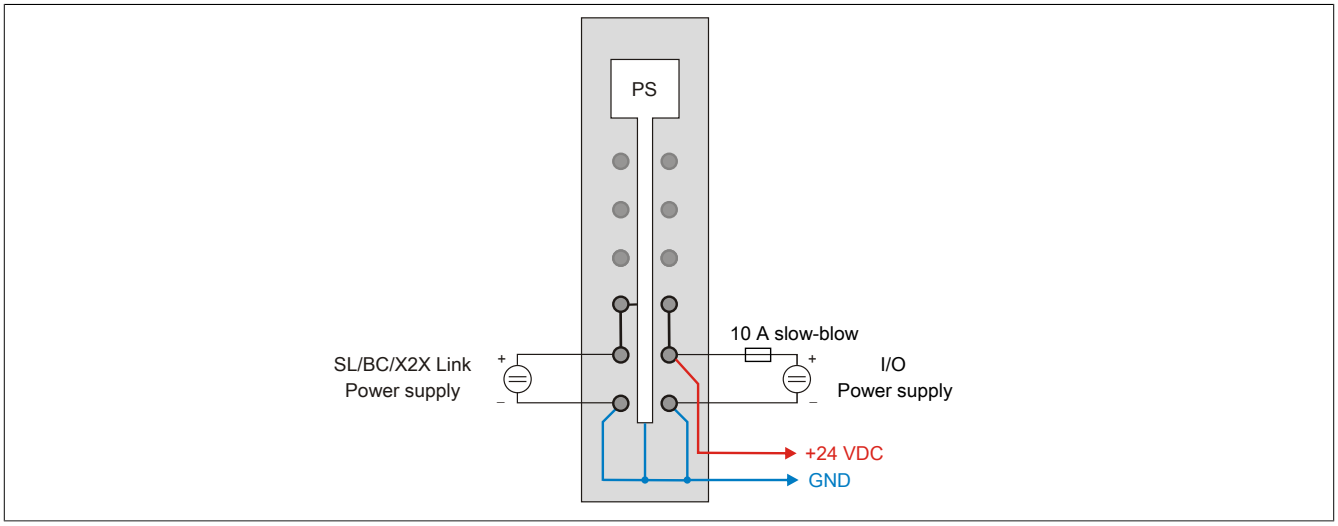


Figure 12: X20SL8101 - Connection example with 2 isolated power supplies

X20SL8101 - With one power supply and jumper

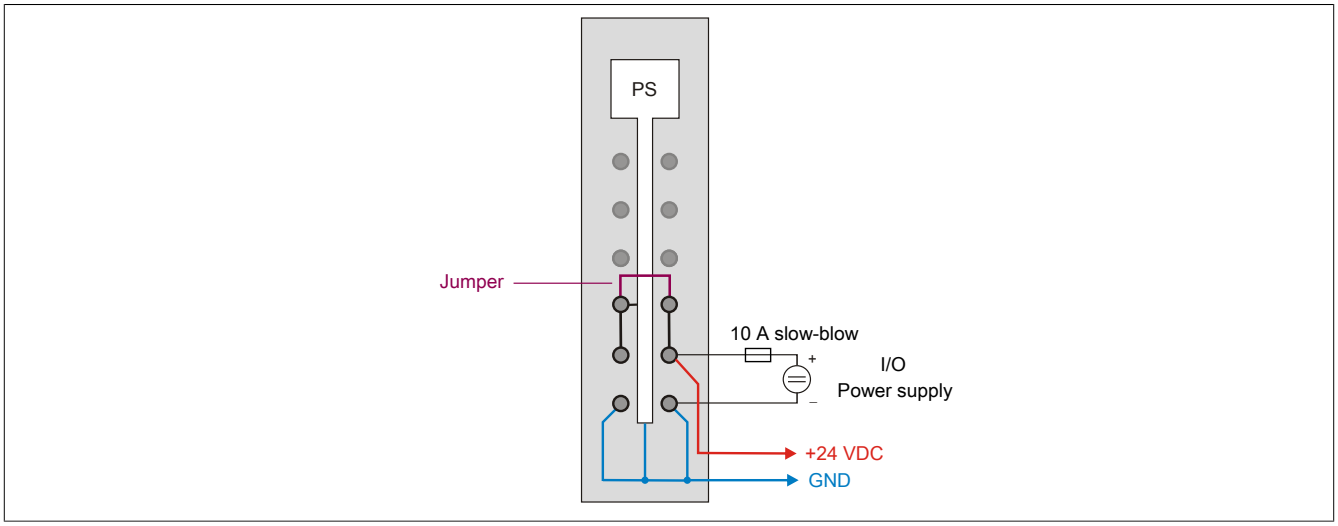


Figure 13: X20SL8101 - Connection example with a supply and jumper

5 Register description

5.1 Parameters in the I/O configuration

Group: POWERLINK parameters

Parameter	Description	Default value	Unit
Mode	SafeLOGIC can only be operated as a "controlled node" (CN). A "managing node" (MN) is not supported.	Controlled node	-

Table 15: Parameters I/O configuration: POWERLINK parameters

> **Information:**
>
> **Additional configuration parameters are available.**
> **For details, see Automation Help under "Communication → POWERLINK → AR configuration → POWERLINK controlled node configuration (SG4)".**

Group: Function model

Parameter	Description	Default value	Unit
Function model	This parameter is reserved for future functional expansions.	Default	-

Table 16: I/O configuration parameters: Function model

Group: General

Parameter	Description	Default value	Unit
Module supervised	System behavior when a module is missing	On	-
	Parameter value / **Description** On: Missing module triggers service mode Off: Missing module is ignored		
Interface Slot Enable (only X20SL8110, hardware upgrade 1.10.1.3 or later)	This parameter enables data transfer to the interface card.	On	-
	Parameter value / **Description** On: Data transfer to the interface card is enabled. Off: Data transfer to the interface card is disabled.		
Node used as IP gateway	This parameter is reserved for future functional expansions.	240	-
Standalone mode (only X20SL8101, hardware upgrade 1.10.2.x or later and Automation Runtime A4.32 or later)	This parameter enables standalone mode (see section Blackout mode in Automation Help under: Hardware → X20 system → Additional information → Blackout mode) and allows the SafeLOGIC controller to be started up without an active master.	Off	-
	Parameter value / **Description** On: Standalone mode is enabled. Off: Standalone mode is disabled.		
SafeLOGIC ID	In applications with multiple SafeLOGIC controllers, this parameter defines the unique SafeLOGIC address. • Permissible values: 1 to 1024	Assigned automatically	-
SafeMODULE ID	Unique safety address of the module • Permissible values: 1	1	-
SafeDESIGNER project	Name of the safety project	Assigned automatically	-
SafeDESIGNER version	SafeDESIGNER version of the safety project for this SafeLOGIC controller.	Assigned automatically	-
Authorization	For information about activating the "Authorization" function, see "Authorization (X20SL8xxx series only)".	Disabled	-
	Parameter value / **Description** Enabled: The "Authorization" function is enabled; the standard CPU can block acknowledgment actions from the SafeLOGIC controller. Disabled: The "Authorization" function is disabled; the standard CPU has no effect on acknowledgment functions.		

Table 17: Parameters I/O configuration: General

Group: SafeDESIGNER to SafeLOGIC communication

Starting with SafeLOGIC V1.4.0.0 and Automation Runtime V3.04:

When SPROXY is enabled, the SafeLOGIC controller can be accessed via a TCP/IP port on the standard CPU.

This uses the SafeDESIGNER setting "SL communication via the CPU" (SafeDESIGNER V2.80 or higher).

Parameter	Description	Default value	Unit
Activate SPROXY	Enables the SafeDESIGNER online connection	On	-
Server communication port	TCP/IP port number used to access the SafeLOGIC controller • Recommended values: 50,000 to 50,100 **Note:** If multiple SafeLOGIC controllers are being used in the project, then a different port number must be configured for each one!	50000	-

Table 18: I/O configuration parameters: SafeDESIGNER to SafeLOGIC communication

Group: CPU to SafeLOGIC communication

Parameter	Description	Default value	Unit
Number of BOOL channels	Number of BOOL channels from the CPU to the SafeLOGIC controller • Permissible values: 0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96.	8	-
Number of extended BOOL channels	Number of BOOL channels from the CPU to the SafeLOGIC controller • Permissible values: 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	Number of INT channels from the CPU to the SafeLOGIC controller • Permissible values: 0 to 30.	0	-
Number of UINT channels	Number of UINT channels from the CPU to the SafeLOGIC controller • Permissible values: 0 to 30.	0	-
Number of DINT channels (Safety Release 1.4 and Automation Runtime V3.08 required)	Number of DINT channels from the CPU to the SafeLOGIC controller • Permissible values: 0 to 15.	0	-
Number of UDINT channels	Number of UDINT channels from the CPU to the SafeLOGIC controller • Permissible values: 0 to 15.	0	-

Table 19: Parameters I/O configuration: CPU to SafeLOGIC communication

Group: SafeLOGIC to CPU communication

Parameter	Description	Default value	Unit
Number of BOOL channels	Number of BOOL channels from the SafeLOGIC controller to the CPU • Permissible values: 0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96.	8	-
Number of extended BOOL channels	Number of BOOL channels from the SafeLOGIC controller to the CPU • Permissible values: 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	Number of INT channels from the SafeLOGIC controller to the CPU • Permissible values: 0 to 30.	0	-
Number of UINT channels	Number of UINT channels from the SafeLOGIC controller to the CPU • Permissible values: 0 to 30.	0	-
Number of DINT channels (Safety Release 1.4 and Automation Runtime V3.08 required)	Number of DINT channels from the SafeLOGIC controller to the CPU • Permissible values: 0 to 15.	0	-
Number of UDINT channels	Number of UDINT channels from the SafeLOGIC controller to the CPU • Permissible values: 0 to 15.	0	-

Table 20: Parameters I/O configuration: SafeLOGIC to CPU communication

Group: SafeLOGIC to SafeLOGIC communication

Parameter	Description	Default value	Unit
Use as source SafeLOGIC	This parameter configures this SafeLOGIC controller as a data source for another SafeLOGIC controller.	Off	-
	Parameter value / **Description** On: This SafeLOGIC controller is available as a data source for another SafeLOGIC controller. Off: This SafeLOGIC controller is not available as a data source for other SafeLOGIC controllers.		
Extended source SafeLOGIC communication (Safety Release 1.4 and Automation Runtime V3.08 required)	Enables the option of configuring the number of data points for "SafeLOGIC to SafeLOGIC communication" (for connections where this SafeLOGIC controller serves as a data source for another SafeLOGIC controller).	Off	-
Group: Connected SafeLOGIC modules (Safety Release 1.4 and later)			
Group: Connection xx	Configuration of the maximum SafeLOGIC controllers to which this SafeLOGIC controller will establish a connection.		
SafeLOGIC ID of connection xx	SafeLOGIC ID to which the connection should be established	0	-
Group: Output channels (Safety Release 1.4 and Automation Runtime V3.08 required)			
Number of BOOL channels	Number of channels with the respective data type	8	-
Number of INT channels		0	-
Number of UINT channels		0	-
Number of DINT channels		0	-
Number of UDINT channels		0	-
Group: Input channels (Safety Release 1.4 and Automation Runtime V3.08 required)			
Number of BOOL channels	Number of channels with the respective data type	8	-
Number of INT channels		0	-
Number of UINT channels		0	-
Number of DINT channels		0	-
Number of UDINT channels		0	-

Table 21: Parameters I/O configuration: SafeLOGIC to SafeLOGIC communication

Group: Power Supply Parameter (X20SL8101 only)

Parameter	Description	Default value	Unit
Module status information	This parameter enables/disables additional status information in the I/O mapping.	On	-
Current/voltage information	This parameter enables/disables additional current and voltage information in the I/O mapping.	Off	-

Table 22: I/O configuration parameters: Power Supply Parameter

5.2 Parameters in SafeDESIGNER - up to Release 1.9

Group: Basic

<table>
<tr><th>Parameter</th><th>Description</th><th>Default value</th><th>Unit</th></tr>
<tr><td>Min_required_FW_Rev</td><td>This parameter is reserved for future functional expansions.</td><td>Basic Release</td><td>-</td></tr>
<tr><td>Cycle_Time_us</td><td>This parameter determines the cycle time of the SafeLOGIC controller.
• Permissible values: 800 to 20,000 µs (corresponds to 0.8 to 20 ms)
The set value is internally rounded up to the next whole number multiple of the POWERLINK cycle time.</td><td>2000</td><td>µs</td></tr>
<tr><td>Cycle_Time_max_us
(Release 1.5 and later)</td><td>Parameter for checking whether a maximum time between 2 SafeLOGIC cycles is exceeded.
• Permissible values: 800 to 21,000 µs (corresponds to 0.8 to 21 ms)
IMPORTANT:
This value should not be the same as the actual cycle time. Network jitter must also be taken into account.
The actual cycle time is affected by parameter "Cycle_Time_us".</td><td>21000</td><td>µs</td></tr>
<tr><td>SSDO_Creation</td><td>This parameter defines the number of asynchronous processing steps per SafeLOGIC cycle.
This parameter can be used to optimize the startup behavior of the system.
<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Time dependent</td><td>Depends on the SafeLOGIC cycle time
• Cycle times ≤3 ms = 1 per 5 cycles
• Cycle times >3 ms = 1 per cycle</td></tr><tr><td>1 per 5 cycles</td><td>One asynchronous processing step is distributed over 5 SafeLOGIC cycles
• Can lead to long startup times
• Minimum possible communication overhead in each cycle</td></tr><tr><td>1 per cycle</td><td>One asynchronous processing step per SafeLOGIC cycle
• Average startup times
• Average communication overhead in each cycle</td></tr><tr><td>5 per cycle</td><td>5 asynchronous processing steps per SafeLOGIC cycle
• Minimum startup times
• Maximum possible communication overhead in each cycle</td></tr></table></td><td>Time dependent</td><td>-</td></tr>
<tr><td>Node_Guarding_Timeout_s</td><td>Timeout for changing the safety modules to the PRE_OPERATIONAL state after the SafeLOGIC controller drops out or if there is a communication problem between the safety module and the SafeLOGIC controller.
This parameter also defines how long it takes for the SafeLOGIC controller to detect a missing module.
• Permissible values: 30 to 3000 s
Notes
• The shorter the time, the greater the amount of asynchronous data traffic.
• This setting is not critical to safety functionality. The time for safely cutting off actuators is determined independently using parameter "Worst_Case_Response_Time".</td><td>60</td><td>s</td></tr>
<tr><td>Number_of_scans</td><td>This parameter defines the number of module search scans completed during startup.
This parameter is used to optimize the startup behavior of the system, especially if optional modules are configured but not available.
• Permissible values: 1 to 10</td><td>5</td><td>-</td></tr>
<tr><td>ExternalMachineOptions
(Release 1.4 and later)</td><td>Enables external machine options
<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Yes-ATTENTION</td><td>External machine options are enabled.</td></tr><tr><td>No</td><td>External machine options are disabled.</td></tr></table></td><td>No</td><td>-</td></tr>
<tr><td>ExternalStartupFlags
(Release 1.4 and later)</td><td>Enables external startup flags
<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Yes-ATTENTION</td><td>External startup flags are enabled.</td></tr><tr><td>No</td><td>External startup flags are disabled.</td></tr></table></td><td>No</td><td>-</td></tr>
<tr><td>KeepRemanent</td><td>Automatically resets the remanent data (see Automation Help for SafeDESIGNER function block "SF_RemanentData_SAFEDINT" or "SF_RemanentData_SAFEDWORD")
<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Yes-ATTENTION</td><td>Remanent data not automatically reset</td></tr><tr><td>No</td><td>Remanent data is automatically reset if a modified SafeDESIGNER project (modified CRC and/or timestamp) is loaded to the SafeLOGIC controller.</td></tr></table></td><td>No</td><td>-</td></tr>
</table>

Table 23: SafeDESIGNER parameters: Basic

Information:

Parameter "Cycle_Time_us" must be greater than the processing time for the safety application. The processing time can be determined in the online dialog window using function "Info". If parameter "Cycle_Time_us" is less than or too close to the necessary processing time, a cycle time violation can occur.

Additional information can also be found in section "SafeLOGIC "Info" dialog box in SafeDESIGNER".

Danger!

If parameter "ExternalMachineOptions" or "ExternalStartupFlags" is set to "Yes-ATTENTION", thus enabling one of these functions to be used in SafeDESIGNER, then the associated notices in chapter "Operation via the AsSafety library" must be taken into account. Failure to do so can result in hazardous situations caused by malfunctions.

Danger!

If parameter "KeepRemanent" is set to "Yes-ATTENTION", it is important when saving data after a project download to note that the data still has the same meaning in the application program.

Group: Safety_Response_Time_Defaults

The parameters for the safety response time are generally set in the same way for all stations involved in the application. This is why these parameters are configured for the SafeLOGIC controller in the "Safety_Response_Time_Defaults" group in SafeDESIGNER.

If "Manual_Configuration = No" is set for the individual modules, then these default values are used.

Parameter	Description	Default value	Unit
Default_Synchronous_Network_Only	This parameter describes the synchronization characteristics of the network being used. They are defined in Automation Studio / Automation Runtime. **Parameter value** / **Description** Yes: In order to calculate the safety response time, networks must be synchronous and their cycle times must either be the same or an integer ratio of the cycle times. No: No requirement for synchronization of the networks.	Yes	-
Default_Max_X2X_CycleTime_us	This parameter specifies the maximum X2X cycle time used to calculate the safety response time. • Permissible values: 200 to 30,000 µs (corresponds to 0.2 to 30 ms)	5000	µs
Default_Max_Powerlink_CycleTime_us	This parameter specifies the maximum POWERLINK cycle time used to calculate the safety response time. • Permissible values: 200 to 30,000 µs (corresponds to 0.2 to 30 ms)	5000	µs
Default_Max_CPU_CrossLinkTask_CycleTime_us	This parameter specifies the maximum cycle time for the copy task on the CPU used to calculate the safety response time. The value 0 indicates that a copy task is not included for the response time. • Permissible values: 0 to 30,000 µs (corresponds to 0 to 30 ms)	5000	µs
Default_Min_X2X_CycleTime_us	This parameter specifies the minimum X2X cycle time used to calculate the safety response time. • Permissible values: 200 to 30,000 µs (corresponds to 0.2 to 30 ms)	200	µs
Default_Min_Powerlink_CycleTime_us	This parameter specifies the minimum POWERLINK cycle time used to calculate the safety response time. • Permissible values: 200 to 30,000 µs (corresponds to 0.2 to 30 ms)	200	µs
Default_Min_CPU_CrossLinkTask_CycleTime_us	This parameter specifies the minimum cycle time for the copy task on the CPU used to calculate the safety response time. The value 0 indicates that configurations without a copy task are also included for the response time. • Permissible values: 0 to 30,000 µs (corresponds to 0 to 30 ms)	0	µs
Default_Worst_Case_Response_Time_us	This parameter specifies the limit value for monitoring the safety response time. • Permissible values: 3000 to 500,000 µs (corresponds to 3 to 500 ms)	50000	µs
Default_Node_Guarding_Lifetime	This parameter specifies the maximum number of attempts to be made during the time set with parameter "Node_Guarding_Timeout_s". The purpose of these attempts is to ensure that the module is available. • Permissible values: 1 to 255 **Note** • The larger the configured value, the greater the amount of asynchronous data traffic. • This setting is not critical to safety functionality. The time for safely cutting off actuators is determined independently using parameter "Worst_Case_Response_Time_us".	5	-

Table 24: SafeDESIGNER parameters: Safety_Response_Time_Defaults

Group: Commissioning

Parameters "SafeMachineOption00" to "SafeMachineOption31" make it possible to activate or deactivate dedicated machine options during commissioning.

Parameter	Description	Default value	Unit
SafeMachineOptionXX	With this parameter, individual machine options can be enabled or disabled during commissioning.	OFF	-

Parameter value	Description
ON	Enables machine option XX. The "SafeMachineOptionXX" channel is constantly set to SAFETRUE.
OFF	Disables machine option XX. The "SafeMachineOptionXX" channel is constantly set to SAFEFALSE.

Table 25: SafeDESIGNER parameters: Commissioning

5.3 Parameters in SafeDESIGNER - Release 1.10 and later

Group: Basic

<table>
<tr><th>Parameter</th><th>Description</th><th>Default value</th><th>Unit</th></tr>
<tr><td>Min required FW Rev</td><td>This parameter is reserved for future functional expansions.</td><td>Basic release</td><td>-</td></tr>
<tr><td>SSDO Creation</td><td>This parameter defines the number of asynchronous processing steps per SafeLOGIC cycle.
It can be used to optimize the boot behavior of the system.

<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Time dependent</td><td>Depends on the SafeLOGIC cycle time
• Cycle times ≤3 ms = 1 per 5 cycles
• Cycle times >3 ms = 1 per cycle</td></tr><tr><td>1 per 5 cycles</td><td>One asynchronous processing step is distributed over 5 SafeLOGIC cycles
• Can lead to long boot times
• Minimum possible communication overhead in each cycle</td></tr><tr><td>1 per cycle</td><td>One asynchronous processing step per SafeLOGIC cycle
• Average boot times
• Average communication overhead in each cycle</td></tr><tr><td>5 per cycle</td><td>5 asynchronous processing steps per SafeLOGIC cycle
• Minimum boot times
• Maximum possible communication overhead in each cycle</td></tr></table></td><td>Time dependent</td><td>-</td></tr>
<tr><td>Node Guarding Timeout</td><td>Timeout for changing the safety modules to the PRE_OPERATIONAL state after the SafeLOGIC controller drops out or if there is a communication problem between the safety module and the SafeLOGIC controller.
This parameter also defines how long it takes for the SafeLOGIC controller to detect a missing module.
• Permissible values: 30 to 300 s
Notes
• The shorter the time, the greater the amount of asynchronous data traffic.
• This setting is not critical to safety functionality. The time for safely cutting off actuators is determined independently of this.</td><td>60</td><td>s</td></tr>
<tr><td>Number of scans</td><td>This parameter defines the number of module search scans completed while booting.
This parameter is used to optimize the startup behavior of the system, especially if optional modules are configured but not available.
• Permissible values: 1 to 10</td><td>5.
Hardware upgrade 1.10.1.0 or later: 3</td><td>-</td></tr>
<tr><td>Activate Setup Mode on empty SafeKEY (hardware upgrade 1.10.2.x or later)</td><td>This parameter enables setup mode after downloading a project to a blank SafeKEY.

<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Yes-ATTENTION</td><td>Setup mode is enabled.</td></tr><tr><td>No</td><td>Setup mode is disabled.</td></tr></table></td><td>No</td><td>-</td></tr>
<tr><td>Auto acknowledge firmware mismatch (hardware upgrade 1.10.2.x or later)</td><td>This parameter enables automatic acknowledgment of a firmware exchange (acknowledgment request "Firmware Acknowledge").

<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Yes-ATTENTION</td><td>Automatic acknowledgment of firmware exchange is enabled.</td></tr><tr><td>No</td><td>Automatic acknowledgment of firmware exchange is not enabled.</td></tr></table></td><td>No</td><td>-</td></tr>
<tr><td>Auto acknowledge SafeKEY exchange (hardware upgrade 1.10.2.x or later)</td><td>This parameter enables automatic acknowledgment of a SafeKEY exchange (acknowledgment request "SafeKEY Exchange").

<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Yes-ATTENTION</td><td>Automatic acknowledgment of SafeKEY exchange is enabled.</td></tr><tr><td>No</td><td>Automatic acknowledgment of SafeKEY exchange is not enabled.</td></tr></table></td><td>No</td><td>-</td></tr>
<tr><td>Process Data Transmission Rate (hardware upgrade 1.10.5.x or later)</td><td>This parameter defines the base transfer rate for process data.

<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>High</td><td>Normal transfer rate.</td></tr><tr><td>Low</td><td>Reduced transfer rate to support networks with low transfer rates (data transmission time >1 s).</td></tr></table></td><td>High</td><td>-</td></tr>
</table>

Table 26: SafeDESIGNER parameters: Basic

Information:

Startup time is also affected by the asynchronous bandwidth on the POWERLINK network. For optimization options, see Automation Help under Communication → POWERLINK → General information → Multiple asynchronous send.

Information:

The information in section "Setup mode" on page 70 must be observed when using parameter "Activate Setup Mode on empty SafeKEY". The information in section "Automatic acknowledgment" on page 43 must be observed when using parameters "Auto acknowledge firmware mismatch" and "Auto acknowledge SafeKEY exchange".

Group: Safety Response Time Defaults

The parameters for the safety response time are generally set in the same way for all stations involved in the application. This is why these parameters are configured for the SafeLOGIC controller in group "Safety Response Time Defaults" in SafeDESIGNER.

If "Manual Configuration = No" is set for the individual modules, then these default values are used.

Parameter	Description	Default value	Unit
Default Safe Data Duration	This parameter specifies the maximum permitted data transmission time between the SafeLOGIC controller SafeIO module. For more information about the actual data transmission time, see section Diagnostics and service → Diagnostics tools → Network analyzer → Editor → Calculation of safety runtime of Automation Help. The cycle time of the safety application must also be added. • Permissible values: 2000 to 10,000,000 µs (corresponds to 2 ms to 10 s)	20000	µs
Default Additional Tolerated Packet Loss	This parameter specifies the number of additionally tolerated lost packets during data transfer. • Permissible values: 0 to 10	0	Packets
Default Packets per Node Guarding	This parameter specifies the maximum number of packets used for node guarding. • Permissible values: 1 to 255 **Note** • The larger the configured value, the greater the amount of asynchronous data traffic. • This setting is not critical to safety functionality. The time for safely cutting off actuators is determined independently of this.	5	Packets

Table 27: SafeDESIGNER parameters: Safety Response Time Defaults

Group: Module Configuration

<table>
<tr><th>Parameter</th><th>Description</th><th>Default value</th><th>Unit</th></tr>
<tr><td>External Machine Options</td><td>Enables external machine options

<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Yes-ATTENTION</td><td>Enables external machine options</td></tr><tr><td>No</td><td>Disables external machine options</td></tr></table></td><td>No</td><td>-</td></tr>
<tr><td>External Startup Flags</td><td>Enables external startup flags

<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Yes-ATTENTION</td><td>Enables external startup flags</td></tr><tr><td>No</td><td>Disables external startup flags</td></tr></table></td><td>No</td><td>-</td></tr>
<tr><td>Keep Remanent</td><td>Automatically resets the remanent data (see Automation Help for SafeDESIGNER function block "SF_RemanentData_SAFEDINT" or "SF_RemanentData_SAFEDWORD")

<table><tr><th>Parameter value</th><th>Description</th></tr><tr><td>Yes-ATTENTION</td><td>Remanent data not automatically reset</td></tr><tr><td>No</td><td>Remanent data is automatically reset if a modified SafeDESIGNER project (modified CRC and/or timestamp) is loaded to the SafeLOGIC controller.</td></tr></table></td><td>No</td><td>-</td></tr>
<tr><td>Cycle Time</td><td>This parameter determines the cycle time of the safety application.
• Permissible values: 800 to 20,000 µs (corresponds to 0.8 to 20 ms)
The configured value is internally rounded up to the next whole number multiple of the POWERLINK cycle time.</td><td>2000</td><td>µs</td></tr>
<tr><td>Cycle Time max
(up to hardware upgrade 1.10.1.0)</td><td>Parameter for checking whether a maximum time between 2 SafeLOGIC cycles is exceeded.
• Permissible values: 800 to 21,000 µs (corresponds to 0.8 to 21 ms)
Important:
This value should not be the same as the actual cycle time. Network jitter must also be taken into account.
The actual cycle time is affected by the "Cycle Time" parameter.</td><td>21000</td><td>µs</td></tr>
</table>

Table 28: SafeDESIGNER parameters: Basic

Information:

The parameter "Cycle Time" must be greater than the processing time for the safety application. The processing time can be determined in the online dialog window using function "Info". If the parameter "Cycle Time" is less than or too close to the necessary processing time, a cycle time violation can occur.

Additional information can also be found in section "SafeLOGIC "Info" dialog box in SafeDESIGNER".

Danger!

If parameter "External Machine Options" or "External Startup Flags" is set to "Yes-ATTENTION", thus enabling one of these functions to be used in SafeDESIGNER, then the associated notices in chapter "Operation via the AsSafety library" must be taken into account. Failure to do so can result in hazardous situations caused by malfunctions.

Danger!

If parameter "Keep Remanent" is set to Yes-ATTENTION, it is important when saving data after a project download to note that the data still has the same meaning in the application program.

Group: Commissioning

Parameters "SafeMachineOption00" to "SafeMachineOption31" make it possible to activate or deactivate dedicated machine options during commissioning.

Parameter	Description	Default value	Unit
SafeMachineOptionXX	With this parameter, individual machine options can be enabled or disabled during commissioning.	OFF	-

Parameter value	Description
ON	Enables machine option XX. The "SafeMachineOptionXX" channel is constantly set to SAFETRUE.
OFF	Disables machine option XX. The "SafeMachineOptionXX" channel is constantly set to SAFEFALSE.

Table 29: SafeDESIGNER parameters: Commissioning

5.4 SafeLOGIC - Channel list

Channel name	Access via Automation Studio	Access via SafeDESIGNER	Data type	Description
ModuleOk	Read	-	BOOL	Indicates if the module is OK
SerialNumber	Read	-	UDINT	Module serial number
ModuleID	Read	-	UDINT	Module ID
HardwareVariant	Read	-	UDINT	Hardware variant
FirmwareVersion	Read	-	UDINT	Firmware version of the module
SafeFirmwareVersion	Read	-	UINT	Hardware upgrade 1.10.1.4 or later: Channel for reading the version of the safe firmware
UDID_low	Read	-	UDINT	UDID, lower 4 bytes
UDID_high	Read	-	UINT	UDID, upper 2 bytes
BOOL1xx	Write	Read	BOOL	CPU to SafeLOGIC communication channel
BOOLext1xxx	Write	Read	BOOL	CPU to SafeLOGIC communication channel
INT1xx	Write	Read	INT	CPU to SafeLOGIC communication channel
UINT1xx	Write	Read	UINT	CPU to SafeLOGIC communication channel
DINT1xx	Write	Read	DINT	CPU to SafeLOGIC communication channel
UDINT1xx	Write	Read	UDINT	CPU to SafeLOGIC communication channel
BOOL0xx	Read	Write	BOOL	SafeLOGIC to CPU communication channel
BOOLext0xxx	Read	Write	BOOL	SafeLOGIC to CPU communication channel
INT0xx	Read	Write	INT	SafeLOGIC to CPU communication channel
UINT0xx	Read	Write	UINT	SafeLOGIC to CPU communication channel
DINT0xx	Read	Write	DINT	SafeLOGIC to CPU communication channel
UDINT0xx	Read	Write	UDINT	SafeLOGIC to CPU communication channel
SafeBOOLx	-	Write	SAFEBOOL	SafeLOGIC to SafeLOGIC communication channel
SafeMachineOptionxx	-	Read	SAFEBOOL	Internal channel for machine options
ExternalMachineOptionsBITxxx	-	Read	SAFEBOOL	Internal channels for external machine options
ExternalMachineOptionsINTxx	-	Read	SAFEINT	Internal channels for external machine options
ExternalMachineOptionsUINTxx	-	Read	SAFEWORD	Internal channels for external machine options
ExternalMachineOptionsDINTxx	-	Read	SAFEDINT	Internal channels for external machine options
ExternalMachineOptionsUDINTxx	-	Read	SAFEDWORD	Internal channels for external machine options

Table 30: SafeLOGIC - Channel list

Information:

Channels for SafeLOGIC to SafeLOGIC communication: See Display in SafeDESIGNER

Information:

Additional diagnostic data points are available on the X20SL8101 and the X20SL8110.

For details, see Communication → POWERLINK → Diagnostics → Diagnostic data points → Bus controller in Automation Help.

In addition, the following data can be read via POWERLINK registers:

Index:Subindex	Object name	Data type	Access	Values	Description
0x2000:0x04	SafetyFWversion1	UDINT	Read	-	Higher-order 2 bytes: Hardware variant of the module Lower-order 2 bytes: Firmware version - Safety processor 1
0x2000:0x05	SafetyFWversion2	UDINT	Read	-	Higher-order 2 bytes: Hardware variant of the module Lower-order 2 bytes: Firmware version - Safety processor 2
0x2000:0x08	Project_CRC	UDINT	Read	-	CRC of the SafeDESIGNER project
0x2000:0x09	Project_Time	DATE_AND_TIME	Read	-	Timestamp of the SafeDESIGNER project
0x2000:0x0C	Project_Name	STRING (without zero termination)	Read	-	Project name of the SafeDESIGNER project
0x2000:0x0D	Project_Author	STRING (without zero termination)	Read	-	Name of the author of the SafeDESIGNER project
0x2000:0x0E	SafeOS_RUN_STATE	BOOL	Read	0	SafeOS is not in RUN (identical to SafeOSstate!=0x66)
				1	SafeOS is in RUN (identical to SafeOSstate==0x66)
0x2000:0x0F	BOOT_STATE	UDINT	Read	General firmware startup status. Using the updated "Bootstate" object (0x2410:0x01) is recommended.	
				0x00	Startup not yet begun
				0x01	Initialization started
				0x10	Cyclic hardware tests running
				0x11	openSAFETY stack running
				0x12	SafeOS running
0x2000:0x10	openSAFETYstate	UDINT	Read	0	PREOPERATIONAL state (all cyclic safe data zeroed out)
				1	OPERATIONAL state
0x2000:0x11	SafeOsState	UDINT	Read	Status of the safety application, corresponds to the R/E LED on the SafeLOGIC controller. For details, see "SafeLOGIC "Info" dialog box in SafeDESIGNER".	
				0x00	Invalid (e.g. SafeKEY blank) or startup still active (BOOT_STATE!=0x12)
				0x0F	ON (startup / internal initialization) or error (check logbook)
				0x33	Loading (startup / internal initialization)
				0x55	Stop [Safe]
				0x66	Run [Safe]
				0x99	Halt [Debug]
				0xAA	Stop [Debug]
				0xCC	Run [Debug]
				0xF0	No execution
0x2000:0x12	Temperature	INT	Read	-	Measured temperature in 0.1°C

The following objects are available in hardware upgrade 1.10.4.0 and later:

Index:Subindex	Data type	Access	Values	Description
0x2410:0x01	UDINT	Read	Boot state. Startup state of the SafeLOGIC controller. Notes: • Some of the boot states do not occur during normal startup or are cycled through so quickly that they are not visible externally. • The boot states usually cycle through in ascending order. There are cases, however, in which a previous value is captured.	
			0x0003	Startup communication processor OK, no communication to the safety processors
			0x0008	SafeKEY check (valid SafeKEY not connected)
			0x0010	FAILSAFE. At least one of the safety processors is in the safe state.
			0x0020	Internal communication to safety processors started
			0x0024	Firmware update of safety processors
			0x0030	Startup of safety processors
			0x0040	Firmware of safety processors started
			0x0440	Firmware of safety processors running
			0x0840	Loads the SafeDESIGNER application or valid SafeDESIGNER application not found
			0x1840	Waiting for acknowledgments (e.g. module replacement)
			0x2040 ... 0x2A40	SCAN: The safety modules being used are being looked for in the network and configured. Multiple scan cycles are carried out based on SafeDESIGNER parameter "Number of Scans" until all modules are found: 0x2040: First cycle 0x2140: Second cycle 0x2240: Third cycle ...
			0x3040	Missing modules. Startup cannot be resumed since modules are missing that are configured with "Optional = No".
			0x3440	Configuration of existing safety modules completed. Stabilizing cyclic openSAFETY data exchange. **Note:** If the boot state remains here, check SafeDESIGNER parameters "(Default) Safe Data Duration", "(Default) Additional Tolerated Packet Loss".
			0x4040	RUN. Final state, startup completed.
0x2410:0x02	UDINT	Read	-	SCAN progress (how many modules have already been processed in the current scan)

Index:Subindex	Data type	Access	Values	Description
0x2410:0x03	UDINT	Read	-	Supply voltage (in mV)
0x2410:0x04	UDINT	Read	-	CRC of firmware header on safety processor 1
0x2410:0x05	UDINT	Read	-	CRC of firmware header on safety processor 2
0x2410:0x06	UDINT	Read	-	Maximum cycle time (time from cycle start to cycle end)
0x2410:0x07	UDINT	Read	-	Cycle start interval (time from one cycle start to next cycle start)
0x2410:0x08	UDINT	Read	-	SafeLOGIC status word
0x2410:0x09	UDINT	Read	-	Number of missing modules
0x2410:0x0A	UDINT	Read	-	Number of UDID mismatches
0x2410:0x0B	UDINT	Read	-	Number of firmware mismatches
0x2410:0x0C	UDINT	Read	-	Number of configured modules
0x2410:0x0D	UDINT	Read	-	Flag for missing subsequently loadable files: Bit 0: Machine options missing in AUTOCNF.BIN Bit 1: Startup flags missing in AUTOCNF.BIN Bit 2: EMODATA1.BIN missing Bit 3: TABDATA1.BIN
0x2410:0x0E	UDINT	Read	-	openSAFETY common event counter SERR_k_SFS_LENGTH
0x2410:0x0F	UDINT	Read	-	openSAFETY common event counter SERR_k_SFS_TOO_LONG
0x2410:0x10	UDINT	Read	-	openSAFETY common event counter SERR_k_SFS_FRM_ID
0x2410:0x11	UDINT	Read	-	openSAFETY common event counter SERR_k_SFS_SADR_INV
0x2410:0x12	UDINT	Read	-	openSAFETY common event counter SERR_k_SFS_SDN_INV
0x2410:0x13	UDINT	Read	-	openSAFETY common event counter SERR_k_SFS_TADR_INV
0x2410:0x14	UDINT	Read	-	openSAFETY common event counter SERR_k_SFS_CRC1
0x2410:0x15	UDINT	Read	-	openSAFETY common event counter SERR_k_SFS_CRC2
0x2410:0x16	UDINT	Read	-	openSAFETY common event counter SERR_k_SFS_DATA
0x2410:0x17	UDINT	Read	-	openSAFETY common event counter SERR_k_CYC_REJECT
0x2410:0x18	UDINT	Read	-	openSAFETY common event counter SERR_k_CYC_ERROR
0x2410:0x19	UDINT	Read	-	openSAFETY common event counter SERR_k_ACYC_REJECT
0x2410:0x1A	UDINT	Read	-	openSAFETY common event counter SERR_k_ACYC_RETRY
0x2410:0x1B to 0x2410:0x1F	UDINT	Read	-	Reserved for future openSAFETY common event counters
0x2410:0x20	UDINT	Read	-	Number of SCFM errors
0x2410:0x21	UDINT	Read	-	Number of SCM errors
0x2410:0x22	UDINT	Read	-	Number of SDN errors
0x2410:0x23	UDINT	Read	-	Number of SFS errors
0x2410:0x24	UDINT	Read	-	Number of SHNF errors
0x2410:0x25	UDINT	Read	-	Number of SNMTM errors
0x2410:0x26	UDINT	Read	-	Number of SNMTS errors
0x2410:0x27	UDINT	Read	-	Number of SOD errors
0x2410:0x28	UDINT	Read	-	Number of SPDO errors
0x2410:0x29	UDINT	Read	-	Number of SSC errors
0x2410:0x2A	UDINT	Read	-	Number of SSDOC errors
0x2410:0x2B	UDINT	Read	-	Number of SSDOS errors
0x2410:0x2C to 0x2410:0xFE	UDINT	Read	-	Reserved for future expansions
0x2424:0x01	UDINT	Read	-	AutoCnf.bin - Timestamp
0x2424:0x02	UDINT	Read	-	AutoCnf.bin - Number of CRCs
0x2424:0x03	UDINT	Read	-	AutoCnf.bin - Size of file in bytes
0x2424:0x04 to 0x2424:0x0A	UDINT	Read	-	AutoCnf.bin - Reserved for future expansions
0x2424:0x0B to 0x2424:0xn	UDINT	Read	-	AutoCnf.bin - CRC 1 to N
0x2424:0xn+1 to 0x2424:0xFE	UDINT	Read	-	AutoCnf.bin - Reserved for future expansions
0x2425:0x01	UDINT	Read	-	EmoData1.bin - Timestamp
0x2425:0x02	UDINT	Read	-	EmoData1.bin - Number of CRCs
0x2425:0x03	UDINT	Read	-	EmoData1.bin - Size of file in bytes
0x2425:0x04 to 0x2425:0x0A	UDINT	Read	-	EmoData1.bin - Reserved for future expansions
0x2425:0x0B to 0x2425:0xn	UDINT	Read	-	EmoData1.bin - CRC 1 to N
0x2425:0xn+1 to 0x2425:0xFE	UDINT	Read	-	EmoData1.bin - Reserved for future expansions
0x2426:0x01	UDINT	Read	-	TabData1.bin - Timestamp
0x2426:0x02	UDINT	Read	-	TabData1.bin - Number of CRCs
0x2426:0x03	UDINT	Read	-	TabData1.bin - Size of file in bytes
0x2426:0x04 to 0x2426:0x0A	UDINT	Read	-	TabData1.bin - Reserved for future expansions
0x2426:0x0B to 0x2426:0xn	UDINT	Read	-	TabData1.bin - CRC 1 to N
0x2426:0xn+1 to 0x2426:0xFE	UDINT	Read	-	TabData1.bin - Reserved for future expansions
0x2427:0x01	UDINT	Read	-	ParData1.bin - Timestamp
0x2427:0x02	UDINT	Read	-	ParData1.bin - Number of CRCs

Index:Subindex	Data type	Access	Values	Description
0x2427:0x03	UDINT	Read	-	ParData1.bin - Size of file in bytes
0x2427:0x04 to 0x2427:0x0A	UDINT	Read	-	ParData1.bin - Reserved for future expansions
0x2427:0x0B to 0x2427:0xn	UDINT	Read	-	ParData1.bin - CRC 1 to N
0x2427:0xn+1 to 0x2427:0xFE	UDINT	Read	-	ParData1.bin - Reserved for future expansions

The following information about each openSAFETY node can be retrieved in object range 0x2416 to 0x2423 (data type: UDINT, Access: Read):

Parameter ID	Value
0	SafeModule ID
1	Status word Bit 0: Missing module Bit 1: Firmware mismatch on module Bit 2: UDID mismatch on module Bit 3: Reserved Bit 4: Reserved Bit 5: "Connection valid" bit of module Bit 6 to 31: Reserved
2	Connection valid statistics (number of negative edges of the connection valid bit)
3	Propagation delay statistics (average value of the data transmission time). Unit: 100 µs

The following formulas must be used to calculate the index/subindex.

$$Index = \frac{Module\ \ number}{23} + 0x2416$$

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

Module number: Sequential number of the desired module
Parameter ID: See previous table

5.5 Power supply module (X20SL8101 only) - Channel list

A power supply module is already integrated on station 1 on the X2X Link.

Channel name	Access via Automation Studio	Access via SafeDESIGNER	Data type	Description
ModuleOk	Read	-	BOOL	Indicates if the module is OK
ModuleID	Read	-	UINT	Module code
HardwareVariant	Read	-	UINT	Hardware variant
FirmwareVersion	Read	-	UINT	Firmware version of the module
StatusInput01	Read	-	BOOL	Warning if overcurrent (>2.3 A) or undervoltage (<4.7 V)
StatusInput02	Read	-	BOOL	I/O power supply below the warning level of 20.4 V
SupplyCurrent	Read	-	USINT	Bus supply current with a resolution of 0.1 A
SupplyVoltage	Read	-	USINT	Bus supply voltage with a resolution of 0.1 V

Table 31: Power supply module channel list

5.6 SafeLOGIC "Info" dialog box in SafeDESIGNER

Dialog box "SafePLC info" appears if the "Info" button in dialog box "SafePLC" (control dialog box) or in dialog box "Debug" is pressed.

The dialog box shows information about the current project in the safe programming system, the project stored/ running on the safety controller, the current status of the safety controller, debugging information, etc.

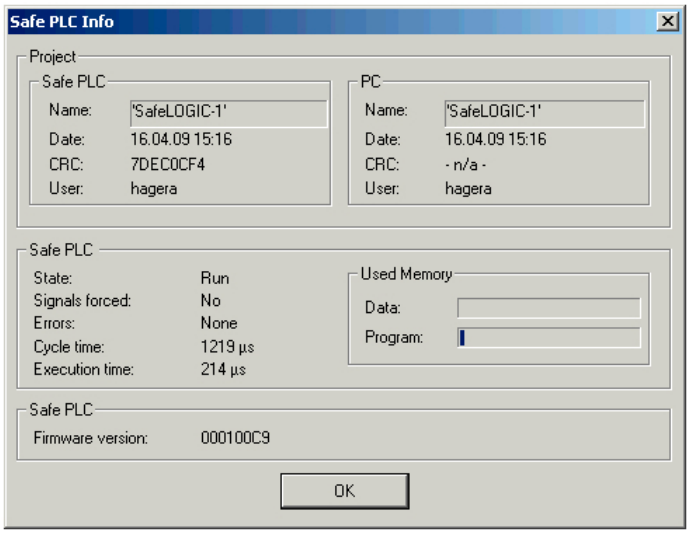


Figure 14: SafeLOGIC "Info" dialog box

Project	**Project-defining data**	
Safe PLC	Project data saved on the SafeKEY being used for the SafeLOGIC controller	
	Name	Name of the project
	Date	Date of the last change
	CRC	CRC
	User	User who made the last change
PC	SafeDESIGNER project data on the PC	
	Name	Name of the project
	Date	Date of the last change
	CRC	CRC, "- n/a -" if the project is not yet compiled
	User	User who made the last change
Safe PLC	**Status and information about the SafeLOGIC controller**	
State	Indicates the operating states of the safety controller.	
Signals forced	No	No variables are forced.
	Yes	Variables are forced.
Errors	Information regarding error messages present in the SafeDESIGNER message window	
Cycle time	Cycle time that is actually required, maximum value since the last power up This value is only relevant if "Safe PLC state = Run".	
Execution time	Actual application execution time This value corresponds to the "Safe PLC Cycle time" minus system and communication overhead.	
Used memory	Bar that shows the system resources being used	
	Data	Data memory for the safety application
	Program	Application memory for the safety application
Firmware version	Firmware version	

6 Maintenance scenarios

The operating elements on the SafeLOGIC controller (X20SL8xxx series) or the operating elements of the "Remote Control" in SafeDESIGNER (X20SL8xxx series and X20SLXxxx series) are available to handle the following maintenance scenarios.

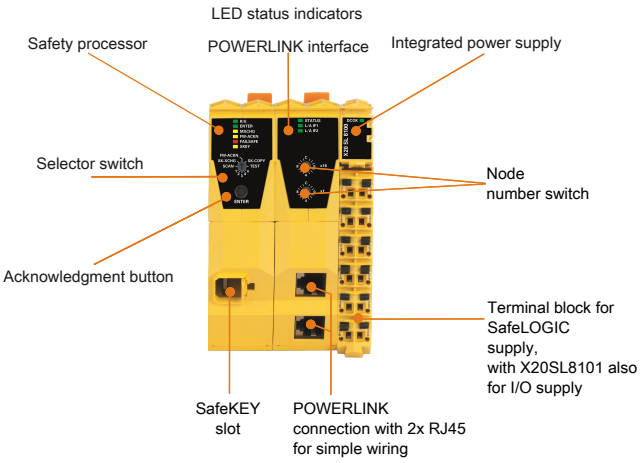


Figure 15: X20SL810x - Operating elements

For a detailed description of operating elements, see section Operating and connection elements of the technical data sheet for X20SL8xxx-series devices.

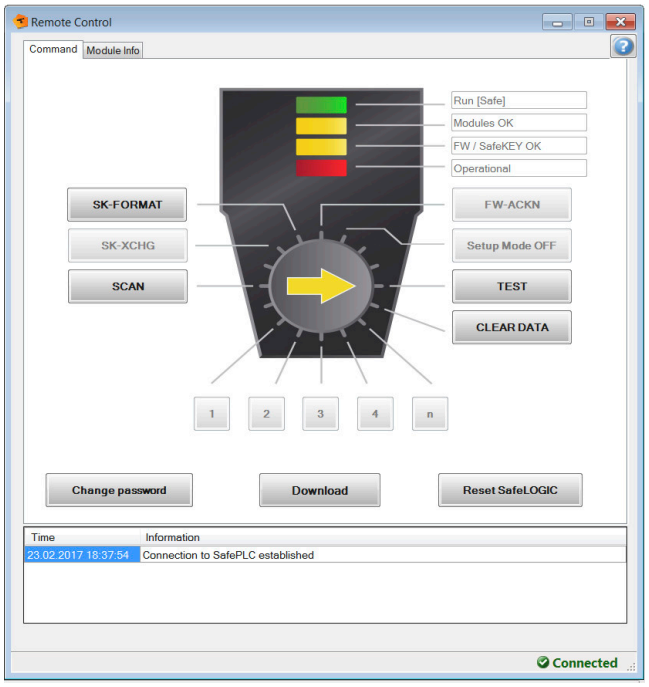


Figure 16: SafeDESIGNER - "Remote control" operating elements

For a detailed description of operating elements, see SafeDESIGNER section Operating elements of the Remote Control in Automation Help.

6.1 Module replacement

The SafeLOGIC controller recognizes on its own when safe modules have been replaced. Following a module replacement, the complete system (SafeLOGIC, SafeLOGIC-X system components, openSAFETY) automatically ensures that the module operates again using the correct parameters and that incompatible modules are rejected. Nevertheless, the following errors are still possible after a module replacement:

- Terminals swapped between several modules
- Wiring errors
- SafeIO modules swapped with each other

6.1.1 Terminals swapped between several modules

To determine whether terminals have been swapped between several modules, the user must test the safety function by performing a wiring test.

> **Danger!**
>
> **The user must ensure that the wiring test can detect when terminals have been swapped.**
>
> **Be sure to validate the entire safety function!**

6.1.2 Wiring errors

A wiring error can occur if the wiring between the sensor or actuator and the X20 terminal is disconnected. To detect this sort of error in the wiring, the user must test the safety function by performing a wiring test.

Danger!

The user must make sure that the wiring test can detect wiring errors.

Be sure to validate the entire safety function!

6.1.3 SafeIO modules swapped with each other

Errors in the standard application can cause SafeIO modules to become swapped, which appears identical to a module replacement to the SafeLOGIC controller. To detect this error, the user must confirm the number of replaced modules. This links the number of modules replaced by the user and the replacements recognized by the system so that any additional replacements can be detected.

The user is informed of the number of detected module replacements via the MXCHG status. In the process, the module identifiers (UDIDs) on the SafeKEY or in the safety section of the CompactFlash card are compared to the UDIDs of the modules in the network.

If there are 1, 2, 3 or 4 different UDIDs, the user is provided information about the exact number of differences. The user must then check whether the number of replaced modules recognized by the SafeLOGIC controller corresponds to the actual number of replaced modules. If the values are the same, the user must confirm the number and perform a wiring test. This wiring test can be limited specifically to the modules that have been replaced.

If there are more than 4 different UDIDs, a standard message is provided indicating that there are differences on more than 4 modules. In this case, the user must perform a comprehensive wiring test for all modules.

If the number of modules indicated and the actual number of replaced modules do not match, the user must confirm the number of replacements determined by the SafeLOGIC controller and perform a comprehensive wire test for all modules.

Danger!

Be sure to validate the entire safety function!

6.1.4 Replacing an individual module

If only one module was replaced (MXCHG status indicates 1 module was replaced) and the wiring was not changed, the user can skip the wiring test because in this case the following errors can be ruled out:

- Terminals swapped between several modules
- Wiring errors
- SafeIO modules swapped with each other

Danger!

The wiring test can only be excluded if no additional changes are made when replacing an individual module (e.g. unplugging terminals, removing the wiring, etc.).

6.1.5 Confirming a module replacement

To confirm the number of the replaced modules, the correct number of modules must be selected:

- 1 - One module replaced
- 2 - Two modules replaced
- 3 - Three modules replaced
- 4 - Four modules replaced
- n - Five or more modules replaced

The replacement can be confirmed and the accompanying wiring test can be limited to the replaced modules when up to four modules are replaced. When more than four modules are replaced, a comprehensive wiring test must be performed for all modules.

Following confirmation of the module replacement, the SafeLOGIC controller immediately commences a module scan.

Danger!

The user must ensure that the wiring test can detect a wiring error or when terminals have been swapped.

Be sure to validate the entire safety function!

6.2 Other errors in module configuration

The aforementioned differences are limited exclusively to module replacements. An error – "Missing module" status – is reported if a device is missing (except when the device is defined as optional), has an incorrect hardware code or other problems are present on the module (e.g. incorrect parameters that may not be changed by the SafeLOGIC controller). This status is only indicated if a module or firmware replacement is not being indicated. This status cannot be acknowledged.

Danger!

It is your responsibility to ensure that all necessary repair measures are initiated after an error occurs since subsequent errors can result in a hazard!

6.3 Acknowledging a firmware modification

A change to the firmware is indicated by the FW-ACKN status and must be confirmed using the FW-ACKN action. A firmware modification must always be concluded with full functional testing.

Danger!

Functional testing is only permitted to be performed by personnel familiar with the safety application and its functions and trained in the procedure of exchanging firmware.

Be sure to validate the entire safety function!

Danger!

Only use firmware versions listed in the FS certificates for B&R safety technology. These FS certificates are available for download from the B&R website at http://www.br-automation.com.

6.4 Triggering a module scan

A module scan determines if all configured modules are present in the application and if they correspond to the project configuration. The module scan runs automatically but at large time intervals. To minimize the time it takes for the SafeLOGIC controller to recognize a newly replaced module, this function can also be triggered manually by the user. The result of the scan is described in the following sections:

- "Module replacement"
- "Other errors in module configuration"
- "Acknowledging a firmware modification"

The process itself is started using the SCAN function and indicated using the "Scanning" status. The results are reported after the "Scanning" status is completed (e.g. three modules replaced).

6.5 SafeKEY or safety section of the CompactFlash card

The following data is stored on the SafeKEY (X20SL8xxx series) or in the safety section of the CompactFlash card (X20SLXxxx series):

- SafeDESIGNER application (application and all SafeDESIGNER parameters for the modules)
- Configuration (unique module code (UDID), firmware versions of modules)
- Subsequently loadable data elements (machine options, tables, etc.)

Size of the SafeDESIGNER application on the SafeKEY

The size of the current application on the SafeKEY is calculated by SafeDESIGNER during compilation and displayed in the message window (e.g. "The safety application uses 0.688 MB (11 sectors) memory.").

Notes:

- The output only takes the size of the SafeDESIGNER application into account. Space on the data storage device used by firmware or subsequently loadable data (tables, machine options, etc.) is not taken into account.
- If the online project comparison is not needed (see Automation Help → SafeDESIGNER), the download size of the application can be reduced by disabling the following communication setting: Online → Communication settings → Download project source to SL.

6.5.1 Removing a SafeKEY (X20SL8xxx series only)

Removing a SafeKEY always results in a change to BOOT mode, and the safety application is completely shut down.

Information:

Removing a SafeKEY during operation causes the SafeLOGIC controller to be restarted and all safety-related actuators to be cut off.

Removing a SafeKEY during operation can destroy the data on the SafeKEY.

Removing a SafeKEY during operation must therefore be avoided at all cost.

The "Backing up the SafeKEY" sequence is not affected by this general rule.

6.5.2 Acknowledging a SafeKEY replacement

Replacing a SafeKEY or replacing a CompactFlash card with a CompactFlash that has a modified safety section is indicated by the "FW-ACKN" status and must be acknowledged with the SK-XCHG function. Complete functional testing is then required.

Information:

A SafeKEY replacement can only be acknowledged if a valid SafeDESIGNER project has already been transferred to the SafeKEY or CompactFlash card.

Danger!

Replacing a SafeKEY or CompactFlash card will enable the safety application stored on the SafeKEY or CompactFlash card. Always check the project CRC and date that the safety application project was saved on the SafeKEY or CompactFlash card.

Danger!

Be sure to validate the entire safety function!

6.5.3 Changing the application on the SafeLOGIC controller by replacing the SafeKEY (X20SL8xxx series only)

All relevant configuration data and all application data and parameters are stored on the SafeKEY. In order to transfer the previous configuration data to a new SafeKEY when changing the application, the following sequence must be carried out.

- Set the selector switch to the SK-COPY position.
- Press the acknowledgment button - Action confirmed by the ENTER LED.
- The SafeKEY configuration data is saved on the SafeLOGIC controller. The SKEY LED blinks with each access.
- The FW-ACKN LED will flash after the copying procedure. This SafeKEY can now be replaced by the SafeKEY with the new application. 30 seconds are provided to do this. The FW-ACKN LED blink frequency increases after 20 seconds to signal the end of the replacement phase.
- The acknowledgment button must be pressed again after the new SafeKEY has been inserted. The selector switch remains on the setting SK-COPY.
- The internal, temporarily saved configuration data is saved on the new SafeKEY. A reset is then triggered automatically, and the data from the new SafeKEY is applied.
- Following the reset, the SafeKEY replacement must be acknowledged. To do this, move the selector switch to the setting SK-XCHG.
- Press the acknowledgment button - Action confirmed by the ENTER LED.
- Perform complete functional testing.

Information:

If the new SafeKEY is not acknowledged after 30 seconds, the function will end, i.e. if the function is triggered inadvertently, the copy function ends automatically after 30 seconds. If a SafeKEY is not inserted after 30 seconds, the SafeLOGIC controller switches to BOOT mode.

Danger!

This procedure enables the safety application stored on the new SafeKEY. Always check the project CRC and date that the safety application project was saved on the SafeKEY.

Danger!

Be sure to validate the entire safety function!

Information:

This sequence can also be used to create a SafeKEY backup using a second SafeKEY with an identical safety application. After executing the sequence, two identical SafeKEYs are available (backup copy).

Information:

Only data relevant to the machine is copied, not all of the safety application data.

6.6 Replacing a SafeLOGIC controller

Replacing a SafeLOGIC controller involves the same procedures as a normal module replacement. When replacing a SafeLOGIC controller, the SafeKEY from the SafeLOGIC controller being replaced must be kept in order to avoid activating an old safety-related application.

Danger!

Be sure to validate the entire safety function!

6.7 Authorization (X20SL8xxx series only)

The following functions can be blocked by the standard CPU:

- Confirming a module replacement
- Acknowledging a firmware modification
- Acknowledging a SafeKEY replacement
- Backing up the SafeKEY
- Replacing a SafeLOGIC controller

This allows actions to be executed in accordance with an application-specific user concept. This option is not possible from a safety perspective, however, since these functions are executed on the standard CPU.

The following table lists the associated objects in Index "0x2402" that can be accessed using the POWERLINK library.

Index:Subindex	Object description	Data type	Access	Value	Description
0x2402:0x00	NumberOfEntries	USINT	R	0x22	Number of entries in this index
0x2402:0x01	EnableAuthorization	UDINT	RW	"AENA", 0x41454E41	Enables authorization
				"ADIS", 0x41444953	Disables authorization
0x2402:0x04	EnableModuleExchange	UDINT	RW	"UDID", 0x55444944	Provides authorization to acknowledge a module replacement
				All other values	Does not provide authorization to acknowledge a module replacement
0x2402:0x05	EnableFWMismatch	UDINT	RW	"FWAC", 0x46574143	Provides authorization to acknowledge a firmware replacement
				All other values	Does not provide authorization to acknowledge a firmware replacement
0x2402:0x06	EnableSKeyExchange	UDINT	RW	"SKEY", 0x534B4559	Provides authorization to acknowledge a SafeKEY replacement
				All other values	Does not provide authorization to acknowledge a SafeKEY replacement

User requests made to the SafeLOGIC controller that are not authorized by the CPU are indicated by a steadily lit ENTER LED.

7 Software functions

7.1 Operation via the AsSafety library

Information about using library "AsSafety" is available under Programming -> Libraries -> Safety -> AsSafety in Automation Help.

7.2 Automatic acknowledgment

As specified in previous chapters, automatic acknowledgment is usually not permitted. Provided that the user implements appropriate quality assurance measures and/or constraints, it is nevertheless possible to deviate from this to permit the following automatic acknowledgment.

Danger!

The automatic acknowledgment of SafeLOGIC controller acknowledgment requests under improper circumstances is not permitted and can lead to dangerous states.

It is the sole responsibility of the user to assess the requirements of the safety application in order to determine whether additional measures are necessary.

7.2.1 "SafeKEY exchange" acknowledgment request

The SafeDESIGNER application and machine option are saved in the safety section of the CompactFlash card (X20SLXxxx series) or on the SafeKEY (X20SL8xxx series). Replacing the CompactFlash card or SafeKEY may result in the unintended exchange of this data. The "SafeKEY exchange" acknowledgment request is meant to prevent this unintentional exchange of data.

It is important to ensure that the following criteria are met with regard to automatic acknowledgment that potentially involves CompactFlash cards or SafeKEYs:

- The SafeDESIGNER application must be completely validated on a reference machine.
- The machine options file must be completely validated on a reference machine.
- Sufficient measures must be implemented to prevent the SafeDESIGNER application or machine options file from being mixed up across different machine types.
- No test versions of the SafeDESIGNER application or machine options file are permitted.

Under the conditions specified, an automated update of the SafeDESIGNER application or machine options file is permitted to be implemented on the SafeLOGIC/SafeLOGIC-X controller.

7.2.2 "Firmware acknowledge" acknowledgment request

B&R Automation Runtime sees to it independently that the firmware versions stored on the CompactFlash card are transferred to the automation components in the network. This mechanism may cause other firmware versions to be enabled in the system than those that were active when the SafeDESIGNER application was validated. A change to the firmware of the safety modules always requires revalidation of the SafeDESIGNER application. The "Firmware acknowledge" acknowledgment request is meant to prevent an unintentional exchange of firmware versions.

It is important to ensure that the following criteria are met with regard to automatic acknowledgment that potentially involves CompactFlash cards:

- The firmware files installed on the safety modules must be completely validated together with the SafeDESIGNER application on a reference machine.

7.2.3 "UDID mismatch" acknowledgment request

The "UDID mismatch" request occurs in the following situations:

- When modules are exchanged by the user (e.g. during a service call). In this case, it is possible for the connection lines to be mixed up.
- When errors occur in the standard application that lead to a mix-up of modules.

To rule out these mix-ups, a wiring test must be performed after a "UDID mismatch" request is acknowledged.

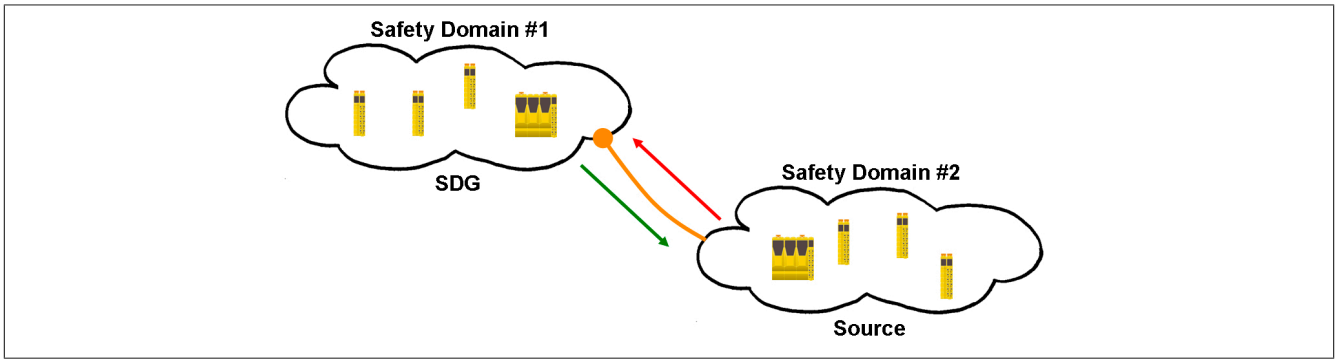
The "UDID mismatch" acknowledgment request is meant to prevent the unintentional mix-up of signals caused by exchanging a module or errors in the standard application.

- Service personnel are to be informed that the mandatory wiring test when exchanging modules must be performed independently of the automatic acknowledgment of the "UDID mismatch" request.
- It is not permitted to use more than 1 module per module type in the Automation Studio application or SafeDESIGNER application.

If the last requirement cannot be met, a "UDID mismatch" acknowledgment request is not permitted to be acknowledged automatically since it would not cover the possible mix-up of signals caused by errors in the standard application.

7.3 SafeLOGIC to SafeLOGIC communication

The safety system makes it possible to exchange safety-related information between two safety controllers (SafeLOGIC). SafeLOGIC to SafeLOGIC communication can be used to implement functions such as a global E-stop across a machine network or if a dependency exists between the safety applications on two or more machines. This makes it possible to establish a central collection point for safety information that will be responsible for distributing current values to all relevant locations.



Information:

The safety domain number is taken from the SafeLOGIC ID. In order to use SafeLOGIC to SafeLOGIC communication, the SafeLOGIC IDs must be unique. This uniqueness should be taken into consideration from the very beginning.

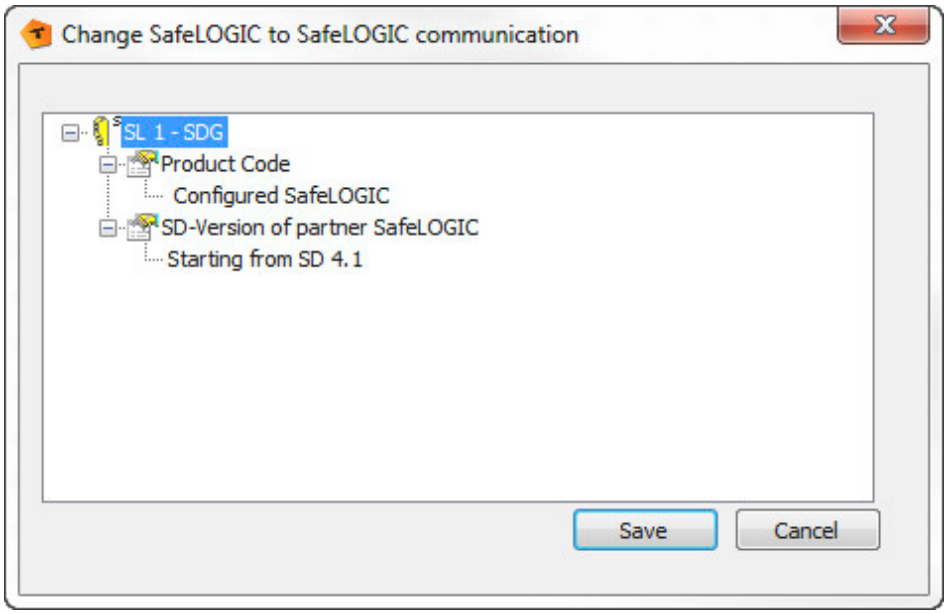
To help with this, a SafeLOGIC controller provides a Safety Domain Gateway (SDG) that can be used to connect additional SafeLOGIC controllers (source controllers). This gateway functionality ensures communication between several safety domains. The connection between source SafeLOGIC controllers and SDG SafeLOGIC controller is indicated in the source SafeLOGIC controller's project as an additional safety module that provides additional communication channels. An SDG SL controller itself can also be used as a source controller and connected to another SDG SL controller. This can be done to achieve cascading communication relationships.

A source SL controller can also be connected several times to the same SDG SL controller, just as it is possible for the source SL controller to communicate with several SDG SL controllers. This results in several ways for SafeLOGIC to SafeLOGIC communication to take place.

7.3.1 System requirements

The following points must be taken into account for safe data exchange between at least 2 SafeLOGIC controllers:

- SafeDESIGNER <4.1: The same SafeDESIGNER versions must be used.
- SafeDESIGNER 4.1 to 4.2.1: The SafeDESIGNER versions must be within this version range.
- SafeDESIGNER 4.2.2 and later: SafeDESIGNER 3.0 or later is permitted to be used.
  The corresponding parameters in the following dialog box must be configured in order to establish a connection to the remote station.



  - Configured SafeLOGIC: Remote station with which communication takes place (e.g. X20SL8100)
  - SD-Version of partner SafeLOGIC: Version with which the application on the remote station was created

7.3.2 Possibilities

The system supports various communication options. The corresponding communication type is defined via parameters in Automation Studio (see "Group: SafeLOGIC to SafeLOGIC communication").

Fixed communication

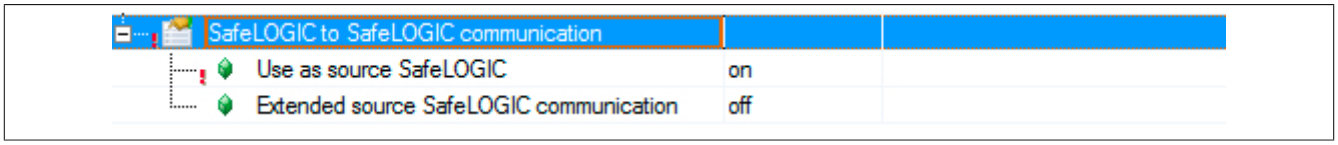
- 8 BOOL channels (1 byte) per communication direction
- One source SL controller can only communicate with one SDG SL controller
- No "any to any" constellation
- Cannot be used with SafeLOGIC-X

Extended communication (Release 1.4 or later and Automation Studio 3.0.90 or later)

- Freely configurable communication channels
- Limited to 16 channels (where 8 BOOLs count as 1 channel; other data types are calculated 1:1).
- One source SL controller can communicate with several SDG SL controllers
- "Any to any" constellation possible

7.3.3 Configuration in Automation Studio

To use SafeLOGIC to SafeLOGIC communication, a SafeLOGIC controller first needs to be configured as a source SL controller. This is done in the I/O configuration.

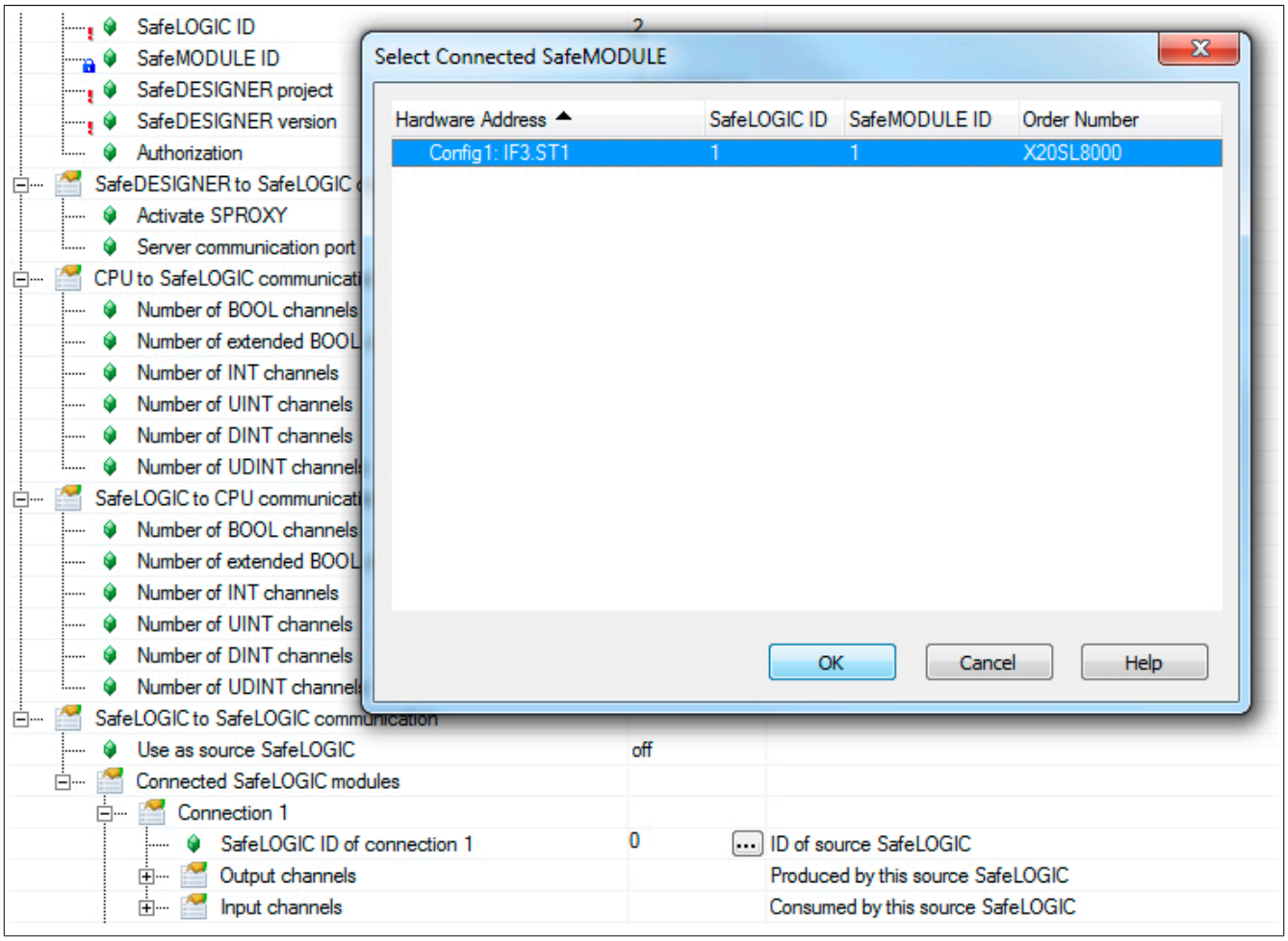


After the "Use as source SafeLOGIC" parameter has been enabled, it is possible to define the type of SafeLOGIC to SafeLOGIC communication as fixed or extended. If the "Extended source SafeLOGIC communication" parameter is not enabled, then fixed communication is used.

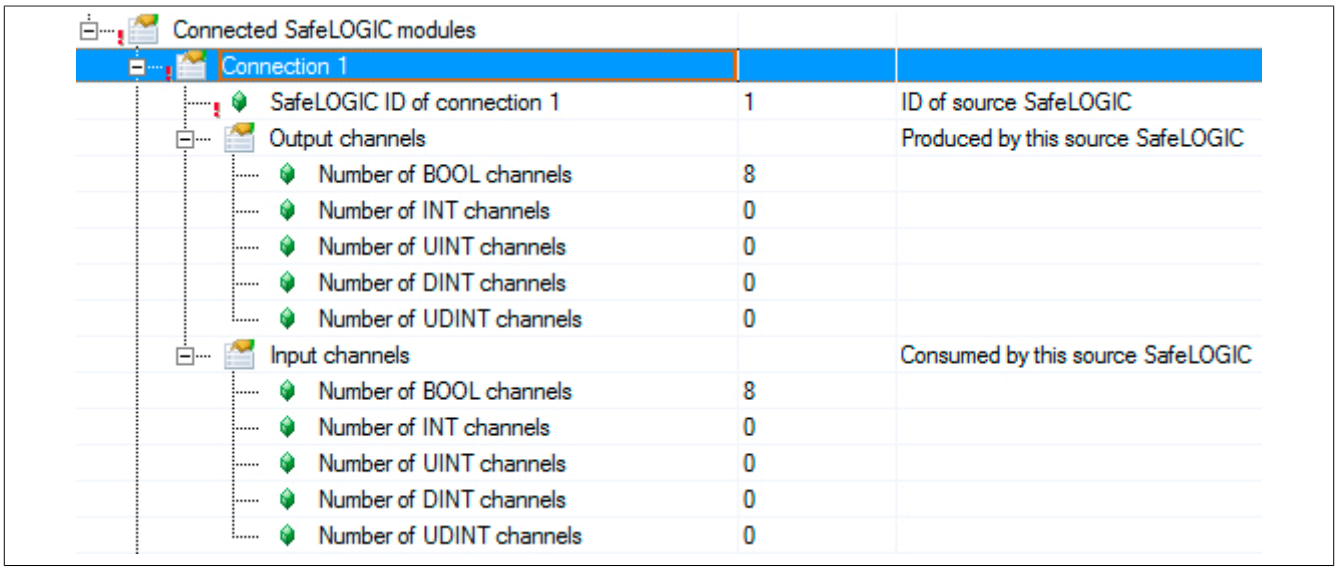
Information:

Changing the type of communication (fixed or extended) at a later time may result in channel overlaps in SafeDESIGNER; the communication channels must therefore be reconnected.

The source SL controller is then connected to the SDG SL controller in the next step. This is done using the connection points in Automation Studio under the I/O configuration of a SafeLOGIC controller (X20SL80x1 and X20SL81xx). Each SafeLOGIC ID (safety domain) is specified from the connection sections using the wizard in Automation Studio.



The necessary communication channels must be defined under each connection. With fixed communication, they are limited to 8 BOOL channels in each direction.



If SafeLOGIC to SafeLOGIC communication should be established between existing or separate Automation Studio projects, several things must be taken into consideration:

- SafeLOGIC IDs must be unique.
- A dummy configuration that includes all safety components must be created on the peer station.
- The dummy configuration must match the real configuration - the SafeMODULE IDs are important here.
- If the projects have multiple iCNs (intelligent controlled nodes), all iCNs must always be taken into account in the iCN project.

7.3.4 Display in SafeDESIGNER

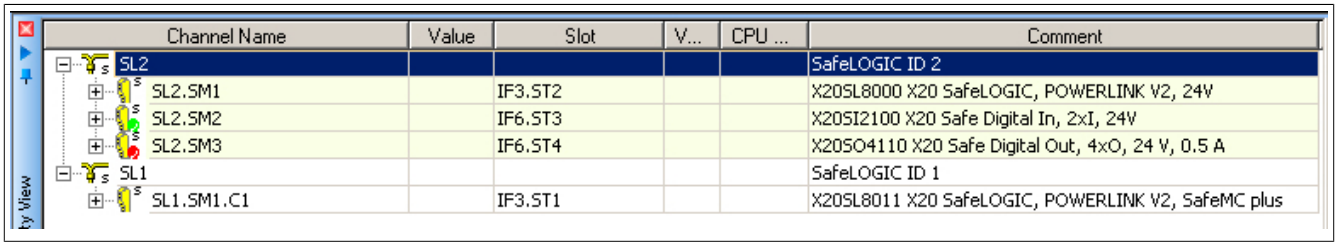
The communication channels are also shown in the SafeDESIGNER project for the respective SafeLOGIC controller (source or SDG).

Danger!

All of the communication channels being used in the project must be mapped in both SafeDESIGNER projects using the same variable names. Channels and variable names are used to calculate a checksum that is then checked at runtime. If the checksum does not match, then the system issues a corresponding logger message in the Safety Logger and communication does not take place.

7.3.4.1 SafeDESIGNER project – Source SL controller

In the source SL controller's SafeDESIGNER project, communication is indicated by an additional module. This module has its own node that represents the connection to this safety domain.

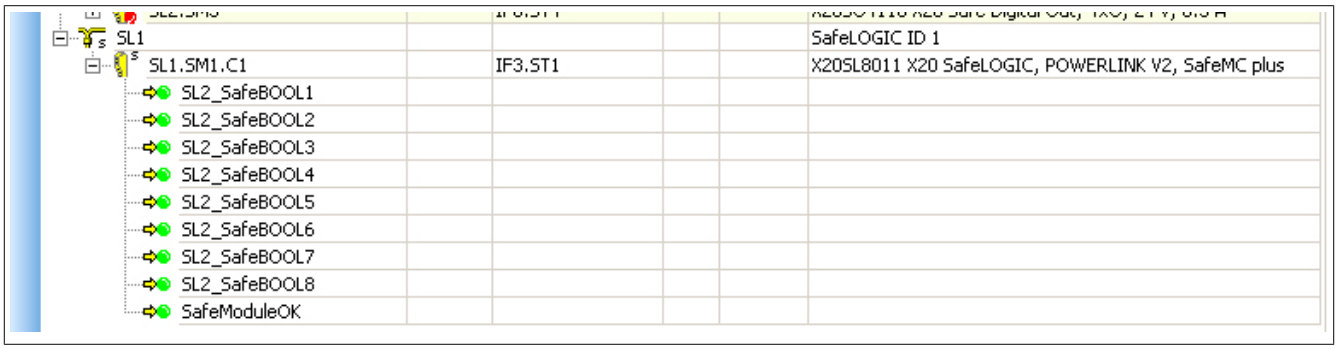


Channel Name	Value	Slot	V...	CPU ...	Comment
SL2					SafeLOGIC ID 2
SL2.SM1		IF3.ST2			X20SL8000 X20 SafeLOGIC, POWERLINK V2, 24V
SL2.SM2		IF6.ST3			X20SI2100 X20 Safe Digital In, 2xI, 24V
SL2.SM3		IF6.ST4			X20SO4110 X20 Safe Digital Out, 4xO, 24 V, 0.5 A
SL1					SafeLOGIC ID 1
SL1.SM1.C1		IF3.ST1	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

If this module is selected, it is possible to configure its safety-related parameters (see section "Parameters for connection - Release 1.10 and later").

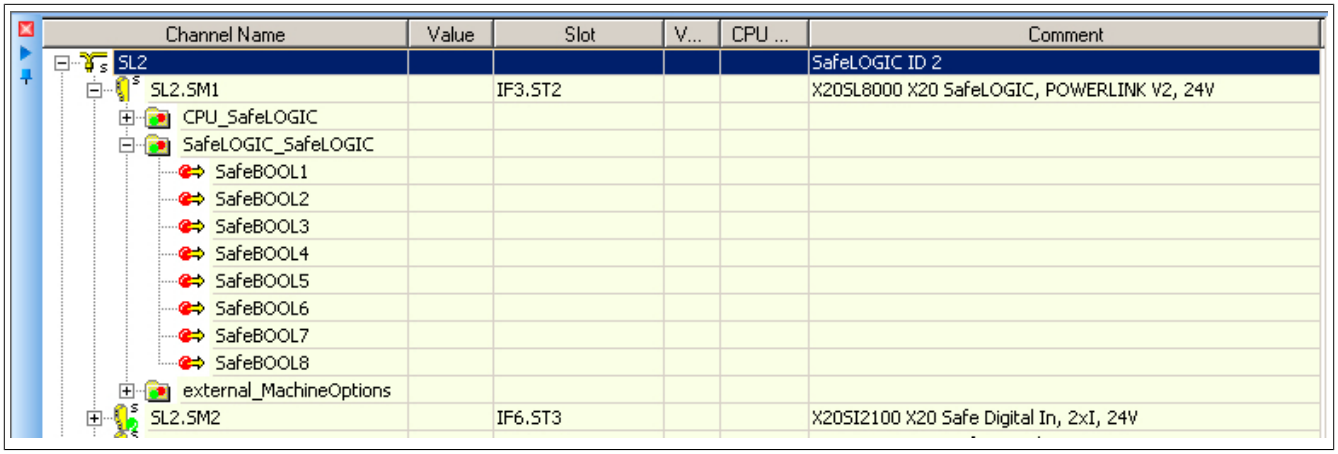
Fixed communication

The input channels sent from the SDG SL controller to the source SL controller and bit information about the status of the connection are listed under the module.



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			

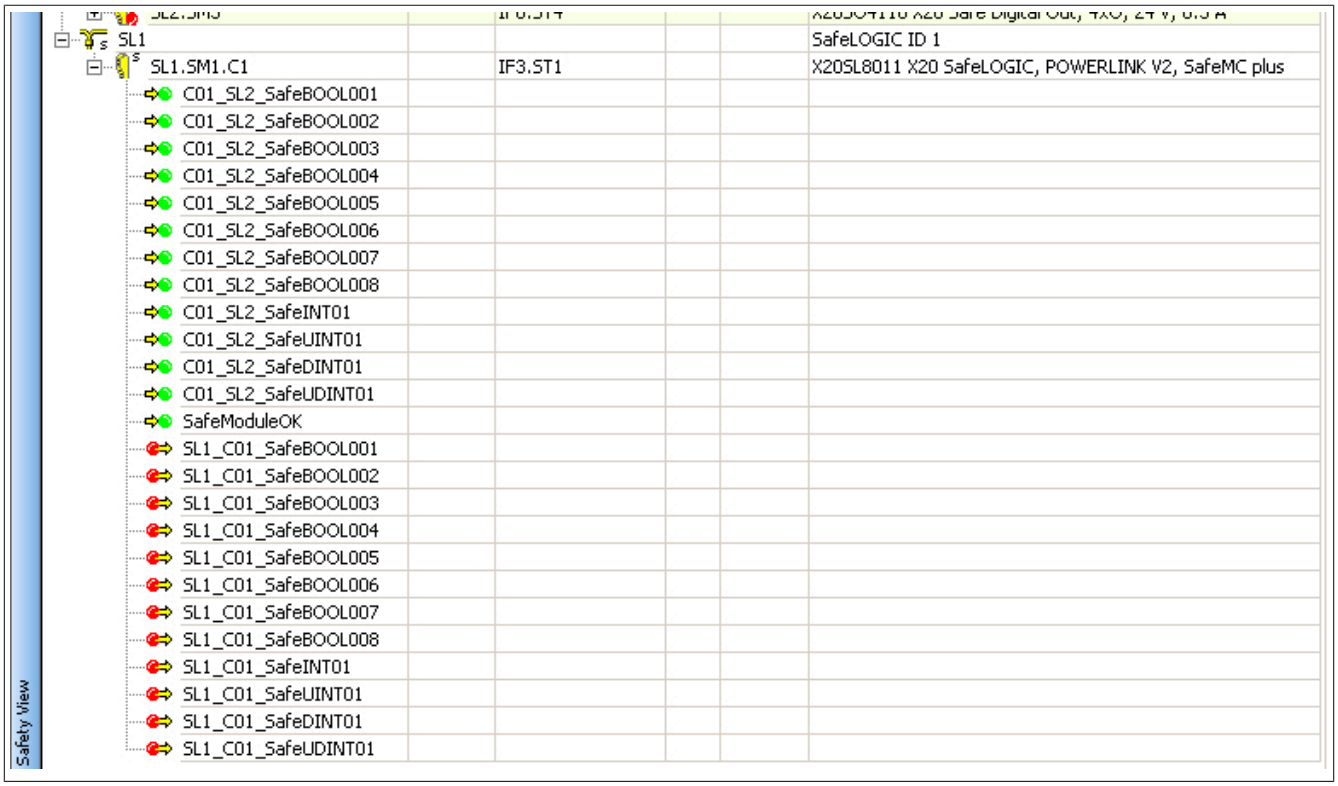
The output channels sent from the source SL controller to the SDG SL controller are listed under the actual SL controller in the project in section "SafeLOGIC_SafeLOGIC".



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

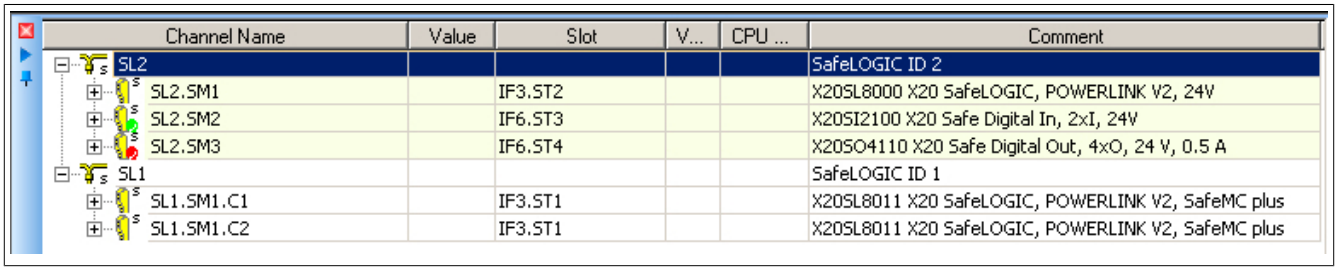
Extended communication

The input channels, output channels and bit information regarding the status of the connection are listed under the module.

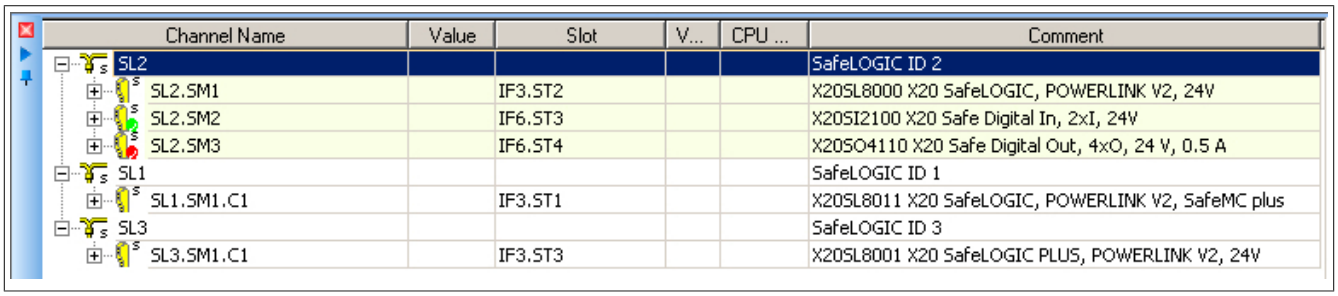


Additional connection

If the source SL controller should be connected once again to the same SDG SL controller, an additional module underneath the same node is available with the necessary parameters and communication channels.

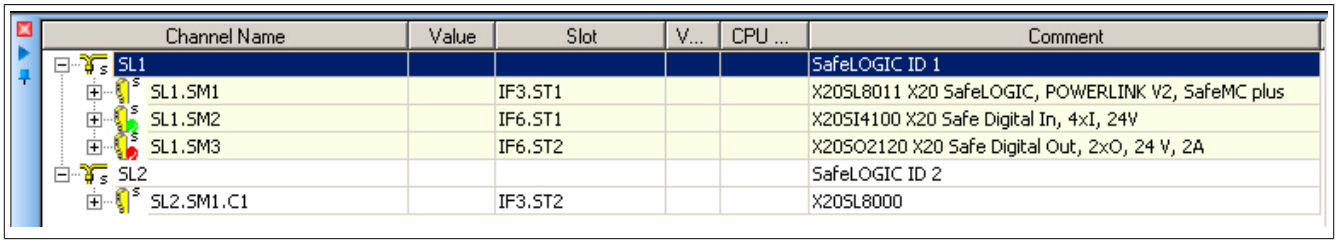


If the source SL controller should be connected to another SDG SL controller, an additional node for the safety domain as well as a module with the necessary parameters and communication channels is available.



7.3.4.2 SafeDESIGNER project – SDG SL controller

In the SDG SL controller's SafeDESIGNER project, communication is indicated by an additional module. This module has its own node that represents the connection to this safety domain.



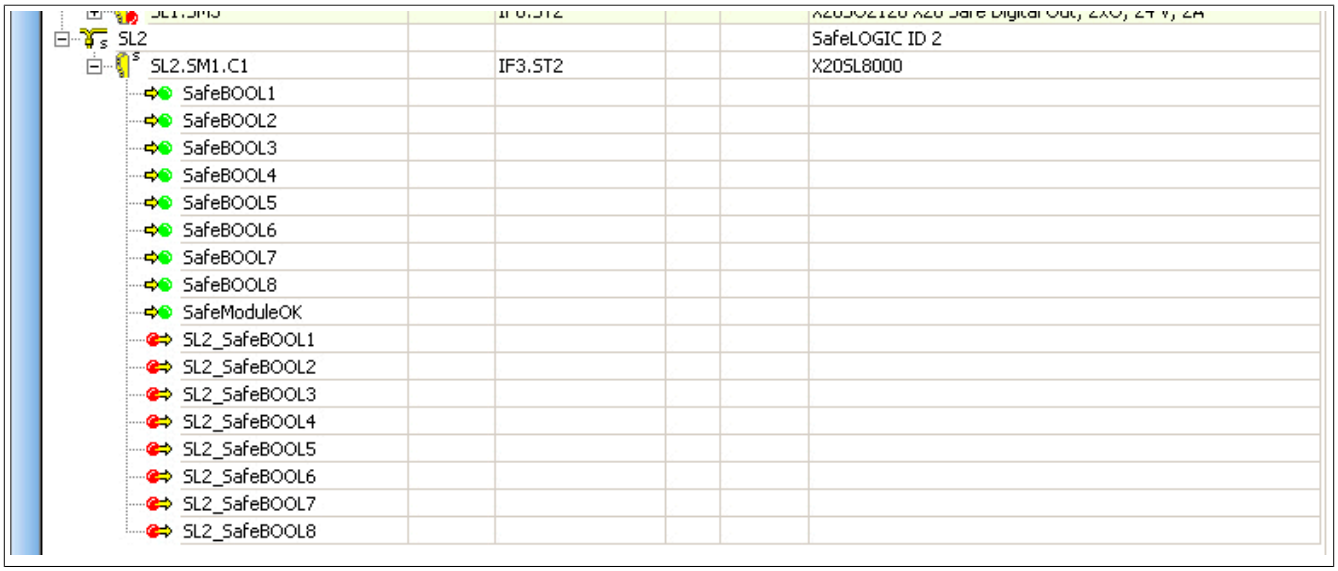
Channel Name	Value	Slot	V...	CPU ...	Comment
SL1					SafeLOGIC ID 1
SL1.SM1		IF3.ST1			X20SL8011 X20 SafeLOGIC, POWERLINK V2, SafeMC plus
SL1.SM2		IF6.ST1			X20SI4100 X20 Safe Digital In, 4xI, 24V
SL1.SM3		IF6.ST2			X20SO2120 X20 Safe Digital Out, 2xO, 24 V, 2A
SL2					SafeLOGIC ID 2
SL2.SM1.C1		IF3.ST2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

Information:

No connection parameters are available in the SDG SL controller's project. They must be configured in the source SL controller's project.

Fixed communication

The input channels, output channels and bit information regarding the status of the connection are listed under the module.



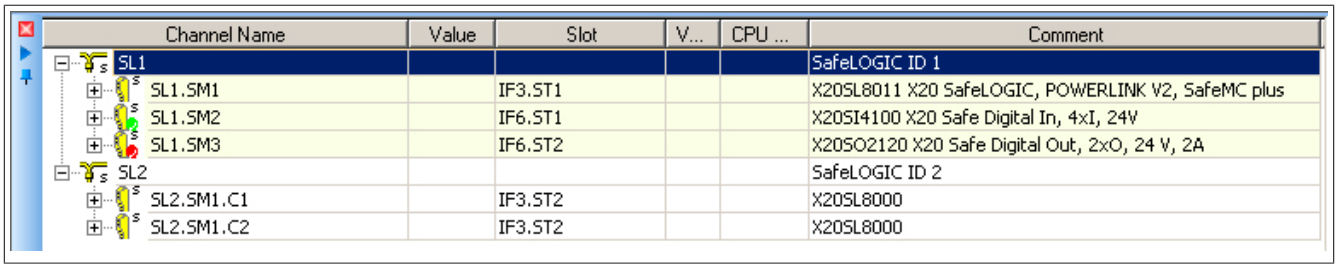
SL2					SafeLOGIC ID 2
SL2.SM1.C1		IF3.ST2			X20SL8000
SafeBOOL1					
SafeBOOL2					
SafeBOOL3					
SafeBOOL4					
SafeBOOL5					
SafeBOOL6					
SafeBOOL7					
SafeBOOL8					
SafeModuleOK					
SL2_SafeBOOL1					
SL2_SafeBOOL2					
SL2_SafeBOOL3					
SL2_SafeBOOL4					
SL2_SafeBOOL5					
SL2_SafeBOOL6					
SL2_SafeBOOL7					
SL2_SafeBOOL8					

Extended communication

The input channels, output channels and bit information regarding the status of the connection are listed under the module.

Additional connection

If the source SL controller should be connected once again to the SDG SL controller, an additional module underneath the same node is available with the necessary communication channels.



7.3.5 Parameters for connection - up to Release 1.9

Safety Release 1.4 or higher:

Cycle time parameters are also available for communication in order to define the "Worst_Case_Response_Time_us". As with communication that takes place with other safety modules, this is a timeout value that elapses whenever an error occurs (e.g. lost network connection).

Information:

Since SafeLOGIC to SafeLOGIC communication is represented as an additional safety module to the source SafeLOGIC controller, the parameters for the connection are available and must be configured in the source SL controller's project.

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

Group: Basic

<table>
<tr><th>Parameter</th><th>Description</th><th>Default value</th><th>Unit</th></tr>
<tr><td>Min_required_FW_Rev</td><td>This parameter is reserved for future functional expansions.</td><td>Basic Release</td><td>-</td></tr>
<tr><td>Optional</td><td>This parameter can be used to configure the module as "optional". Optional modules do not have to be present, i.e. the SafeLOGIC controller will not indicate that these modules are not present. However, this parameter does not influence the module's signal or status data.</td><td>No</td><td>-</td></tr>
<tr><td></td><td colspan="3"><table>
<tr><th>Parameter value</th><th>Description</th></tr>
<tr><td>No</td><td>This module is mandatory for the application.

The module must be in OPERATIONAL mode after startup, and safe communication to the SafeLOGIC controller must be established without errors (SafeModuleOK = SAFETRUE). Processing of the safety application on the SafeLOGIC controller is delayed after startup until this state is achieved for all modules with "Optional = No".

After startup, module problems are indicated by a quickly blinking "MXCHG" LED on the SafeLOGIC controller. An entry is also made in the logbook.</td></tr>
<tr><td>Yes</td><td>The module is not required for the application.

The module is not taken into account during startup, which means the safety application is started regardless of whether the modules with "Optional = Yes" are in OPERATIONAL mode or if safe communication is properly established between these modules and the SafeLOGIC controller.

After startup, module problems are NOT indicated by a quickly blinking "MXCHG" LED on the SafeLOGIC controller. An entry is NOT made in the logbook.</td></tr>
<tr><td>Startup</td><td>This module is optional. The system determines how the module will proceed during startup.

If it is determined that the module is physically present during startup (regardless of whether it is in OPERATIONAL mode or not), then the module behaves as if "Optional = No" is set.

If it is determined that the module is not physically present during startup, then the module behaves as if "Optional = Yes" is set.</td></tr>
<tr><td>Not_Present
(Release 1.9 and later)</td><td>The module is not required for the application.

The module is ignored during startup, which means the safety application is started regardless of whether the modules with "Optional = Not_Present" are physically present.

Unlike when "Optional = Yes" is configured, the module is not started with "Optional = Not_Present", which optimizes system startup behavior.

After startup, module problems are NOT indicated by a quickly blinking "MXCHG" LED on the SafeLOGIC controller. An entry is NOT made in the logbook.</td></tr>
</table></td></tr>
<tr><td>External_UDID</td><td>This parameter enables the option on the module for the expected UDID to be specified externally by the CPU.</td><td>No</td><td>-</td></tr>
<tr><td></td><td colspan="3"><table>
<tr><th>Parameter value</th><th>Description</th></tr>
<tr><td>Yes-ATTENTION</td><td>The UDID is determined by the CPU. The SafeLOGIC controller must be restarted if the UDID is changed.</td></tr>
<tr><td>No</td><td>The UDID is specified by a teach-in procedure during startup.</td></tr>
</table></td></tr>
</table>

Table 32: SafeDESIGNER parameters: Basic

Danger!

If function "External_UDID = Yes-ATTENTION" is used, incorrect specifications from the CPU can lead to safety-critical situations.
Perform an FMEA (Failure Mode and Effects Analysis) in order to detect these situations and implement additional safety measures to handle them.

Group: Safety_Response_Time

Parameter	Description	Default value	Unit
Synchronous_Network_Only	This parameter describes the synchronization characteristics of the network being used. They are defined in Automation Studio / Automation Runtime.	Yes	-
	Parameter value / **Description** Yes: In order to calculate the safety response time, networks must be synchronous and their cycle times must either be the same or an integer ratio of the cycle times. No: No requirement for synchronization of the networks.		
Max_SDG_Powerlink_CycleTime_us	This parameter specifies the maximum cycle time of the POWERLINK network in which the other SafeLOGIC controller is operated. • Permissible values: 200 to 30,000 µs (corresponds to 0.2 to 30 ms)	5000	µs
Max_Powerlink_CycleTime_us	This parameter specifies the maximum POWERLINK cycle time used to calculate the safety response time. • Permissible values: 200 to 30,000 µs (corresponds to 0.2 to 30 ms)	5000	µs
Max_CPU_CrossLinkTask_CycleTime_us	This parameter specifies the maximum cycle time for copying data between the two POWERLINK networks. The value 0 means that both SafeLOGIC controllers are in the same POWERLINK network. • Permissible values: 0 to 3,000,000 µs (corresponds to 0 to 3 s)	5000	µs
Min_SDG_Powerlink_CycleTime_us	This parameter specifies the minimum cycle time of the POWERLINK network in which the other SafeLOGIC controller is operated. • Permissible values: 200 to 30,000 µs (corresponds to 0.2 to 30 ms)	200	µs
Min_Powerlink_CycleTime_us	This parameter specifies the minimum POWERLINK cycle time used to calculate the safety response time. • Permissible values: 200 to 30,000 µs (corresponds to 0.2 to 30 ms)	200	µs
Min_CPU_CrossLinkTask_CycleTime_us	This parameter specifies the minimum cycle time for copying data between the two POWERLINK networks. The value 0 means that both SafeLOGIC controllers are in the same POWERLINK network. • Permissible values: 0 to 3,000,000 µs (corresponds to 0 to 3 s)	0	µs
Worst_Case_Response_Time_us	This parameter specifies the limit value for monitoring the safety response time. • Permissible values: 3000 to 12,500,000 µs (corresponds to 3 ms to 12.5 s) **Note:** Keep parameter "Slow_Connection" in mind when entering large values here!	100000	µs
Node_Guarding_Lifetime	This parameter specifies the maximum number of attempts to be made during the time set with parameter "Node_Guarding_Timeout_s". The purpose of these attempts is to ensure that the module is available. • Permissible values: 1 to 255 **Note** • The larger the configured value, the greater the amount of asynchronous data traffic. • This setting is not critical to safety functionality. The time for safely cutting off actuators is determined independently using parameter "Worst_Case_Response_Time_us".	5	-
Max_SDG_Cycle_Time_us	This parameter specifies the maximum cycle time of the other SafeLOGIC controller used to calculate the safety response time. • Permissible values: 800 to 20,000 µs (corresponds to 0.8 to 20 ms)	5000	µs
Min_SDG_Cycle_Time_us	This parameter specifies the minimum cycle time of the other SafeLOGIC controller used to calculate the safety response time. • Permissible values: 800 to 20,000 µs (corresponds to 0.8 to 20 ms)	1600	µs
Slow_Connection	This parameter specifies whether this connection is a slow connection.	No	-
	Parameter value / **Description** Yes: This is a connection with a large ratio between the SafeLOGIC cycle time and the telegram runtime (affects the parameter calculation internally). Rule of thumb: "Yes" from ratio 50:1 (telegram runtime: SafeLOGIC cycle time) No: Default connection, parameter calculation unchanged		

Table 33: SafeDESIGNER parameters: Safety_Response_Time

Information:

Parameter "CPU_CrossLinkTask_CycleTime_us" is needed if the source SL and SDG SL controllers are in different networks or located on different controllers. If this is not the case, the minimum and maximum value must be set to "0".
For this parameter, the entire connection distance between the controllers must be taken into account – including copy times between the interfaces involved.

Information:

Parameter "Slow_Connection" can also be used to specify that the connection between the source SL and SDG SL controllers is slow. If a value of just a few seconds is needed for the connection timeout, then this parameter must be enabled ("Slow_Connection = Yes").

7.3.6 Parameters for connection - Release 1.10 and later

Cycle time parameters are also available for communication in order to define the maximum data transmission time. As with communication that takes place with other safety modules, this is a timeout value that elapses whenever an error occurs (e.g. lost network connection).

Information:

Since SafeLOGIC to SafeLOGIC communication is represented as an additional safety module to the source SafeLOGIC controller, the parameters for the connection are available and must be configured in the source SL controller's project.

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

Group: Basic

<table>
<tr><th>Parameter</th><th>Description</th><th>Default value</th><th>Unit</th></tr>
<tr><td>Min required FW Rev</td><td>This parameter is reserved for future functional expansions.</td><td>Basic Release</td><td>-</td></tr>
<tr><td>Optional</td><td>This parameter can be used to configure the module as "optional". Optional modules do not have to be present, i.e. the SafeLOGIC controller will not indicate that these modules are not present. However, this parameter does not influence the module's signal or status data.</td><td>No</td><td>-</td></tr>
<tr><td></td><td colspan="3"><table>
<tr><th>Parameter value</th><th>Description</th></tr>
<tr><td>No</td><td>This module is absolutely necessary for the application.

The module must be in OPERATIONAL mode after startup, and safe communication to the SafeLOGIC controller must be established without errors (SafeModuleOK = SAFETRUE). Processing of the safety application on the SafeLOGIC controller is delayed after startup until this state is achieved for all modules with "Optional = No".

After startup, module problems are indicated by a quickly blinking "MXCHG" LED on the SafeLOGIC controller. An entry is also made in the logbook.</td></tr>
<tr><td>Yes</td><td>This module is not necessary for the application.

The module is not taken into account during startup, which means the safety application is started regardless of whether the modules with "Optional = Yes" are in OPERATIONAL mode or if safe communication is properly established between these modules and the SafeLOGIC controller.

After startup, module problems are NOT indicated by a quickly blinking "MXCHG" LED on the SafeLOGIC controller. An entry is NOT made in the logbook.</td></tr>
<tr><td>Startup</td><td>This module is optional. The system determines how the module will proceed during startup.

If it is determined that the module is physically present during startup (regardless of whether it is in OPERATIONAL mode or not), then the module behaves as if "Optional = No" is set.

If it is determined that the module is not physically present during startup, then the module behaves as if "Optional = Yes" is set.</td></tr>
<tr><td>NotPresent</td><td>This module is not necessary for the application.

The module is ignored during startup, which means the safety application is started regardless of whether the modules with "Optional = NotPresent" are physically present.

Unlike when "Optional = Yes" is configured, the module is not started with "Optional = NotPresent", which optimizes system startup behavior.

After startup, module problems are NOT indicated by a quickly blinking "MXCHG" LED on the SafeLOGIC controller. An entry is NOT made in the logbook.</td></tr>
</table></td></tr>
<tr><td>External UDID</td><td>This parameter enables the option on the module for the expected UDID to be specified externally by the CPU.</td><td>No</td><td>-</td></tr>
<tr><td></td><td colspan="3"><table>
<tr><th>Parameter value</th><th>Description</th></tr>
<tr><td>Yes-ATTENTION</td><td>The UDID is determined by the CPU. The SafeLOGIC controller must be restarted if the UDID is changed.</td></tr>
<tr><td>No</td><td>The UDID is specified by a teach-in procedure during startup.</td></tr>
</table></td></tr>
</table>

Table 34: SafeDESIGNER parameters: Basic

Danger!

If function "External UDID = Yes-ATTENTION" is used, incorrect specifications from the CPU can lead to safety-critical situations.
Perform an FMEA (Failure Mode and Effects Analysis) in order to detect these situations and implement additional safety measures to handle them.

Group: Safety Response Time

Parameter	Description	Default value	Unit
Safe Data Duration	This parameter specifies the maximum permitted data transmission time between the SafeLOGIC controller and SafeIO module. For more information about the actual data transmission time, see section Diagnostics and service → Diagnostics tools → Network analyzer → Editor → Calculation of safety runtime of Automation Help. The cycle time of the safety application must also be added. • Permissible values: 2000 to 10,000,000 µs (corresponds to 2 ms to 10 s)	20000	µs
Additional Tolerated Packet Loss	This parameter specifies the number of additional tolerated lost packets during data transfer. • Permissible values: 0 to 10	0	Packets
Slow Connection	This parameter specifies whether this connection is classified as a slow connection.	No	-
Packets per Node Guarding	This parameter specifies the maximum number of packets used for node guarding. • Permissible values: 1 to 255 **Note** • The larger the configured value, the greater the amount of asynchronous data traffic. • This setting is not critical to safety functionality. The time for safely cutting off actuators is determined independently of this.	5	Packets
Max SDG Cycletime	This parameter specifies the maximum cycle time of the other SafeLOGIC controller used to calculate the safety response time. • Permissible values: 800 to 20,000 µs (corresponds to 0.8 to 20 ms)	5000	µs
Min SDG Cycletime	This parameter specifies the minimum cycle time of the other SafeLOGIC controller used to calculate the safety response time. • Permissible values: 800 to 20,000 µs (corresponds to 0.8 to 20 ms)	1600	µs

Parameter value	Description
Yes	This is a connection with a large ratio between the SafeLOGIC cycle time and the telegram runtime (affects the parameter calculation internally). Rule of thumb: "Yes" from ratio 50:1 (telegram runtime: SafeLOGIC cycle time)
No	Default connection, parameter calculation unchanged

Table 35: SafeDESIGNER parameters: Safety Response Time

Information:

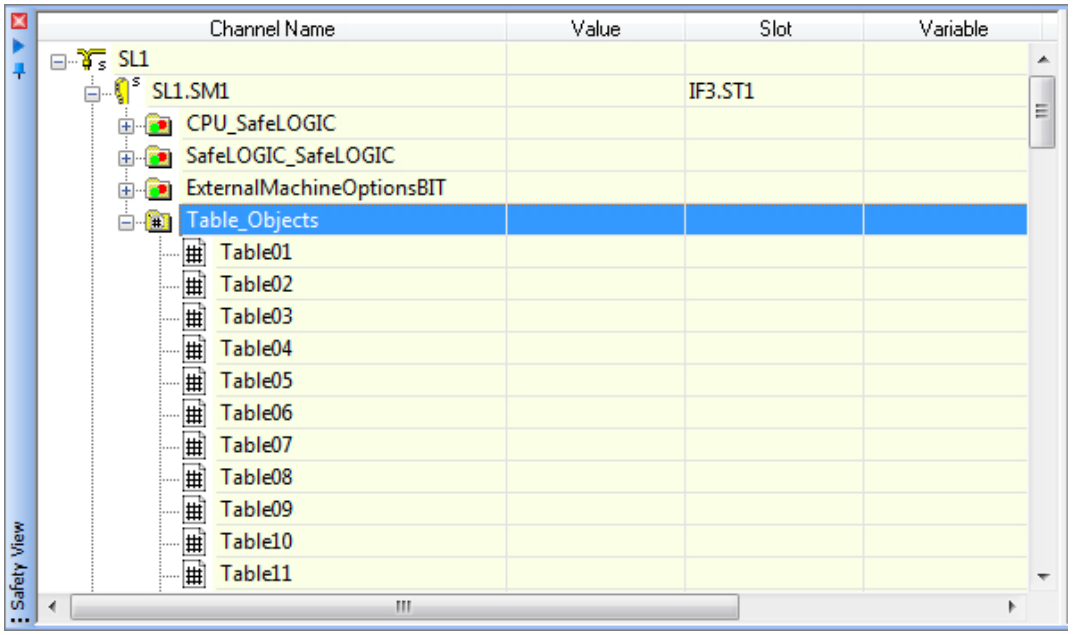
Parameter "Slow Connection" can also be used to specify that the connection between the source SL and SDG SL controllers is slow. If a value of just a few seconds is needed for the connection timeout, then this parameter must be enabled ("Slow Connection = Yes").

7.4 Table objects

A table object is a CSV file with a certain structure and certain data. Up to 99 table objects are available in SafeDESIGNER under the SafeLOGIC controller. Each object represents the connection to a CSV file with the corresponding data. In addition, SafeDESIGNER contains library "Table_SF" for evaluating the various table objects. The function blocks of this library must be linked to a table object.

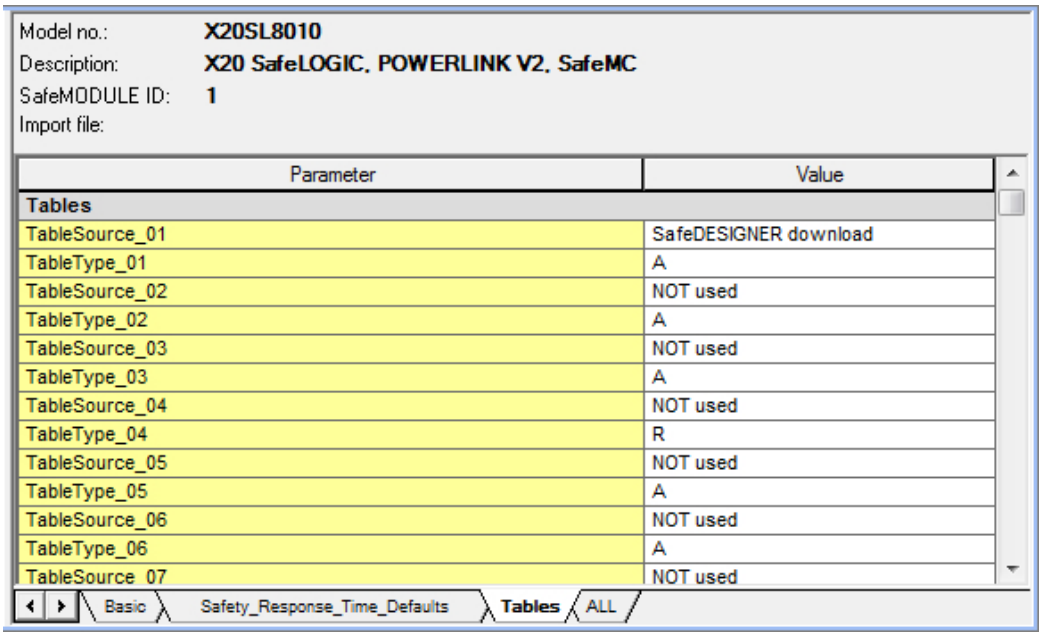
Information:

The validation and lock functions implemented in SafeDESIGNER, together with the validation of the table data by the user, allow the use of commercial off-the-shelf (COTS) editors for table data.



The necessary settings for these table objects can be controlled using SafeLOGIC controller parameters. There is a tab called "Tables" available for this. The following settings can then be made for each table object:

- TableSource → Where the table data is coming from
  - NOT used → Table object not used
  - SafeDESIGNER download → Data transferred with the application
  - Remote download → Data not transferred with the application. It must be transferred subsequently using the AsSafety library.
- TableType → The type of table
  - A - Q
  - R - Z → Table types for SafeROBOTIC



Information:

For details about the structure of the table objects or data, see the help documentation of the function block to be used.

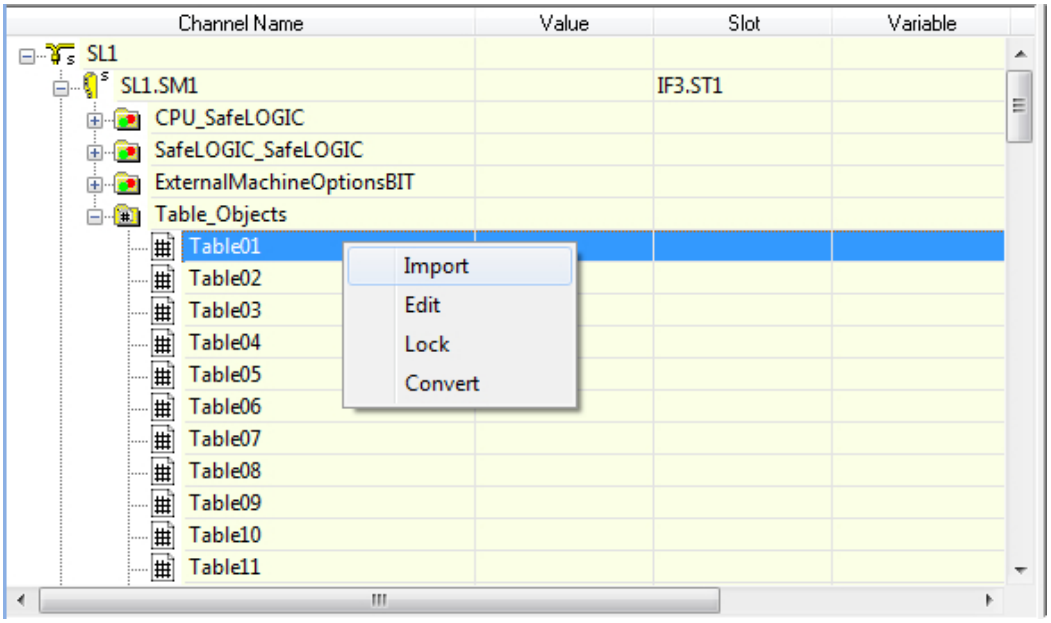
7.4.1 Procedure

To start, each table object must be assigned the proper type and source.

Information:

If a table object is being used in the application but parameter "TableSource" is set to "NOT used", then an error message will be generated when the project is compiled.

Several different actions can be carried out from the table object's shortcut menu (right-click on the table object).



7.4.1.1 Import

This menu item can be used to import an existing CSV file with corresponding data suitable to the selected table type.

Information:

If a file that does not match the table type is imported, then an error message will be generated when the project is compiled.

7.4.1.2 Edit

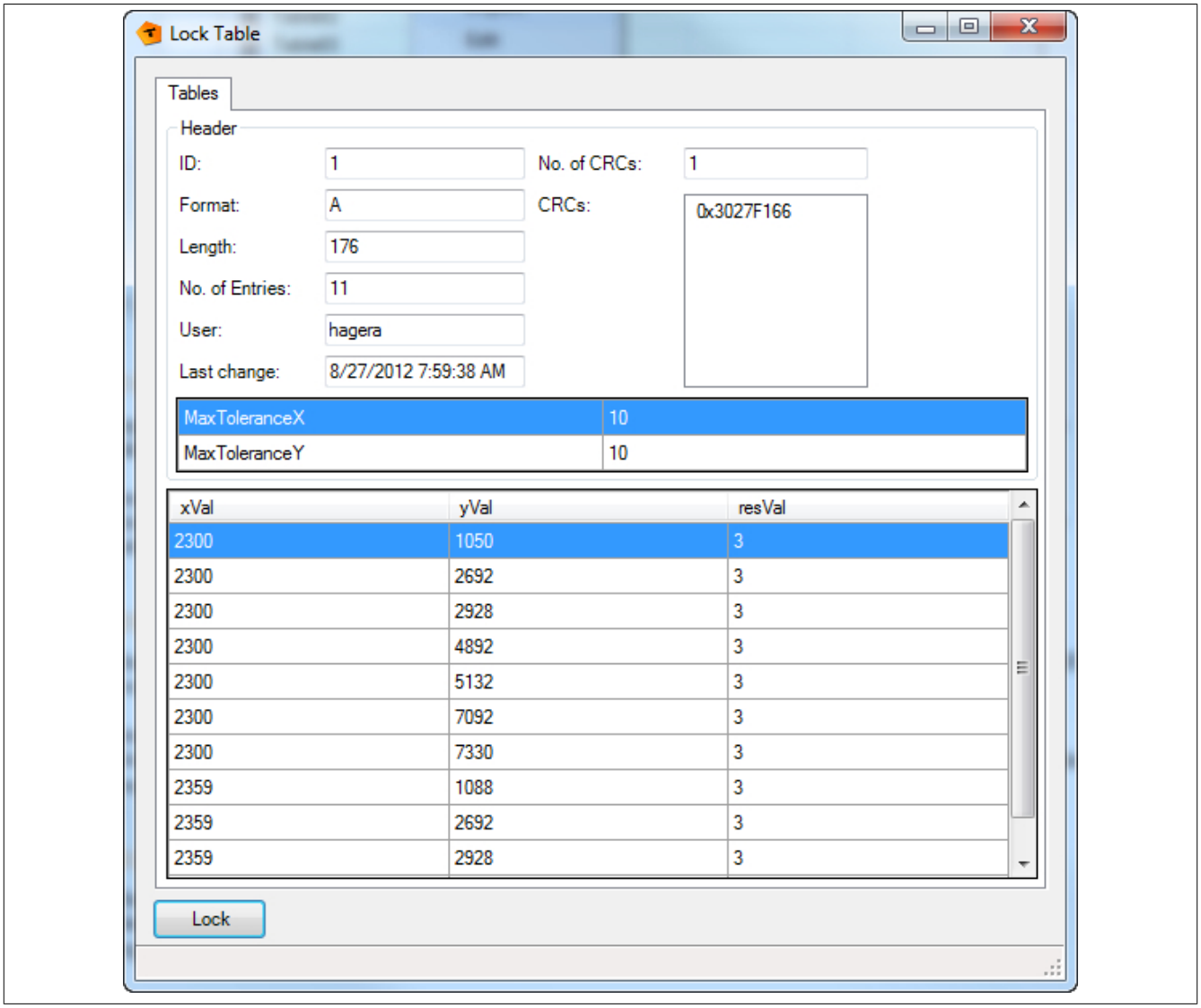
This menu item allows the file to be edited using the default program for CSV files (e.g. MS Excel).

Information:

If a file is being edited, it is required that it is locked again ("Lock" action). Otherwise, the file's CRC will be invalid.

7.4.1.3 Lock

This menu item locks the file and calculates a CRC for its current content. The data is also displayed once more in a new window according to the specified table type.

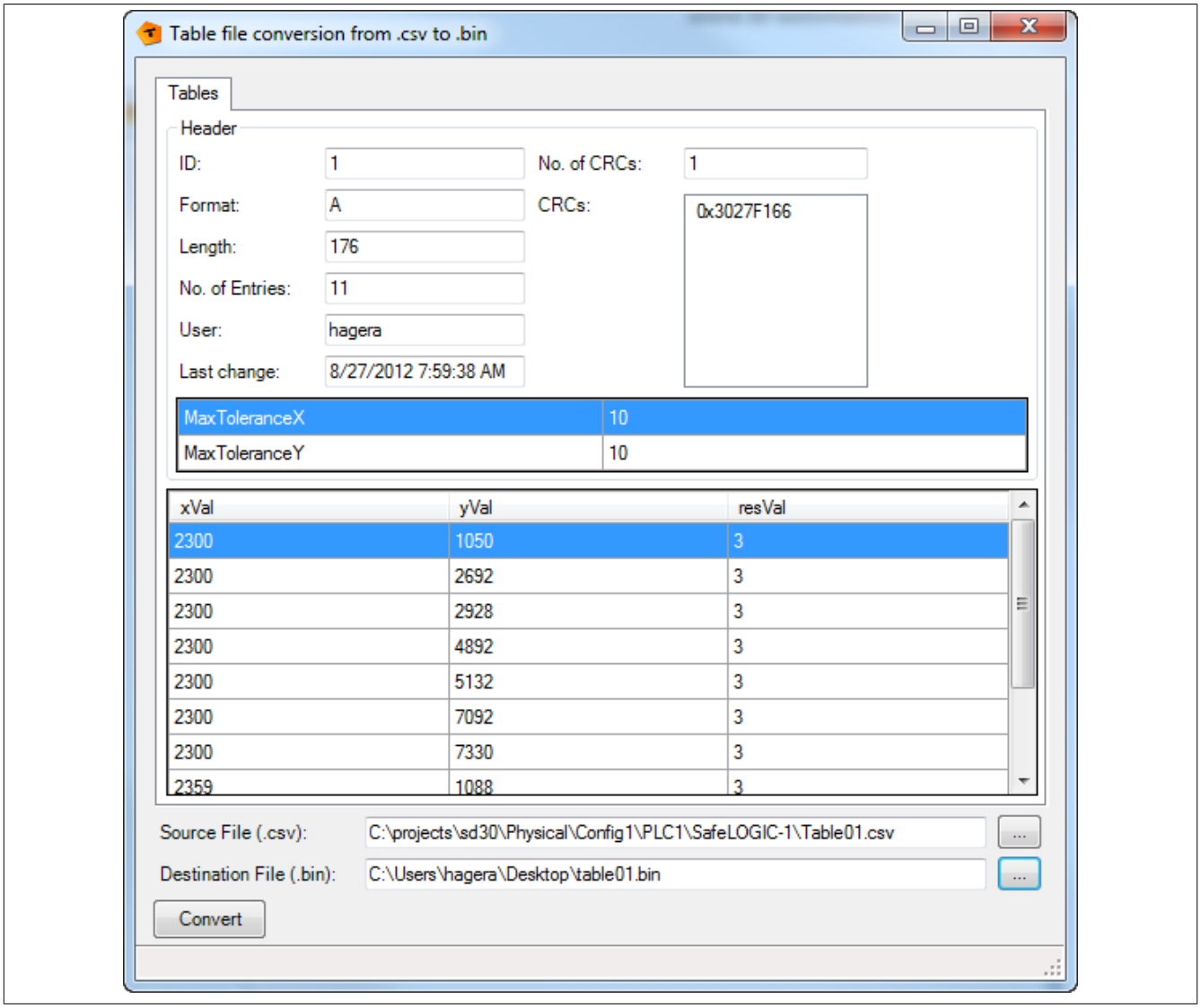


Information:

Error messages will also be displayed in this window if there are any problems with the file (e.g. invalid format, cannot open file, etc.).

7.4.1.4 Convert

This menu item can be used to convert the file to binary format for the SafeLOGIC controller. The path where the binary file is to be saved must be specified.



Information:

This binary file can then be used for downloading via the standard CPU.

7.4.2 Usage in the application

To use table objects, an associated function block must first be used in the application (see library "Table_SF").

Input "S_TableID" must be linked to a table object. This is done in the safety view by selecting the table object and dragging it into the application. It is also possible to provide a meaningful name for the connection.

Information:

An error message will be output during compilation if there are any problems or errors.

7.5 Blackout mode

Blackout mode allows users to continue execution of the application in lower-level subsystems if components of the B&R system fail. In this way, the B&R system – independently of redundancy technology – makes it possible to respond to system-critical situations based on the specific application.

The use of blackout-capable modules is recommended for the following requirements:

- Exit routines on system failure, e.g. to enable the opening of a press if the system fails.
- Stopping or controlled setting of an output on system failure, e.g. to automatically close inflow valves.
- Deceleration sequences on system failure, e.g. to reduce motor speeds before transmitting a stop command.

If blackout-capable modules are configured accordingly, blackout mode will be carried out if the network connection to the higher-level controller or CPU is interrupted.

As soon as the network disturbance has been corrected, blackout mode is stopped by the modules and bumpless synchronization with the network takes place.

Requirements for operation

The following requirements must be met in order to use blackout mode:

- The module being used must support blackout mode.
- Parameter "Blackout mode" must be enabled in Automation Studio.

7.5.1 Areas of use

Through the use of blackout-capable modules, a part of the control system can also remain functional if a disturbance in the network or X2X Link connection between the modules occurs.

7.5.1.1 Loss of POWERLINK connection

Initial situation

Several stations in an application are connected to the CPU via network cables. A fault occurs that interrupts data transfer between the CPU and stations.

Effect

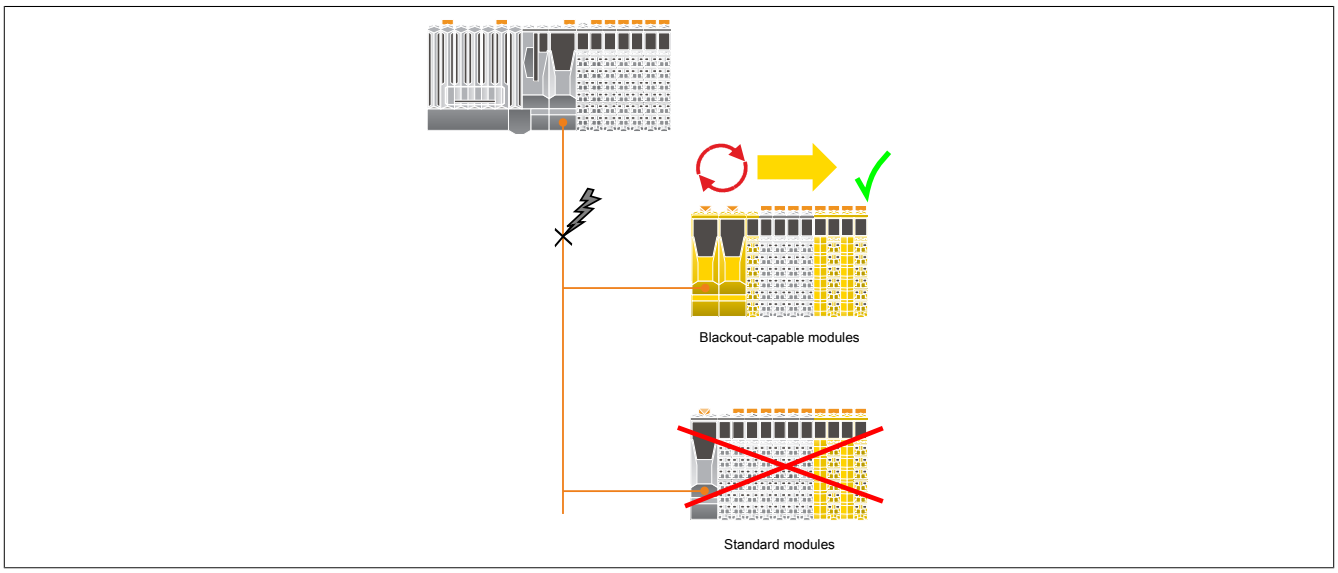
Non-blackout modules are reset and operated according to their default characteristics.

Blackout-capable modules show the following behavior:

- The programmed function continues to be executed.
- Subordinate networks continue to work.
- Data from the CPU is initialized with "0".
- After the disturbance has been corrected, the module bumplessly returns to the higher-level network.

Warning!

Blackout mode causes data from the CPU to be initialized with "0". If blackout mode is used in combination with "output inversion", this can lead to the unwanted setting of outputs.



7.5.1.2 Loss of X2X Link connection

Initial situation

Modules in an application are connected to the network via X2X Link cables. A defect in the X2X Link cable causes the data transfer between the CPU and modules to be interrupted.

Effect

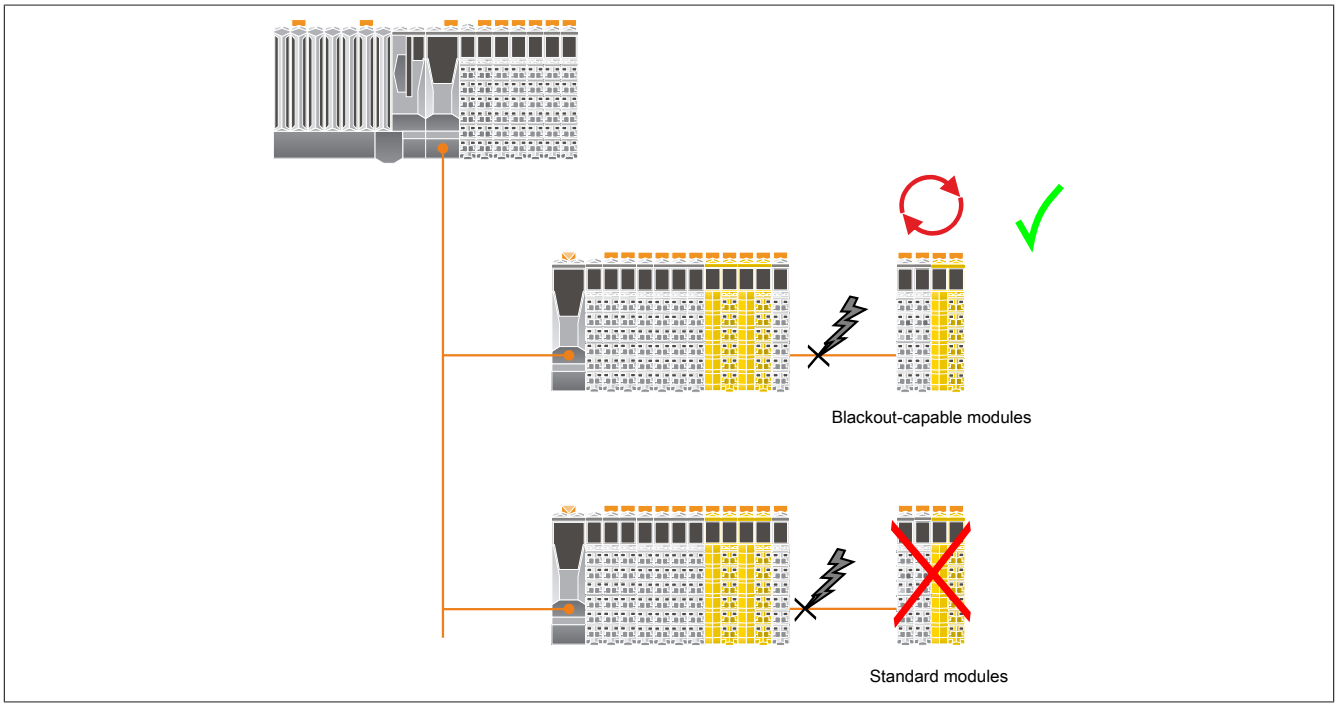
Non-blackout modules are reset and operated according to their default characteristics.

Blackout-capable modules show the following behavior:

- The programmed function continues to be executed.
- Subordinate networks continue to work.
- Data from the CPU is initialized with "0".
- After the disturbance has been corrected, the module bumplessly returns to the higher-level network.

Warning!

Blackout mode causes data from the CPU to be initialized with "0". If blackout mode is used in combination with "output inversion", this can lead to the unwanted setting of outputs.



7.5.2 Programming blackout mode

Blackout mode cannot be detected by the blackout-capable modules themselves. If it is necessary to program specific blackout behavior in an application, an indirect method must therefore be chosen.

One possibility is to implement a counter in the blackout-capable module's higher-level CPU and query it cyclically. Blackout mode would make itself noticeable in this case by a counter value that no longer changes or a counter value of zero.

Blackout-capable modules can be divided into 2 categories:

- **Programmable modules**
  The blackout function is programmed using existing function blocks. In other words, the existing technologies for application programming or reACTION Technology are used.
  The blackout function is executed largely independently of other system components.
- **Standard function modules**
  These modules are not programmable and maintain their default behavior in blackout mode.

7.5.3 Standalone function

The standalone function is an extension of blackout mode. After switching on the power supply, blackout mode is enabled immediately regardless of whether a network connection exists. This means that after switching on the power supply, the module begins executing the most recently saved configuration or application without waiting for activity or synchronization with a higher-level CPU or SafeLOGIC controller.

As soon as the network is active, bumpless synchronization between the module and existing network takes place.

Warning!

Standalone modules act identically to blackout mode on system startup and until the network connection is established. Their use therefore requires extreme caution!

Requirements for operation

The following requirements must be met in order to use the standalone function:

- The module being used must support the standalone function.
- Parameter "Standalone mode" must be enabled in Automation Studio.
- For the standalone function on the bus controller (e.g. X20SL8101), blackout mode is enabled for at least 1 module on the local X2X Link network.
- The module must have been operated with a CPU at least once in order to have a valid configuration.

Information:

The use of the standalone function in connection with DNA is not permitted. Static addresses must be used.

Warning!

The following aspects need to be taken into account in particular:

- **The module must be clearly (and permanently) identified to highlight its distinctive behavior from the standard.**
- **Service technicians must be well-versed with the special characteristics of these modules.**
- **Before connecting the terminal block to a module with an enabled standalone function, at least one of the following conditions must be met:**
  - **It must be ensured that the module is really meant to be operated with the standalone function and the configuration on the module has been checked for correctness.**
  - **The flashing sequence of the module indicates the "normal, network-connected operational state" of the module.**

7.5.3.1 Area of application

Initial situation

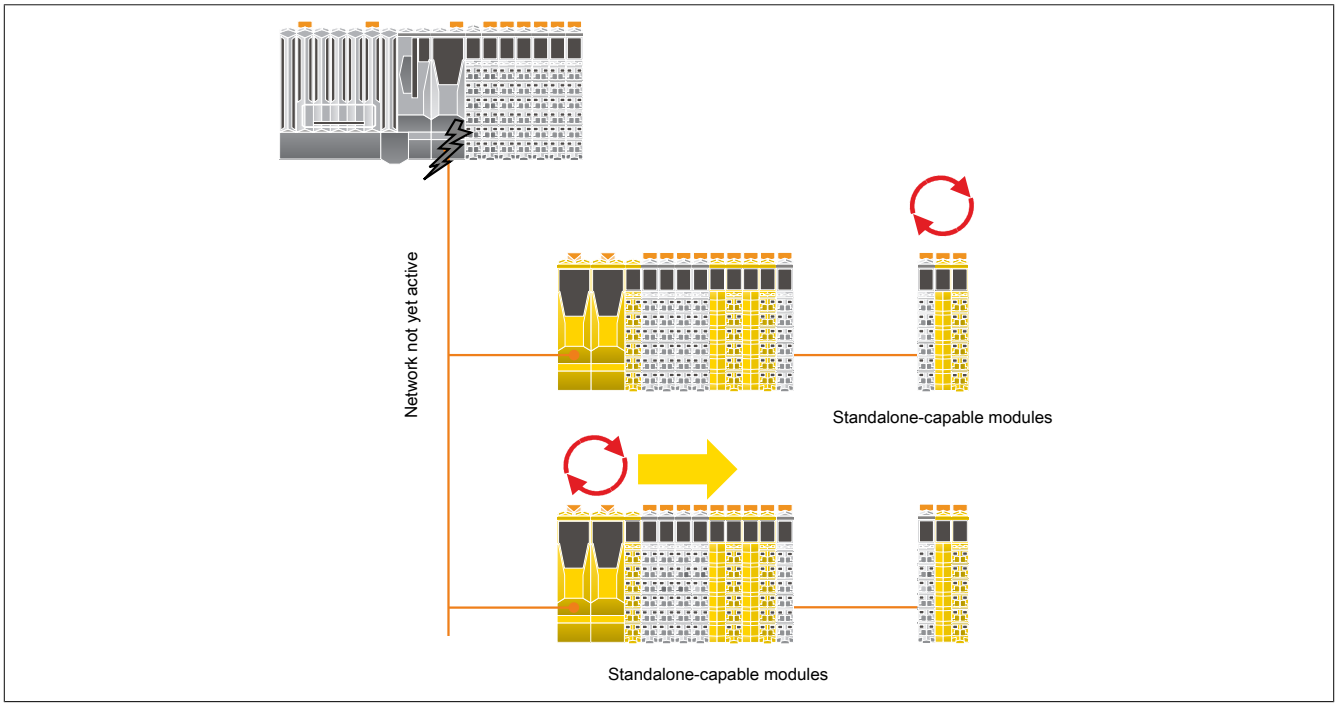
Several stations in an application are connected to the CPU via network cables. After the entire system has been switched off and on, a fault results in the network connection not being established.

Effect

Non-standalone modules are put into the active state only after the application starts up.

Standalone-capable modules show the following behavior:

- The boot procedure is started without waiting on a higher-level network.
- The module behaves identically to blackout mode.
- As soon as the network becomes active, it is bumplessly added to the higher-level network.



7.6 Setup mode

Setup mode supports the user during commissioning.

Setup mode is supported in hardware upgrade 1.10.2.x and later.
Automation Runtime B4.26 or higher is required to use setup mode.

Active setup mode is indicated by both the FAILSAFE LED (X20SL81xx series) or SE LED (X20SLXxxx series) as well as an entry in the logbook.

When setup mode is active, acknowledgment requests "SafeKEY exchange", "Firmware acknowledge" and "UDID mismatch" are no longer necessary.

Setup mode can be enabled and disabled using the operating elements of the "Remote Control" in SafeDESIGNER (X20SL81xx and X20SLXxxx series) or using the selector switch and acknowledgment button (X20SL81xx series).

Danger!

Setup mode is only permitted to be enabled during the commissioning of the machine/system.
Setup mode must be disabled during operation.

Danger!

After setup mode is ended, functional testing including a wiring test must be carried out.
If a SafeKEY or SafeLOGIC controller is replaced while setup mode is active, then setup mode will be disabled.
Functional testing must also be carried out in this case.

Functional testing is only permitted to be performed by personnel familiar with the safety application and its functions.

Be sure to validate the entire safety function!

8 Safety response time

The safety response time is the time between the arrival of the signal on the input channel and the output of the cutoff signal on the output.

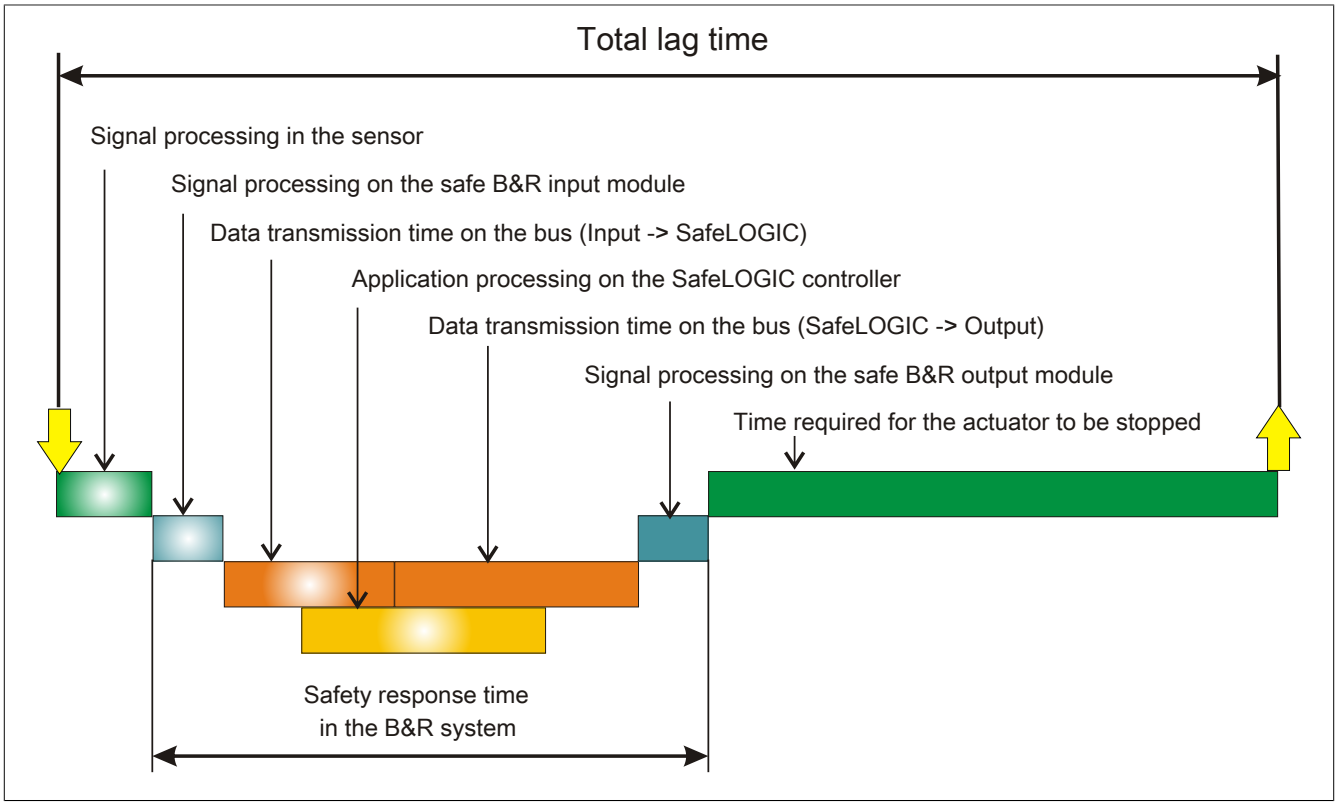


Figure 17: Total lag time

As illustrated in the figure, the safety response time in the B&R system is composed of the following partial response times:

- Signal processing on the safe B&R input module
- Data transmission time on the bus (Input -> SafeLOGIC)
- Data transmission time on the bus (SafeLOGIC -> Output)
- Signal processing on the safe B&R output module

Danger!

The following sections are dedicated exclusively to the safety response time in the B&R system. When assessing the complete safety response time, the user must include signal processing in the sensor as well as the time until the actuator is stopped.

Be sure to validate the total lag time on the system!

Information:

The safety response time in B&R products already contains all delays caused by sampling input data (sampling theorem).

8.1 Signal processing on the safe B&R input module

The maximum I/O update time in the "I/O update time" chapter for the respective module must be taken into account when processing signals in the safe B&R input module.

8.2 Data transmission time on the bus

The following relationship must be taken into consideration for the data transmission time on the bus:

- The time needed to transfer data from the input to the SafeLOGIC controller or to the output depends on the sum of the cycle times and CPU copy times in effect on the transfer line.
- POWERLINK MN (managing node, standard CPU) settings are important for the actual timing on the bus, but they cannot be used from a safety point of view since the values can be changed at any time in the course of modifications made outside of the safety application.
- In the SafeLOGIC controller, data transmission times are monitored on the bus using openSAFETY services. The time needed to process the application on the SafeLOGIC controller is taken into account in this test (system-dependent). Monitoring is defined in SafeDESIGNER using the parameters in parameter group "Safety Response Time".

Information:

The safety components located in this network segment could be cut off by the SafeLOGIC controller if modified parameters on the POWERLINK MN alter the data transmission times on the bus so that they lie outside of the SafeDESIGNER parameters defined in parameter group "Safety Response Time".

Information:

The safety components located in this network segment could be cut off by the SafeLOGIC controller if EMC disturbances cause data failures that fall outside of the SafeDESIGNER parameters defined in parameter group "Safety Response Time".

Calculating the maximum data transmission time - up to Release 1.9:

- The total max. data transmission time on the bus is calculated by adding parameter "Worst_Case_Response_Time_us" for the safe input module and parameter "Worst_Case_Response_Time_us" for the safe output module. When doing this, be sure to check parameter "Manual_Configuration". If parameter "Manual_Configuration" is set to "No", the value specified for parameter "Default_Worst_Case_Response_Time_us" is used.
- **Special case: Local inputs on the X20SLX module:**
  The total max. data transmission time on the bus is calculated by adding parameter "Cycle_Time_max_us" + 2000 µs and parameter "Worst_Case_Response_Time_us" for the safe output module. When doing this, be sure to check parameter "Manual_Configuration". If parameter "Manual_Configuration" is set to "No", the value specified for parameter "Default_Worst_Case_Response_Time_us" is used.

Calculating the maximum data transmission time - Release 1.10 and later:

The following parameters are relevant for calculating the data transmission time between the safe input module and safe output module; parameter "Manual Configuration" deserves special attention.

- Relevant parameters for "Manual Configuration = No":
  - "PacketLoss1": Parameter "Default Additional Tolerated Packet Loss" of group "Safety Response Time Defaults" of the SafeLOGIC controller
  - "DataDuration1": Parameter "Default Safe Data Duration" of group "Safety Response Time Defaults" of the SafeLOGIC controller
  - "NetworkSyncCompensation1": 12 ms
  - "PacketLoss2": Same as "PacketLoss1"
  - "DataDuration2": Same as "DataDuration1"
  - "NetworkSyncCompensation2": Same as "NetworkSyncCompensation1"
- Relevant parameters for "Manual Configuration = Yes":
  - "PacketLoss1": Parameter "Additional Tolerated Packet Loss" of group "Safety Response Time" of the safe input module
  - "DataDuration1": Parameter "Safe Data Duration" of group "Safety Response Time" of the safe input module
  - "NetworkSyncCompensation1": 12 ms
  - "PacketLoss2": Parameter "Additional Tolerated Packet Loss" of group "Safety Response Time" of the safe output module
  - "DataDuration2": Parameter "Safe Data Duration" of group "Safety Response Time" of the safe output module
  - "NetworkSyncCompensation2": Same as "NetworkSyncCompensation1"
- **Special case: Local inputs on the X20SLX module:**
  - "PacketLoss1": 0
  - "DataDuration1": Parameter "Cycle Time max" of group "Module Configuration" of the X20SLX + 2000 µs
  - "NetworkSyncCompensation1": 0 ms
- **Special case: Local outputs on the X20SLX module:**
  - "PacketLoss2": 0
  - "DataDuration2": Parameter "Cycle Time max" of group "Module Configuration" of the X20SLX + 2000 µs
  - "NetworkSyncCompensation2": 0 ms
- **Special case: Linking local inputs with local outputs on the X20SRT module:**
  - "PacketLoss1": 0
  - "PacketLoss2": 0
  - "DataDuration1": Parameter "Cycle time" of group "General"
  - "DataDuration2": Parameter "Cycle time" of group "General"
  - "NetworkSyncCompensation1": 0 ms
  - "NetworkSyncCompensation2": 0 ms

The following equation is used to calculate the maximum data transmission time between the safe input module and safe output module:

Maximum data transmission time = (PacketLoss1+1)* DataDuration1 + NetworkSyncCompensation1 + (Packet-Loss2+1)* DataDuration2 + NetworkSyncCompensation2

Information:

In addition to the data transmission time on the bus, the time for signal processing in the safe B&R input and output module must be taken into account (see section 8 "Safety response time").

Information:

For more information about the actual data transmission time, see Automation Help, section Diagnostics and service → Diagnostics tools → Network analyzer → Editor → Calculation of safety runtime. The cycle time of the safety application must also be added.

8.3 Signal processing on the safe B&R output module

The maximum I/O update time in the "I/O update time" chapter for the respective module must be taken into account when processing signals in the safe B&R output module.

8.4 Minimum signal lengths

The parameters in group "Safety Response Time" in SafeDESIGNER influence the maximum number of data packets that are permitted to fail without triggering a safety response. These parameters therefore act like a switch-off filter. If several data packets are lost within the tolerated amount, safety signals may not be detected if their low phase is shorter than the determined data transmission time.

Danger!

Lost signals can result in serious safety errors. Check all signals to determine the smallest possible pulse length and make sure that it is larger than the determined data transmission time.

Suggested solution:

- The switch-on filter can be used to extend the low phase of a signal on the input module.
- Low phases of signals from the SafeLOGIC controller can be lengthened with restart interlock functions or timer function blocks.

9 Intended use

Danger!

Danger from incorrect use of safety-related products/functions

Proper functionality is only ensured if the products/functions are used in accordance with their intended use by qualified personnel and the provided safety information is taken into account. The aforementioned conditions must be observed or covered by supplementary measures on your own responsibility in order to ensure the specified protective functions.

9.1 Qualified personnel

Use of safety-related products is restricted to the following persons:

- Qualified personnel who are familiar with relevant safety concepts for automation technology as well as applicable standards and regulations
- Qualified personnel who plan, develop, install and commission safety equipment in machines and systems

Qualified personnel in the context of this manual's safety guidelines are those who, because of their training, experience and instruction combined with their knowledge of relevant standards, regulations, accident prevention guidelines and operating conditions, are qualified to carry out essential tasks and recognize and avoid potentially dangerous situations.
In this regard, sufficient language skills are also required in order to be able to properly understand this manual.

9.2 Application range

The safety-related B&R control components described in this manual were designed, developed and manufactured for special applications for machine and personnel protection. They are not suitable for any use involving serious risks or hazards that could lead to the injury or death of several people or serious environmental impact without the implementation of exceptionally stringent safety precautions. In particular, this includes the use of these devices to monitor nuclear reactions in nuclear power plants, flight control systems, air traffic control, the control of mass transport vehicles, medical life support systems and the control of weapon systems.

When using safety-oriented control components, the safety precautions applying to industrial control systems (e.g. the provision of safety devices such as emergency stop circuits, etc.) must be observed in accordance with applicable national and international regulations. The same applies for all other devices connected to the system, e.g. drives or light curtains.

The safety guidelines, information about connection conditions (nameplate and documentation) and limit values specified in the technical data must be read carefully before installation and commissioning and must be strictly observed.

9.3 Security concept

B&R products communicate via a network interface and were developed for integration into a secure network. The network and B&R products are affected by the following hazards (not a complete list):

- Unauthorized access
- Digital intrusion
- Data leakage
- Data theft
- A variety of other types of IT security breaches

It is the responsibility of the operator to provide and maintain a secure connection between B&R products and the internal network as well as other networks, such as the Internet, if necessary. The following measures and security solutions are suitable for this purpose:

- Segmentation of the network (e.g. separation of the IT and OT networks)
- Firewalls for the secure connection of network segments
- Implementation of a security-optimized user account and password concept
- Intrusion prevention and authentication systems
- Endpoint security solutions with modules for anti-malware, data leakage prevention, etc.
- Data encryption

It is the responsibility of the operator to take appropriate measures and to implement effective security solutions.

B&R Industrial Automation GmbH and its subsidiaries are not liable for damages and/or losses resulting from, for example, IT security breaches, unauthorized access, digital intrusion, data leakage and/or data theft.

Before B&R releases products or updates, they are subjected to appropriate functional testing. Independently of this, the development of customized test processes is recommended in order to be able to check the effects of changes in advance. Such changes include, for example:

- Installation of product updates
- Notable system modifications such as configuration changes
- Import of updates or patches for third-party software (non-B&R software)
- Hardware replacement

These tests should ensure that implemented security measures remain effective and that systems behave as expected.

9.4 Safety technology disclaimer

The proper use of all B&R products must be guaranteed by the customer through the implementation of suitable training, instruction and documentation measures. The guidelines set forth in system user's manuals must be taken into consideration here as well. B&R has no obligation to provide verification or warnings with regard to the customer's purpose of using the delivered product.

Changes to the devices are not permitted when using safety-related components. Only certified products are permitted to be used. Currently valid product versions in each case are listed in the corresponding certificates. Current certificates are available on the B&R website (www.br-automation.com) in the Downloads section for the respective product. The use of non-certified products or product versions is not permitted.

All relevant information regarding these safety products must be read in the latest version of the related data sheet and the corresponding safety notices observed before the safety products are permitted to be operated. Certified data sheets are available on the B&R website (www.br-automation.com) in the Downloads section for the respective product.

B&R and its employees are not liable for any damages or loss resulting from the incorrect use of these products. The same applies to misuse that may result from specifications or statements made by B&R in connection with sales, support or application activities. It is the sole responsibility of the user to check all specifications and statements made by B&R for proper application as it pertains to safety-related applications. In addition, the user assumes sole responsibility for the proper design of the safety function as it pertains to safety-related applications.

9.5 X20 system characteristics

Because all X20 safety products are seamlessly integrated into the B&R base system, the same system characteristics and user notices from the X20 system user's manual also apply to X20 safety products.

Warning!

Possible failure of safety function

Malfunction of module due to unspecified operating conditions
The notes for installation and operation of the modules provided in the applicable documents must be observed.

In this regard, this means the content and user notices in the following applicable documentation must be observed for X20 safety products:

- X20 system user's manual
- Installation / EMC guide

9.6 Installation notes for X20 modules

Products must be protected against impermissible dirt and contaminants. Products are protected from dirt and contaminants up to pollution degree II as specified in the IEC 60664 standard.

Pollution degree II can usually be achieved in an enclosure with IP54 protection, but uncoated modules are NOT permitted to be operated in condensing relative humidity and temperatures under 0°C.

The operation of coated modules is allowed in condensing relative humidity.

Danger!

Pollution levels higher than specified by pollution degree II in standard IEC 60664 can result in dangerous failures. It is extremely important that you ensure a proper operating environment.

Danger!

In order to guarantee a specific voltage supply, a SELV power supply that conforms to IEC 60204 must be used to supply the bus, SafeIO and SafeLOGIC controller. This also applies to all digital signal sources that are connected to the modules.

If the power supply is grounded (PELV system), then only a GND connection is permitted for grounding. Grounding types that have ground connected to +24 VDC are not permitted.

The power supply of X20 potential groups must generally be protected using a fuse with a maximum of 10 A.
For more information, see chapter "Mechanical and electrical configuration" of the X20 or X67 user's manual.

9.7 Safe state

If an error is detected by the module (internal or wiring error), the modules enable the safe state. The safe state is structurally designed as a low state or cutoff and cannot be modified.

Danger!

Applications in which the safe state must actively switch on an actuator cannot be implemented with this module. In these cases, other measures must be taken to meet this safety-related requirement (e.g. mechanical brakes for hanging load that engage on power failure).

9.8 Mission time

All safety modules are designed to be maintenance-free. Repairs are not permitted to be carried out on safety modules.

All safety modules have a maximum mission time of 20 years.

This means that all safety modules must be taken out of service one week (at the latest) before the expiration of this 20-year time span (starting from B&R's delivery date).

Danger!

Operating safety modules beyond the specified mission time is not permitted! The user must ensure that all safety modules are replaced by new safety modules or removed from operation before their mission time expires.

10 Release information

A manual version always describes the respective range of functions for a given product set release. The following table shows the relationship between manual versions and releases.

<table>
<tr><th>Manual version</th><th>Valid for</th></tr>
<tr><td>V1.141
V1.140
V1.131
V1.130
V1.123
V1.122
V1.121
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</td><td>
<table>
<tr><th>Version</th><th>Starting with</th><th>Up to</th></tr>
<tr><td>Product set</td><td>Release 1.2</td><td>Release 1.10</td></tr>
<tr><td>SafeDESIGNER</td><td>2.70</td><td>4.9</td></tr>
<tr><td>Firmware</td><td>270</td><td>399</td></tr>
<tr><td>Upgrades</td><td>1.2.0.0</td><td>1.10.999.999</td></tr>
</table>
</td></tr>
<tr><td>V1.02
V1.01
V1.00</td><td>
<table>
<tr><th>Version</th><th>Starting with</th><th>Up to</th></tr>
<tr><td>Product set</td><td>Release 1.0</td><td>Release 1.1</td></tr>
<tr><td>SafeDESIGNER</td><td>2.58</td><td>2.69</td></tr>
<tr><td>Firmware</td><td>256</td><td>269</td></tr>
<tr><td>Upgrades</td><td>1.0.0.0</td><td>1.1.999.999</td></tr>
</table>
</td></tr>
</table>

Table 36: Release information

11 Version history

Version	Date	Comment
1.141	April 2019	• Chapter 3 "Technical data": Updated standards. • Updated chapter 9.3 "Security concept". • Updated chapter 9.6 "Installation notes for X20 modules".
1.140	February 2019	• Chapter 3 "Technical data": – Updated max. number of openSAFETY nodes. – Limited installation elevation to 2000 m. – Coated module: Extended temperature range. • Chapter 5.3 "Parameters in SafeDESIGNER - Release 1.10 and later": Added parameter "Process Data Transmission Rate" • Chapter 8.2 "Data transmission time on the bus": Updated calculation of maximum data transmission time. • Chapter 9 "Intended use": Added danger notice. • Added chapter "Security notes". • Chapter 9.5 "X20 system characteristics": Added warning notice. • Updated standards. • Editorial changes.
1.120	November 2017	• Chapter 3 "Technical data": – Updated standards and safety characteristics. – Added timing precision. – Updated max. number of openSAFETY nodes. – Added max. number of variable with variable status. • Chapter 5.1 "Parameters in the I/O configuration": Group "POWERLINK parameters": Updated and added information. • Chapter 5.3 "Parameters in SafeDESIGNER - Release 1.10 and later": Group "Safety Response Time Defaults": Updated parameter "Default Safe Data Duration". • Chapter 5.4 "SafeLOGIC - Channel list": Added new objects for hardware upgrade 1.10.4.0 and later. • Chapter 6.5 "SafeKEY or safety section of the CompactFlash card": Updated description. • Chapter 7.3 "SafeLOGIC to SafeLOGIC communication": Added system requirements. • Chapter 7.3.6 "Parameters for connection - Release 1.10 and later": Group "Safety Response Time": Updated parameter "Safe Data Duration". • Chapter 7.5 "Blackout mode": Updated requirements for operation. • Chapter 8.2 "Data transmission time on the bus": Updated description and added information. • Chapter 9.6 "Installation notes for X20 modules": Updated danger notice. • Editorial changes.
1.111	February 2017	• Chapter 5.1 "Parameters in the I/O configuration": Added parameters "Interface Slot Enable" and "Standalone mode". • Chapter 5.3 "Parameters in SafeDESIGNER - Release 1.10 and later": Added parameters "Activate Setup Mode on empty SafeKEY", "Auto acknowledge firmware mismatch" and "Auto acknowledge SafeKEY exchange". • Chapter 5.4 "SafeLOGIC - Channel list": Added channel "SafeFirmwareVersion" • Chapter 7.2 "Automatic acknowledgment": Added.
1.110	January 2017	• Chapter 1.1 "Function": Added blackout mode. • Chapter 3 "Technical data": Updated standards and safety characteristics, added information. • Chapter 4.1.3 "Selector switch and confirmation button": Updated new switch positions. • Chapter 5.3 "Parameters in SafeDESIGNER - Release 1.10 and later": Group "Basic": Added information. • Chapter 6.5.2 "Acknowledging a SafeKEY replacement": Added information. • Chapter 7.1 "Operation via the AsSafety library": Removed content, added reference to Automation Help. • Chapter 7.5 "Blackout mode": Added. • Chapter 7.6 "Setup mode": Added. • Chapter 8.2 "Data transmission time on the bus": Added information about data transmission time.
1.102	June 2016	Renamed documentation from X20SL810x to X20SL81xx. Added module X20SL8110. • Chapter 3 "Technical data": – Updated standards. – Updated technical data.

Table 37: Version history

Version	Date	Comment
1.101	March 2016	• Chapter 8 "Safety response time": Added information.
1.100	January 2016	Merged coated/uncoated modules. Renamed documentation from X20SL8100 to X20SL810x. Added X20SL8101 module. • Chapter 1 "General information": Added. • Chapter 3 "Technical data": – Updated standards. – Updated temperature range. – Updated technical data. • Revised chapter 4.3.2 "LED "STATUS"". • Revised chapter 4.3.4 "RJ45 ports". • Chapter 5.2 "Parameters in SafeDESIGNER - up to Release 1.9": Added parameter "KeepRemanent". • Chapter 5.3 "Parameters in SafeDESIGNER - Release 1.10 and later": Added. • Chapter 5.4 "SafeLOGIC - Channel list": Added additional register description. • Added chapter "Check the version of the library being used". • Chapter 7.2 "Automatic acknowledgment": Added. • Chapter 7.3.6 "Parameters for connection - Release 1.10 and later": Added. • Chapter 8.1 "Signal processing on the safe B&R input module": Updated description. • Chapter 8.2 "Data transmission time on the bus": Updated description with "Release 1.10 and later". • Chapter 8.3 "Signal processing on the safe B&R output module": Updated description. • Chapter 8.4 "Minimum signal lengths": Updated description. • Revised chapter 9.4 "Safety technology disclaimer". • Chapter 10 "Release information": Updated.
1.71	June 2014	• Chapter 3 "Technical data": – Added "Safety-related characteristic values" and deleted chapter "Safety-related characteristic values". – "Functionality": Added following items: - "Max. number of openSAFETY nodes" - "Max. number of POWERLINK controlled nodes" - "Data exchange between CPU and SL" - "Data exchange between SL and SL" – Added "Limit values for SafeDESIGNER application". • Chapter 5.2 "Parameters in SafeDESIGNER - up to Release 1.9": Group "Safety_Response_Time_Defaults": Added parameter "Default_Node_Guarding_Lifetime". • Chapter 7.3.5 "Parameters for connection - up to Release 1.9": Group "Safety_Response_Time": Added parameter "Node_Guarding_Lifetime". • Chapter 8.2 "Data transmission time on the bus": Updated description. • Chapter 9.6 "Installation notes for X20 modules": Removed figure "Protecting various potential groups", updated description accordingly. • Chapter 10 "Release information": Updated.
1.70	October 2013	First edition as a product-specific manual

Table 37: Version history

12 EC declaration of conformity

This document was originally written in the German language. The German edition therefore represents the original documentation in accordance with the 2006/42/EC Machinery Directive. Documents in other languages are to be interpreted as translations of the original documentation.

Product manufacturer:

B&R Industrial Automation GmbH

B&R Strasse 1

5142 Eggelsberg

Austria

Telephone: +43 7748 6586-0

Fax: +43 7748 6586-26

office@br-automation.com

The place of jurisdiction, in accordance with article 17 of the European Convention on Courts of Jurisdiction and Enforcement, is A-4910

Ried im Innkreis, Austria, commercial register court: Ried im Innkreis, Austria

Commercial register number: FN 111651 v.

The place of fulfillment in accordance with article 5 of the European Convention on Courts of Jurisdiction and Enforcement is A-5142 Eggelsberg, Austria

VATIN: ATU62367156

The EC declarations of conformity for B&R products can be downloaded from the B&R website www.br-automation.com.