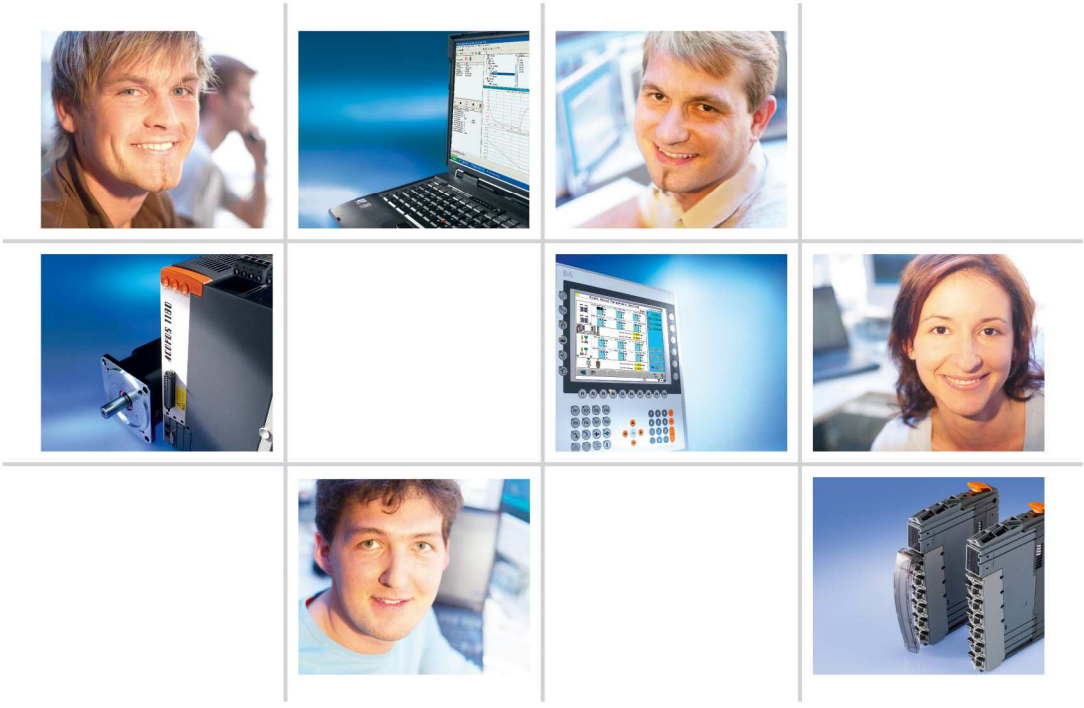
Basics of Integrated Safety Technology

TM500



Perfection in Automation

www.br-automation.com

Requirements

Training modules:	The basics of safety technology
Software:	None
Hardware:	None

Table of contents

1. INTRODUCTION

This training module "Basics of Integrated Safety Technology" offers a brief overview of the B&R safety concept.

Throughout the course of this training, interaction between standards and requirements of machine manufacturers and end users will be explored with regard to safety technology. Furthermore, the safety concept developed by B&R will also be explained.

The B&R safety concept is not only focused on specialized, safety-related components, but also involves the full palette of automation technology.

Fig. 1: Integrated safety technology

Safety technology is usually hard-wired into a machine. As a result, the safety reactions operate according to a strict scheme. This means that the machine or system completely shuts down when a safety door is opened or a light curtain is triggered.

With B&R's Integrated Safety Technology concept, new possibilities for safety technology have become available.

Hard wiring is replaced by secure data transfer

Rigid safety reactions are replaced by flexible solutions

Smart Safe Reactions prevent manipulation and increase machine value

1.1 Objective

The goal of this training module is to get to know B&R Integrated Safety Technology products as well as the philosophy behind their application.

Participants will become acquainted with available components and learn how to configure them for optimal application.

Participants will receive a brief introduction of the initial start-up and maintenance options.

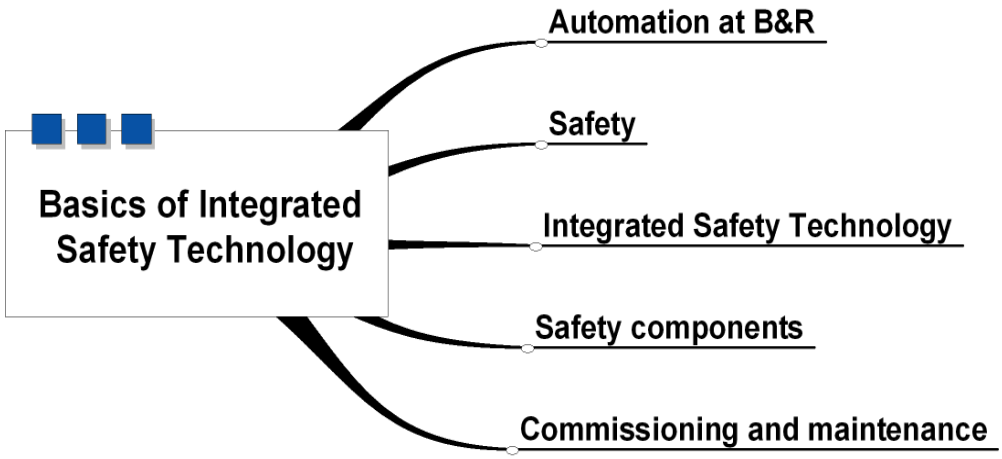


Fig. 2: Overview

2. AUTOMATION AT B&R

Since 1979, B&R has been active in the automation branch with a vision and pioneering spirit to achieve great things. Breadth of vision with regard to market development and trends allows B&R to offer high-tech solutions to customers and set new trends in automation. B&R's innovations and products always allow its customers to remain on the cutting edge.

Perfection in Automation
www.br-automation.com

Fig. 3: Perfection in Automation

2.1 B&R products

B&R's wide range of products offer complete automation solutions from a single source. These include PLCs, industrial PCs, I/Os, visualization devices and APROL drives as well as safety technology. Customers can scale (PLC, I/O systems) and assemble their machines with complete flexibility.

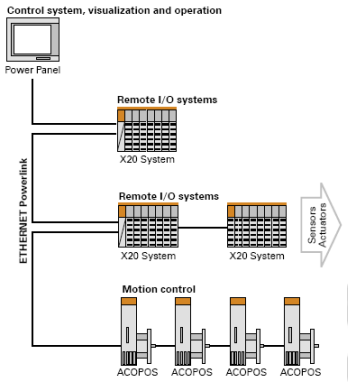


Fig. 4: Configuration 1

The operating device is the central controller. Components, such as I/O systems and drives, are connected via a high-performance network.

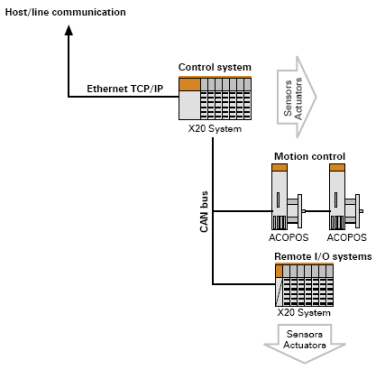


Fig. 5: Configuration 2

The compact controller is integrated in the higher-level company network, which allows external communication. Data can be read from the machine controller and commands can be given over the plant network. Communication with drives and remote I/O systems is possible via the internal machine communication bus.

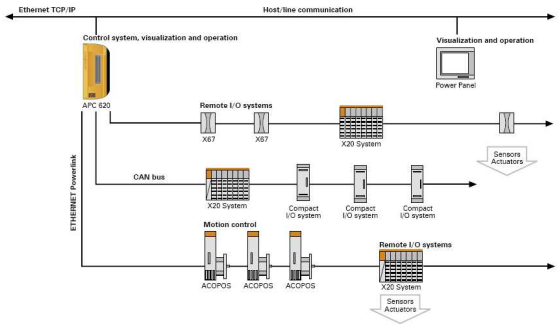


Fig. 6: Configuration 3

The industrial PC handles all automation tasks centrally. I/O peripherals and drives are connected via fieldbus systems and networks. Operation and visualization takes place using a local or remote display unit.

Complete automation solutions from a single source

2.2 Possibilities with B&R

Custom solutions in highly varied branches (packaging, plastics, printing) aid the customer in gaining a distinct competitive edge. B&R products may be implemented in a wide range of industrial branches. Through such realizable, comprehensive automation solutions, the customer can achieve maximum efficiency all from one source.

Fig. 7: Innovations in the packaging industry

Print:

- Print mark detection
- Vertical integration
- Configurable date format
- Custom labeling

Fig. 8: Innovations in the plastic industry

Extruder:

- Control of worm drive
- Start-up profile
- Melt pressure control
- Synchronization of the entire machine

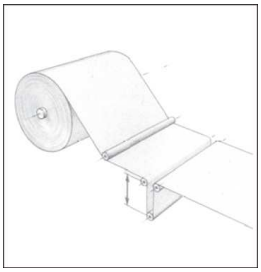


Fig. 9: Innovations in the print industry

Winding:

- Tension control with force measurement roller
- Dancer roll control
- Compensation of mass inertia
- On-the-fly roll switching

Solutions for all industries

2.3 Safe with B&R

Machines and systems may pose potentially life and health-threatening risks for its users. Appropriate safety components help to eliminate these risks.

Fig. 10: Dangers of machines

Today, safety on machines is often limited to E-stop buttons that are wired directly to safety relays in the switching cabinet. The only possible safety reaction is switching off the machine. A disturbance of safety equipment leads to a complete machine shutdown when using additional safety components (safety door, light curtain). This safety technology always functions in the same fixed scheme.

B&R relies on the integration of safety components for innovative solutions. Hard wiring individual safety components is replaced by secure data transfer. A departure from rigid safety reactions is possible because solutions for various safety functions can be integrated.

A safe CPU, safe I/O module and ACOPOS and ACOPOSmulti safe motion control capabilities are available components for safety technology.

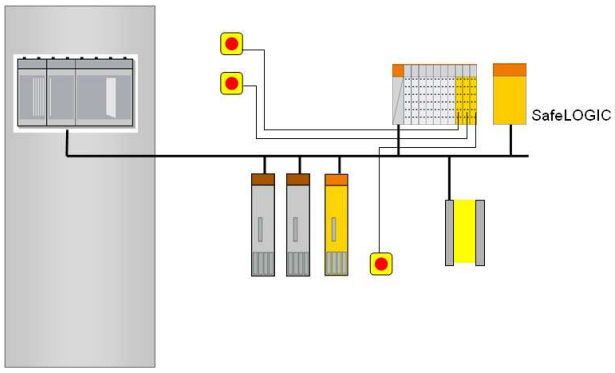


Fig. 11: Safety Hardware

Transfer of secure data takes place using the open communication protocol POWERLINK Safety.

Fig. 12: POWERLINK safety

Now it is possible to program flexible safety functions directly in Automation Studio. The manufacturer-independent PLCopen safety function blocks may be used here.

Fig. 13: PLCopen safety

Innovative solutions for safety technology

3. THE TOPIC OF SAFETY

The safety of a machine or system is significantly influenced by the **"secure function"** of its control and monitoring mechanisms. Safety is ensured if each specific safety function is executed in terms of the associated risk, i.e. the machine may be considered “safe”.

Safety must be guaranteed under normal (undisturbed) circumstances and also in the presence of errors.

3.1 Standards and guidelines

Standards and guidelines are important for machine manufacturers. Guidelines specifying minimum health and safety requirements must be fulfilled by the manufacturers.

The goal of the machine guidelines is to increase, adjust and maintain the **safety level** of machines. These guidelines are based on the following principles:

- The guidelines specify mandatory, fundamental health and safety requirements
- Harmonized standards are made up of technical specifications and detailed solutions.
- A product is produced according to harmonized standards, which allow it to fulfill the fundamental safety requirements of machine guidelines (assumption effect)

Fig. 14: Standards and guidelines

3.2 Requirements for the safety system

Today's safety solutions have **fixed performance**, e.g. the opening of a safety door results in immediate shut down. It is also impossible to enable or disable safety functions while in various machine operating modes.

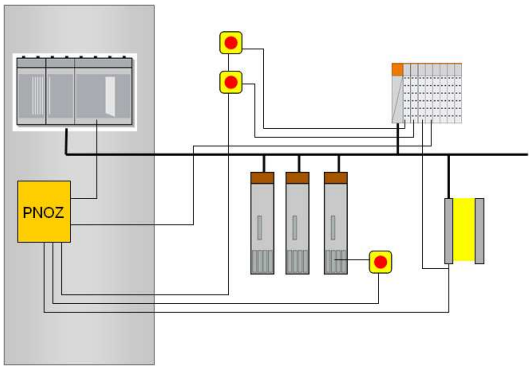


Fig. 15: Safety Technology - hard wired

According to a 2004 study on "Manipulation of Machine Safety Devices" from the Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), nearly **37% of machine safety devices** are constantly or temporarily **manipulated**. Approximately **one half** of these manipulations could lead to **accidents**. According to those interviewed, nearly a quarter of all work-related accidents are traced back to such manipulations. The following reasons for manipulation of safety devices were given in the study:

- 43 % - Time optimization of operational procedures
- 22 % - Saving time / faster operations
- 14 % - Time / performance pressure
- 7 % - Increased production

To the question of what concrete advantage the user gains from manipulation, about a quarter of the study participants attributed increased work process and production. In 9% of the cases, manipulation is necessary for the work process, while 7% manipulate to achieve a faster setup process.

The study clearly highlights the **deficiencies** in the **existing safety concepts**. Following the conclusion of the study, the HVBG recommends the adoption of innovative safety concepts, particularly safety-related **considerations** for **special operating modes** involving machine operation and regulation (process observation, set up, etc.)

3.2.1 Regulations and standards

With consideration to standards, a safety system must conform to the **latest technology**. Furthermore, high demands on **manipulation safety** must also be considered. Worldwide, uniform standards result in one clearly defined safety standard.

3.2.2 Machine manufacturing

Several points stand in the foreground for machine manufacturers. They benefit from an **innovative safety system**, which guarantees a return on investment and is **cost-effective**. Additionally, a high degree of manipulation safety must be guaranteed as well as **flexibility** in machine construction. The selection of the right safety system can consequently increase the value of each individual machine significantly.

3.2.3 End user

The end user desires the **highest possible level of safety** from their machines, in order to best protect their employees and prevent accidents. Furthermore, **high availability** and **low service costs** are also in demand. Downtimes (emptying the machine, setting it up again) in the event of an error must be minimized and service should be prompt and uncomplicated. Innovative safety concepts increase productivity, thereby giving the end user a clear advantage.

3.3 Comparison of hard-wired and integrated safety

Fig. 16 depicts a comparison of hard-wired safety solutions and flexible, integrated solutions with regard to the aforementioned section items, regulations and standars, machine manufacture and end user.

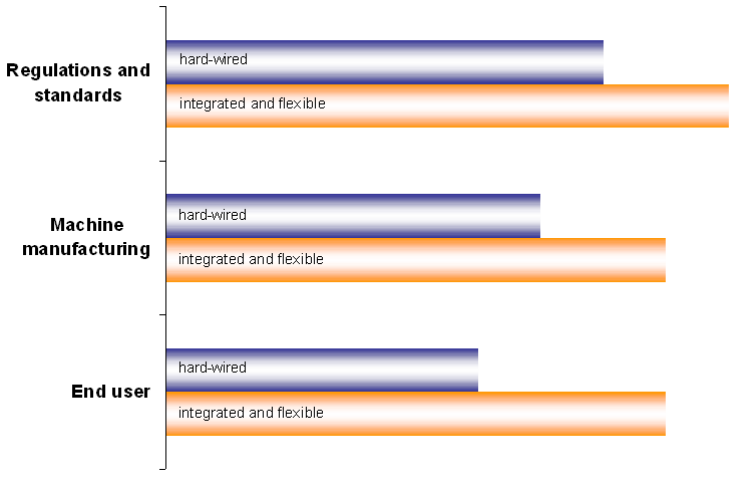


Fig. 16: Comparison

With consideration to **standards and regulations**, the safety system should apply to the latest technology. Integrated and flexible solutions have greater potential because they conform to technological standards and also offer pathways to prevent manipulation.

An integrated and flexible safety system possesses more potential in **machine manufacturing** than a hard-wired solution. This potential is most evident when programming safety applications with flexible reactions to various situations.

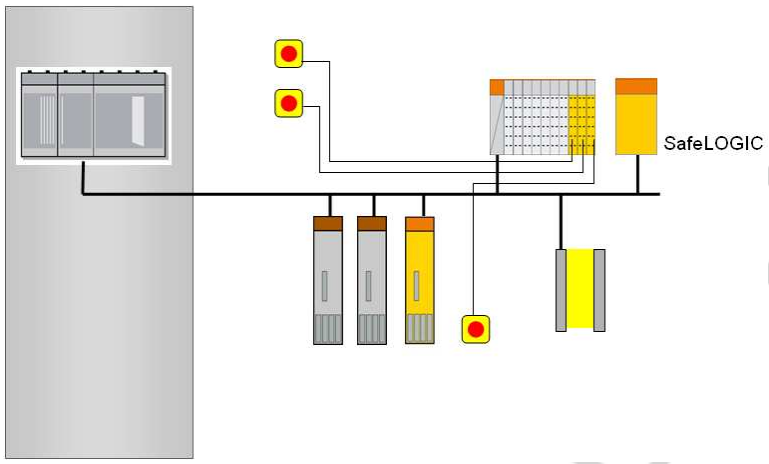


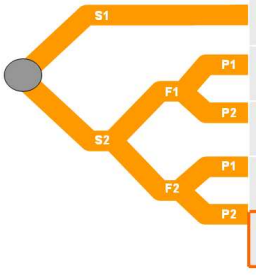
Fig. 17: Safety Technology – integrated and flexible

Hard-wired safety solutions most often fail to offer the **end user** the same opportunities as integrated and flexible safety technology. This is evident in machine availability and productivity, service costs and general machine safety for preventing accidents.

3.4 Risk analysis and risk graph

The manufacturer and his representatives are responsible for machine safety. They must run a risk analysis of the possible dangers of the machine and take appropriate measures to manage and reduce them. One such measure is installing adequate safety devices.

The required safety class of the given standard may be determined based on a starting point in the risk graph and other diverse criteria, i.e. seriousness of injury, frequency and length of exposure to danger.



Preferred category (CAT) EN954-1	Performance Level (PL) EN13849	Safety Integrity Level (SIL) IEC61508	Safety Integrity Level (SIL) IEC62061	Undetected errors per hour
CAT 1	PL a	No specific safety requirements		
CAT 1/2	PL b	SIL 1	SIL 1	$< 10^{-5}$
CAT 2/3	PL c	SIL 1	SIL 1	$< 3 * 10^{-6}$
CAT 3	PL d	SIL 2	SIL 2	$< 10^{-6}$
CAT 4	PL e	SIL 3	SIL 3	$< 10^{-7}$

Fig. 18: International standards and safety levels

The risk graph depicts a comparison of individual standards. Fig. 18 serves as an overview of the relevant standards and their relationship to each safety level. However, the risk probability is not present as each procedure differs under varying standards.

4. INTEGRATED SAFETY TECHNOLOGY

This is a synonym for the way in which the safety-related components work with one another and with standard automation technology.

Fig. 19: Integrated safety technology

Emphasis is clearly placed on the products when it comes to integrated safety technology. All products in this scheme are inter-coordinated and linked with existing automation products. Compatible applications can therefore be created very easily.

Just a few products are revolutionizing safety technology. It's not a question of the hardware used, but in the overall concept. A transformation is taking place in the possibilities of safety technology.

4.1 Philosophy

Automation Studio, with the accompanying **SafeDESIGNER Toolset**, is the only tool necessary for safety applications. The safety application is programmed using certified **PLCopen Safety Library** function blocks. This allows virtual wiring of safety functions.

SafeLOGIC (safe CPUs), **SafeIO** (safe I/O modules) and **SafeMC** (safe motion control) for ACOPOS and ACOPOSmulti are available devices.

Use of the **fastest, real-time safety bus system** meets the highest SIL 3 performance standards with cycle times under 200 µs. This results in a **reaction time** which is comparable with that of a hard-wired system. Similarly, the safe CPU yields **cycle times < 1ms**, making it the fastest on the market. Because the safety concept is based on an **open bus standard**, it remains open for further device connections in the future.

The products of integrated safety technology make it possible to achieve the **highest safety classes** (SIL 3, CAT 4, PL e) for machine manufacturing standards.

4.2 Customer benefits

Smart safe reaction
The programmable safety solution enables **flexible reactions** to safety requirements. The maintenance of machine synchronization has also proven especially advantageous. The possibility of flexible reactions in various operating modes (i.e. opening of a safety door) reduces motivation for manipulation.

Complete
The B&R safety concept spans **all sectors of safety technology** (programming, CPU, I/O, motion). It also guarantees the highest level of safety for machine manufacturing. This makes SIL 3 applications easily realizable.

Integrated but separated
Standard CPUs and safe CPUs may be used **in any combination**. Selective, machine-specific safety functions can be activated or deactivated using commissioning parameters. Documentation of the safety application can be easily compiled using SafeDESIGNER "One Click Printout".

Plug & Run
Safety modules can be **easily** exchanged by **plugging and unplugging**. The system checks the corresponding module for validity. It is then configured with the defined parameters and automatically set to RUN mode.

4.3 Safety principles

Integrated safety technology modules internally possess **much more functionality** than standard modules.

Input modules possess a clock output that is routed to the corresponding input via a switch contact. A defined modulation pattern is sent via this clock output, whereby short-circuits to +24 V or GND can be recognized on the lines.

The **output module** self-tests its outputs in a defined time interval. In this way, the internal module functionality can be checked and wiring problems such as short-circuits to +24V / GND or broken lines can be detected.

The module data is sent via a **secure transfer protocol**. This data is accessed in the safety application via safe data types (i.e. SAFEBOOL). However, data from the functional application can be accessed via standard data types (i.e. BOOL).

4.4 Overview and functionality

The use of safety bus technology results in the **reduction to just one cable** and allows the existing infrastructure to be used for transfer.

Cycle times of 200 µs can be achieved with POWERLINK Safety. This means that the advantages of hard-wired solutions (speed) are compatible with the possibilities of intelligent safety technology (flexibility).

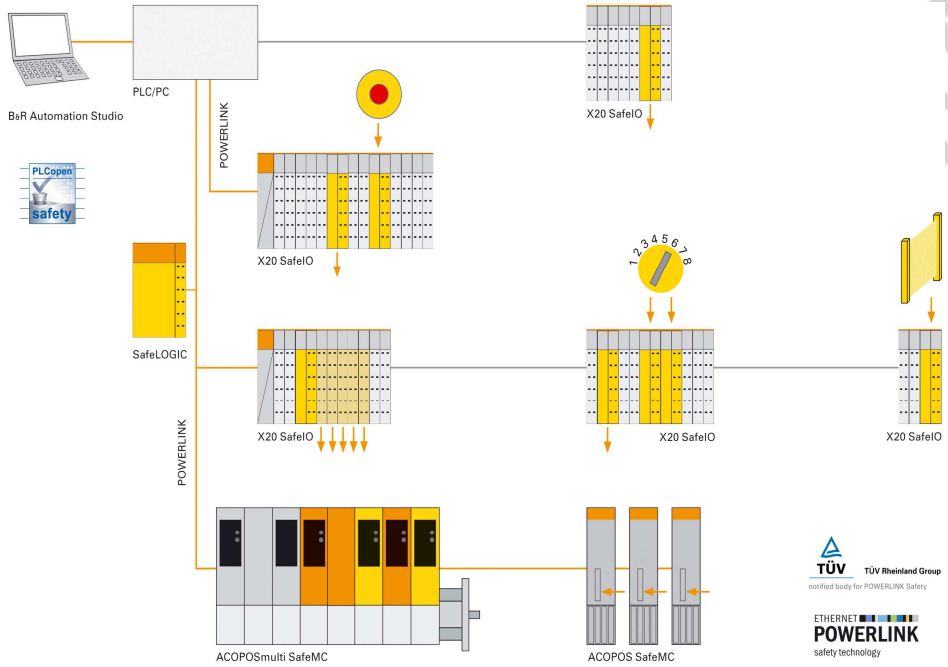


Fig. 20: The system at a glance

Because the safety modules are **completely integrated in the system**, they can be installed wherever needed (directly behind the X20 CPU or behind an X20 Bus connector). This makes it easy to **add** safety functions to an **existing machine**. Decentralized distribution of I/Os increases flexibility and optimally supports **modular machine assembly**.

Data **access** is **absolutely transparent** from a standard application viewpoint. Complicated communication mechanisms between standard and safety applications are no longer needed. However, access is non-reactive, which means the safety-related functions cannot be influenced by the standard application.

The certified function blocks located in the **PLCopen Safety Library** form the basis for **safety programming** and significantly simplify application programming.

Programming safe applications is reduced to **virtually wiring** certified function blocks.

5. SAFETY COMPONENTS

Integrated safety technology components:

- POWERLINK safety
- SafeIO modules based on the X20 system
- ACOPOS and ACOPOSmulti safe motion control (SafeMC) capabilities
- SafeLOGIC
- SafeDESIGNER as an Automation Studio toolset

5.1 POWERLINK safety

B&R uses POWERLINK Safety technology, the first real-time Ethernet-based safety bus, to transfer safety-related data.

Fig. 21: POWERLINK safety

A POWERLINK Safety frame consists of **two subframes** and can transfer up to 254 bytes of safety reference data. Two different CRC algorithms can be used depending on the length of the reference data.

Note:

Safety measures are fully separated from the underlying fieldbus.

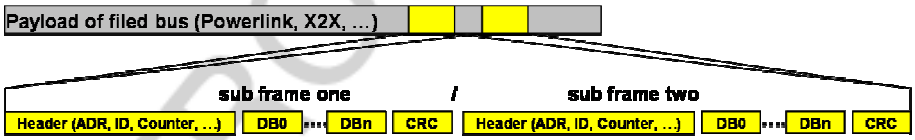


Fig. 22: POWERLINK Safety frame

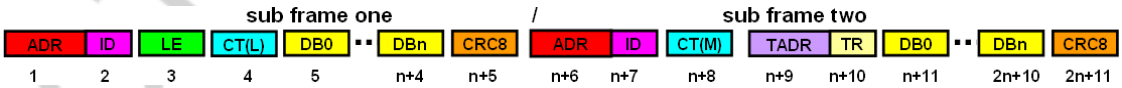


Fig. 23: POWERLINLK Safety frame with n = 0....8 bytes of reference data

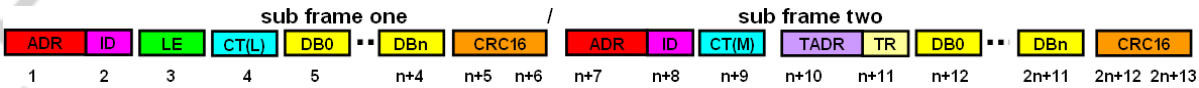


Fig. 24: POWERLINLK Safety frame with n = 9....254 bytes of reference data

5.2 SafeIO

The SafeIO modules are based on the reliable, modular X20 I/O system. For the secure digital connection of sensors and actuators, every model type is available and **multi-functional capabilities** are provided.

Fig. 25: SafeIO

Parameter settings allow adjustments to be made to operating conditions, such as multi-channel analysis, filter parameters and more.

Of course, SafeIO modules are completely integrated in the X20 system family and can be used in any position or combination.

SafeIO modules are differentiated as follows:

- Safe Digital In (SI)
- Safe Digital Out (SO)
- Safe Power (SP)

5.2.1 Safe Digital In

Safe Digital In modules (SI) are used for **safe sensors**. They are characterized by helpful functions, such as multi-channel analysis.

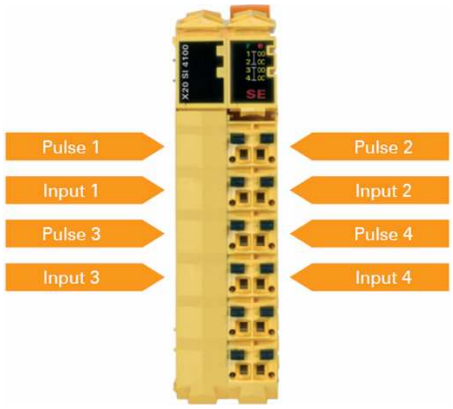


Fig. 26: Safe Digital In (SI)

Direct multi-channel analysis for channels 1 & 2 as well as for 3 & 4 with additional simultaneous operation monitoring is integrated in the modules.

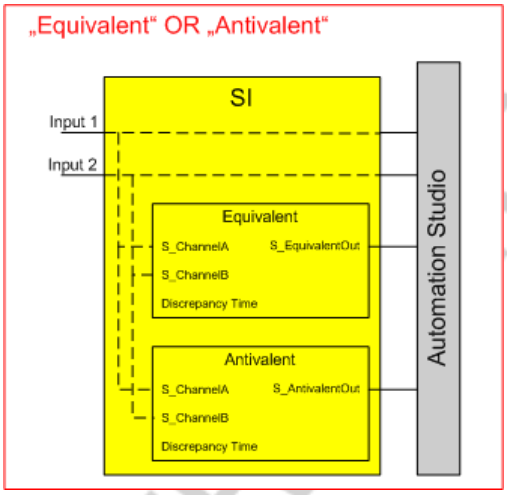


Fig. 27: Multi-channel analysis

Additionally, LEDs are used to signal potential errors on a channel or the entire module. Error information is available for every channel, which can be processed in the standard CPU and in SafeLOGIC (secure data).

Caution:

If an internal hardware error (i.e. input circuit defect) occurs, any of the potential error situations can arise despite correct external wiring!

The available module types differ in number of channels (2 channels or 4 channels).

Because of the aforementioned **multi-function capability**, these modules are deployable in all typical applications:

- Light curtain, laser scanner
- E-stop switch
- Two-hand operation devices
- Operating mode switch

Single-channel connection of electro-mechanical switches

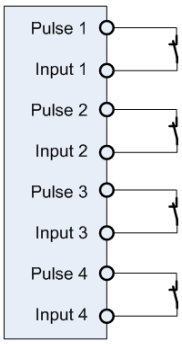


Fig. 28: Single-channel connection

A specific clock output is assigned to each input channel when connecting single-channel, electro-mechanical switches.

Error	Error at	
	N.C. contact	N.O. contact
Ground fault on clock output	Acknowledged	Acknowledged
Clock output shorted to 24 V	Acknowledged	Acknowledged
Cross circuit between clock output and other clock signal	Acknowledged	Acknowledged
Ground fault on signal input	Not acknowledged	Acknowledged
Signal input shorted to 24 V	Acknowledged	Acknowledged
Cross circuit between signal input and other clock signal	Acknowledged	Acknowledged
Cross circuit between clock output and signal input	Not acknowledged	Not acknowledged
Wire break	Not acknowledged	Not acknowledged

Two-channel connection of electro-mechanical switches

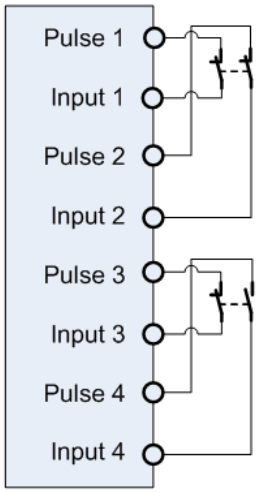


Fig. 29: Two-channel connection

A specific clock output is assigned to each input channel during the connection of two-channel, electro-mechanical switches.

N C contact

Error	N C contact Error at	
	Inactive N C contact	Active N C contact
Ground fault on clock output	Acknowledged	Acknowledged
Clock output shorted to 24 V	Acknowledged	Acknowledged
Cross circuit between clock output and other clock signal	Acknowledged	Acknowledged
Ground fault on signal input	Acknowledged	Acknowledged [1]
Signal input shorted to 24 V	Acknowledged	Acknowledged
Cross circuit between signal input and other clock signal	Acknowledged	Acknowledged
Cross circuit between clock output and signal input	Acknowledged [1]	Acknowledged [1]
Wire break	Acknowledged [1]	Not acknowledged

1) Two-channel evaluation of the module

N O contact

Error	N O contact Error at	
	Inactive N O contact	Active N O contact
Ground fault on clock output	Acknowledged	Acknowledged
Clock output shorted to 24 V	Acknowledged	Acknowledged
Cross circuit between clock output and other clock signal	Acknowledged	Acknowledged
Ground fault on signal input	Acknowledged [1)]	Acknowledged
Signal input shorted to 24 V	Acknowledged	Acknowledged
Cross circuit between signal input and other clock signal	Acknowledged	Acknowledged
Cross circuit between clock output and signal input (N.C.)	Not acknowledged	Acknowledged
Broken connection (N.C.)	Acknowledged	Not acknowledged
Cross circuit between clock output and signal input (N.O.)	Acknowledged [1)]	Not acknowledged
Broken connection (N.O.)	Not acknowledged	Acknowledged [1)]

1) Two-channel evaluation of the module

Connection of multi-channel, electro-mechanical switches

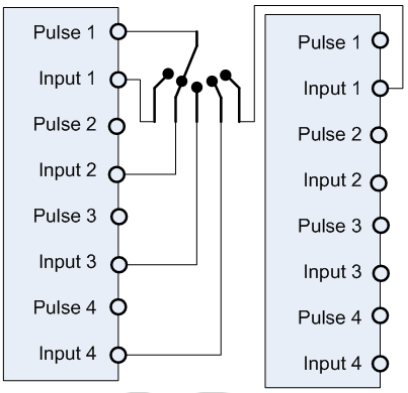


Fig. 30: Multi-channel connection

Multi-channel switches (operating mode switches, switching devices with shifting capability) may be connected to several secure, digital input devices. In this application, the clock evaluation on the second module must be triggered by the first module's clock.

Error	
Ground fault on clock output	Acknowledged
Clock output shorted to 24 V	Acknowledged
Cross circuit between clock output and other clock signal	Acknowledged [1]
Ground fault on signal input (active signal)	Acknowledged [1]
Ground fault on signal input (inactive signal)	Not acknowledged
Signal input shorted to 24 V	Acknowledged
Cross circuit between signal input and other clock signal	Acknowledged [1]
Cross circuit between clock output and signal input (active signal)	Not acknowledged
Broken connection (inactive signal)	Acknowledged [1]
Cross circuit between clock output and signal input (active signal)	Acknowledged [1]
Broken connection (inactive signal)	Not acknowledged

1) detected in the application by PLCopen function block "Mode Selector"

Active sensor connection

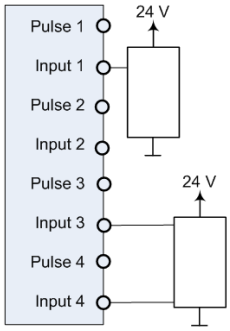


Fig. 31: Active sensor connection

Active sensors (light curtains, laser scanners, inductive sensors) may also be connected to a secure, digital input module. In such applications, the module does not use a timing pattern. Any gaps in the test for the connected OSSD (Output Switching Sensor Device) outputs must be masked out with the module's filter options in order to prevent accidental shut-down.

Caution:

The module does not have error detection because it does not use a pulse pattern.
All potential errors in the wiring must be detected through supplementary measures or connected devices.

5.2.2 Safe Digital Out

Safe Digital Out modules (SO) are used for controlling **secure actuators**.

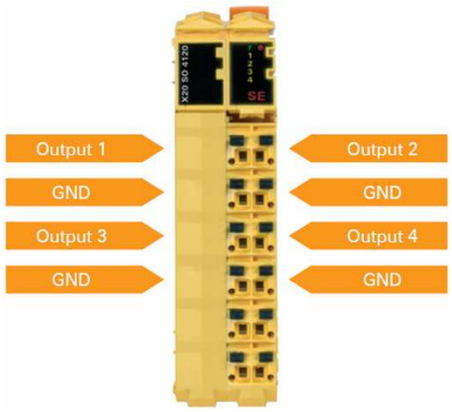


Fig. 32: Safe Digital Out (SO)

Safe Digital Out modules provide two different options for how the output is set. These include the "direct" and "via SafeLOGIC" approval methods.

DIRECT
Within standard application, the module represents a "normal" digital output module. This mode is particularly interesting because, in this mode, the secure digital output module functions identically to that of a standard digital output, and most importantly, is completely compatible with a standard output in terms of time performance.

VIA SafeLOGIC
In this mode, the safety module output is operated completely via SafeLOGIC.

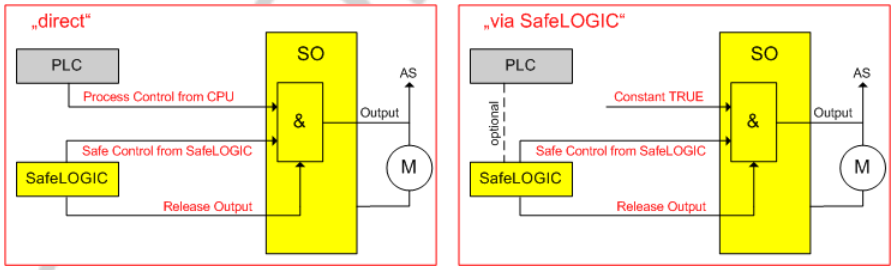


Fig. 33: Approval principle

Each channel possesses its own restart inhibit, i.e. the restart inhibit is activated if the output is switched to LOW via the safety application. The restart inhibit is enabled through a rising edge on the release output.

Each channel has its own read back channel for the analysis of the current physical output status.

LEDs are used to signal the error status of a channel or the complete module. Error information is available for every channel, which can be processed in the standard CPU and in SafeLOGIC (secure data).

Caution:

If an internal hardware error (i.e. output driver) occurs, any of the potential error situations can arise despite correct external wiring!

The module self-checks the functionality of its outputs in a certain time interval. To do this, the output is temporarily set to LOW while controllability is checked. The option is also available to disable this type of monitoring.

The module automatically measures the current on the outputs. This allows easy recognition of a wire break on the channel or a defective muting lamp.

Note:

The characteristics for current measurement are 30 mA - 0.5 A or 30 mA – 2 A.

The available module types have a different output current (0.5 A or 2 A) and number of channels (2 channels or 4 channels).

The module's **multi-functional capability** also ensures its use for many applications:

- ACOPOS and ACOPOSmulti enable input
- Safety valves, safety relays
- Compact motors
- Safety doors
- Muting lamps

Connection of safety actuators

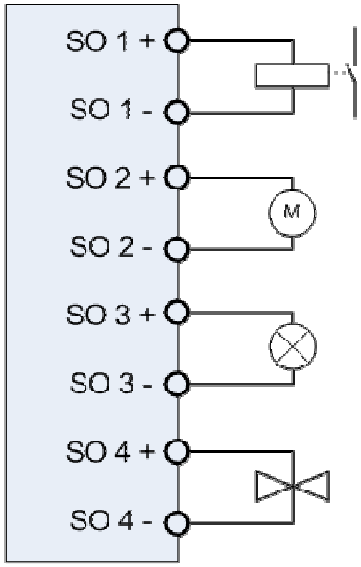


Fig. 34: Connection of safety actuators

Safety actuators (contactors, motors, muting lamps, valves) that are compatible with SO mode performance data may be connected directly.

Error	Error at	
	Open output	Assigned switch
Ground fault on SO x +	Not acknowledged	Acknowledged
SO x + shorted to 24V	Acknowledged	Acknowledged
Ground fault on SO x -	Not acknowledged	Acknowledged
SO x - shorted to 24V	Acknowledged	Acknowledged
Cross circuit between SO x + and the other signal (high)	Acknowledged	Acknowledged
Cross circuit between SO x – and the other signal (high)	Acknowledged	Acknowledged
Wire break	Not acknowledged	Not acknowledged
Cross circuit between SO x + and SO x -	Not acknowledged	Acknowledged

Note:

Potential error behavior of the actuators must be analyzed and prevented with the help of corresponding responses if necessary (forced read-back on a contactor, pressure switch in a valve).

Connection of ACOPOS and ACOPOSmulti (SIL 2, PL d, CAT 3)

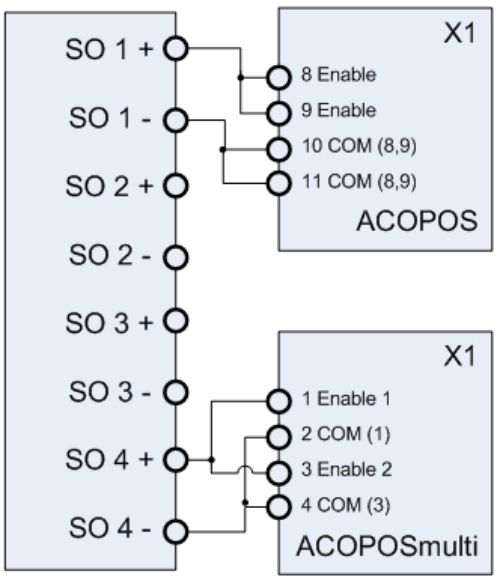


Fig. 35: Connections of ACOPOS and ACOPOSmulti CAT 3

The SO module can be directly connected to ACOPOS and ACOPOSmulti safety inputs.

Error	Error at	
	Open output	Assigned switch
Ground fault on SO x +	Not acknowledged	Acknowledged
SO x + shorted to 24V	Acknowledged	Not acknowledged
Ground fault on SO x -	Not acknowledged	Not acknowledged
SO x - shorted to 24V	Acknowledged	Acknowledged
Cross circuit between SO x + and the other signal (high)	Acknowledged	Not acknowledged
Cross circuit between SO x – and the other signal (high)	Acknowledged	Not acknowledged
Wire break	Not acknowledged	Not acknowledged
Cross circuit between SO x + and SO x -	Not acknowledged	Acknowledged

Note:

When interconnecting the SO modules with ACOPOS devices, the internal module test of the output wiring must be deactivated, otherwise the OSSD (Output Switching Sensor Device) gaps may cause unintended shut down of the ACOPOS device.

Caution:

Shutting off the internal module test results in reduced error detection. Consequently, all module channels are only used in SIL 2, PL d and CAT 3.

Connection of ACOPOSmulti (SIL 3, PL e, CAT 4)

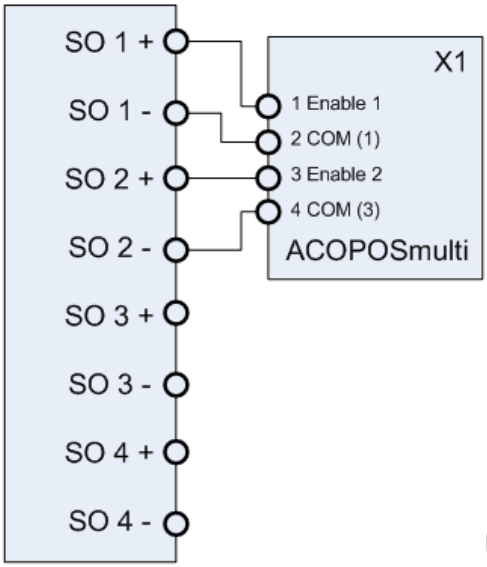


Fig. 36: Connection of ACOPOSmulti CAT 4

SO modules can be directly connected to ACOPOSmulti safety inputs.

Error	Error at	
	Open output	Assigned switch
Ground fault on SO x +	Not acknowledged	Acknowledged
SO x + shorted to 24V	Acknowledged	Acknowledged
Ground fault on SO x -	Not acknowledged	Acknowledged
SO x - shorted to 24V	Acknowledged	Acknowledged
Cross circuit between SO x + and the other signal (high)	Acknowledged	Acknowledged
Cross circuit between SO x – and the other signal (high)	Acknowledged	Acknowledged
Wire break	Not acknowledged	Not acknowledged
Cross circuit between SO x + and SO x -	Not acknowledged	Acknowledged

5.2.3 Safe Power

Safe Power modules (SP) supply successive X20 modules with I/O power.

Fig. 37: Safe Power (SP)

When module safety is required, the I/O power is shut off by the module. The devices connected to the successive X20 modules are switched off. This makes it possible to safely cut-off a potential group. This enables standard modules to be operated safely.

Caution:

- Clean organization of potential groups
- Well organized wiring

Note:

A maximum output value of 10 A is achieved.

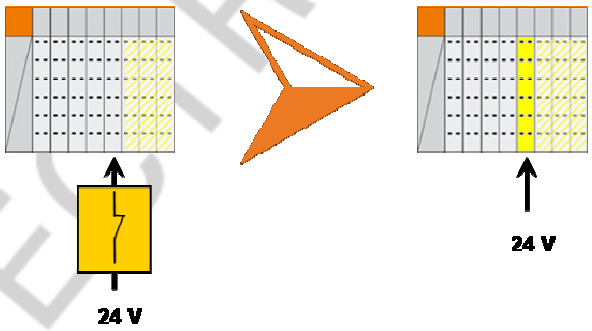


Fig. 38: Use of Safe Power module

5.3 SafeMC

Safe Motion Control (SafeMC) involves the **safety capabilities** of ACOPOS and ACOPOSmulti platforms.

Fig. 39: SafeMC

5.3.1 Standard safety technology

A **safe restart inhibit** in ACOPOS and ACOPOSmulti can be activated via the enable input (EN 954-1).

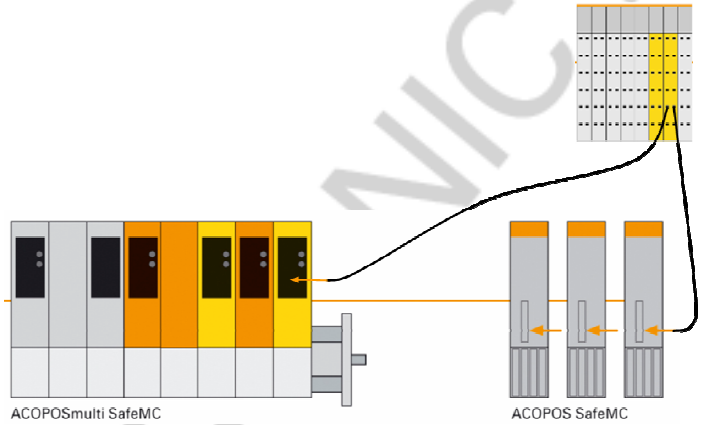


Fig. 40: Integrated restart inhibit according to EN 954-1

Note:

The OSSD (Output Switching Sensor Device) output monitoring must be deactivated in order to use an SO module with the ACOPOS enable input. This meet CAT 3 in accordance to EN-954-1.

5.3.2 Additional safety features

Additional safety functions are available for ACOPOSmulti. Functions such as safe limited speed are enabled directly via the network. Hard-wiring these safety-related signals to the drive is now a thing of the past. The information is transferred over the network using SafeLOGIC.

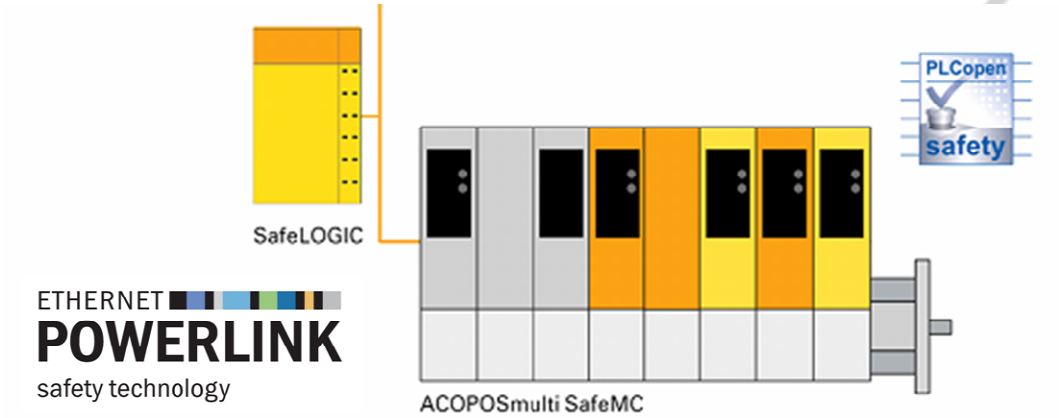


Fig. 41: Safe drive functions according to EN61800-5-2

According to EN61800-5-2, the following **safe drive functions** can be used when using the drive system:

- Safe Torque Off (STO)
- Safe stop 1 (SS1)
- Safe stop 2 (SS2)
- Safe Operating Stop (SOS)
- Safety-Limited Speed (SLS)
- Safe Brake Control (SBC)

Note:

An encoder is used for secure drive functions. This makes it possible to achieve secure drive functions SIL 2 according to IEC62061.

Safe Torque Off (STO)

"No power is fed to the motor that could cause rotation (or a movement in a linear motor) or these motors were shut off by the PDS(PR). The PDS(PR) does not provide power to the motor that could produce torque (or force in a linear motor) (IEC61800-5-2 2005, P. 16).

Caution:

In cases involving external influences (i.e. falling suspended load), further measures (i.e. mechanical brakes) may be required to prevent hazardous situations.

Safe Stop 1 (SS1)

"Either activation of the motor brake and monitoring (or controlling) the motor braking speed within predetermined limits for stopping the motor and activating the STO function when the motor is at standstill; or activating the motor brake and then the STO function after an application-specific time delay" (IEC61800-5-2 2005, p. 17).

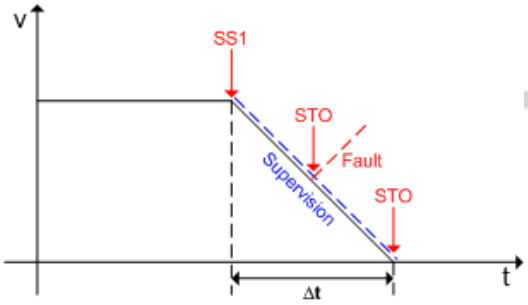


Fig. 42: Safe Stop 1

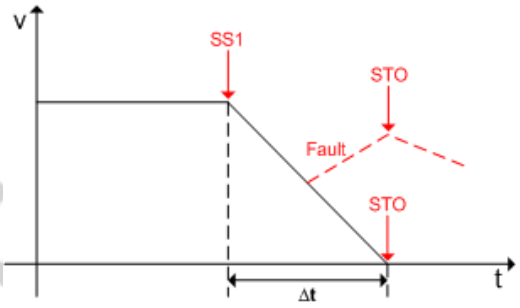


Fig. 43: Safe Stop 1

Safe Stop 2 (SS2)

"Either activation of the motor brake and monitoring (or controlling) the motor braking speed within predetermined limits for stopping the motor and activating the SOS function when the motor is at standstill; or activating the motor brake and then the SOS function after an application-specific time delay" (IEC61800-5-2 2005, p. 17).

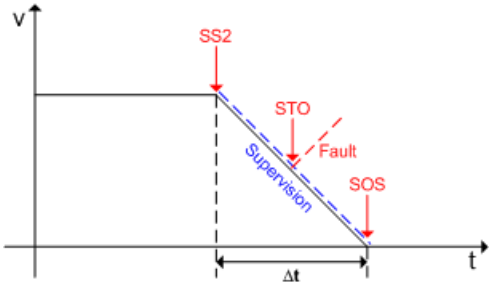


Fig. 44: Safe Stop 2

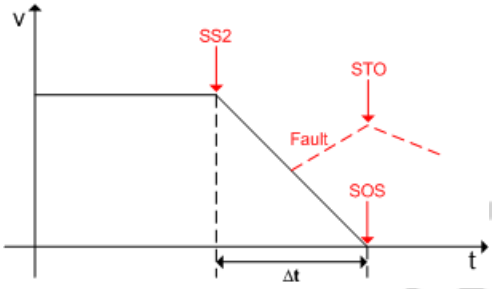


Fig. 45: Safe Stop 2

Safe Operating Stop (SOS)

"The SOS function ensures that the motor remains at a standstill and is not influenced by external forces" (IEC61800-5-2 2005, p. 17).

Safely-Limited Speed (SLS)

"The SLS function prevents the motor from exceeding the determined speed limit" (IEC61800-5-2 2005, p. 17).

Safe Brake Control (SBC)

"The SBC function delivers a safe output signal for controlling an external brake" (IEC61800-5-2 2005, p. 18).

Safe drive function	Safe encoder	
	Yes	No
Safe Torque Off (STO)		x
Safe Stop 1 (SS1) with monitoring of the motor braking speed	x	
Safe Stop 1 (SS1) without monitoring of the motor braking speed		x
Safe Stop 2 (SS2) with monitoring of the motor braking speed	x	
Safe Stop 2 (SS2) without monitoring of the motor braking speed	x	
Safe Operating Stop (SOS)	x	
Safety-Limited Speed (SLS)	x	
Safe Brake Control (SBC)		x

Note:

A user error (i.e. speed specified too high for the safe limit) also leads to system shut down (STO).

5.4 SafeLOGIC

The SafeLOGIC is the safe CPU that handles all central tasks. It is based on a single task system with cycle times under 1 ms.

The **memory medium** for the application, the module configuration, as well as the module parameters are stored on the **SafeKEY**. This is comparable to a CompactFlash and can be **exchanged during maintenance**, so the data can be made available very easily.

Fig. 46: SafeKEY

Fig. 47: SafeLOGIC

The SafeLOGIC covers three different functional areas:

- Configuration management
- Parameter management:
- Processing safety applications

5.4.1 Configuration management

Configuration management takes care of the **safety configuration** of the machine. The module type, hardware and firmware version are examined in order to determine whether or not modules are correctly inserted, are missing, or if new modules are present. Different firmware versions on a replaced module are automatically upgraded or downgraded so that they are compatible.

The hardware configuration is tested after booting and in cyclical intervals during operation.

5.4.2 Parameter management:

Parameter management ensures **parameter consistency** between the modules and the configuration. Module parameters can then be checked against application specifications. If necessary, parameter management carries out a complete parameter download, (i.e. if a new module is installed, then the corresponding parameters are transferred to the module).

5.4.3 Processing safety applications

In addition to testing the configuration and securing consistent module parameters, SafeLOGIC is also responsible for **cyclic processing** of safety applications stored on the SafeKEY.

5.4.4 Scalability of SafeLOGIC

SafeLOGIC Standard	SafeLOGIC Plus
Up to 20 safety nodes	Up to 100 safety nodes
Communication only with SafeLOGIC Plus version SafeLOGIC	Free communication with any other SafeLOGICs
Does not support machine options	Supports machine options

Note:

The SafeLOGIC Plus software versions can be exchanged with the SafeLOGIC Standard versions if the functions of the Plus versions are not needed.
In the same way, the SafeLOGIC Standard can be replaced by SafeLOGIC Plus.

5.5 SafeDESIGNER

The **SafeDESIGNER** is a toolset that must be installed in addition to Automation Studio. It updates Automation Studio with necessary engineering tools and functions for configuration of safety applications.

The safety-related functions are **completely encapsulated** and subject to an independent access rights management system.

A graphic editor for **configuration of safety applications** is the heart of SafeDESIGNER. Ladder diagram and function block programming are available for this. An effective separation of standard data and safety-relevant data makes distinguishing and separating signals easier for the user.

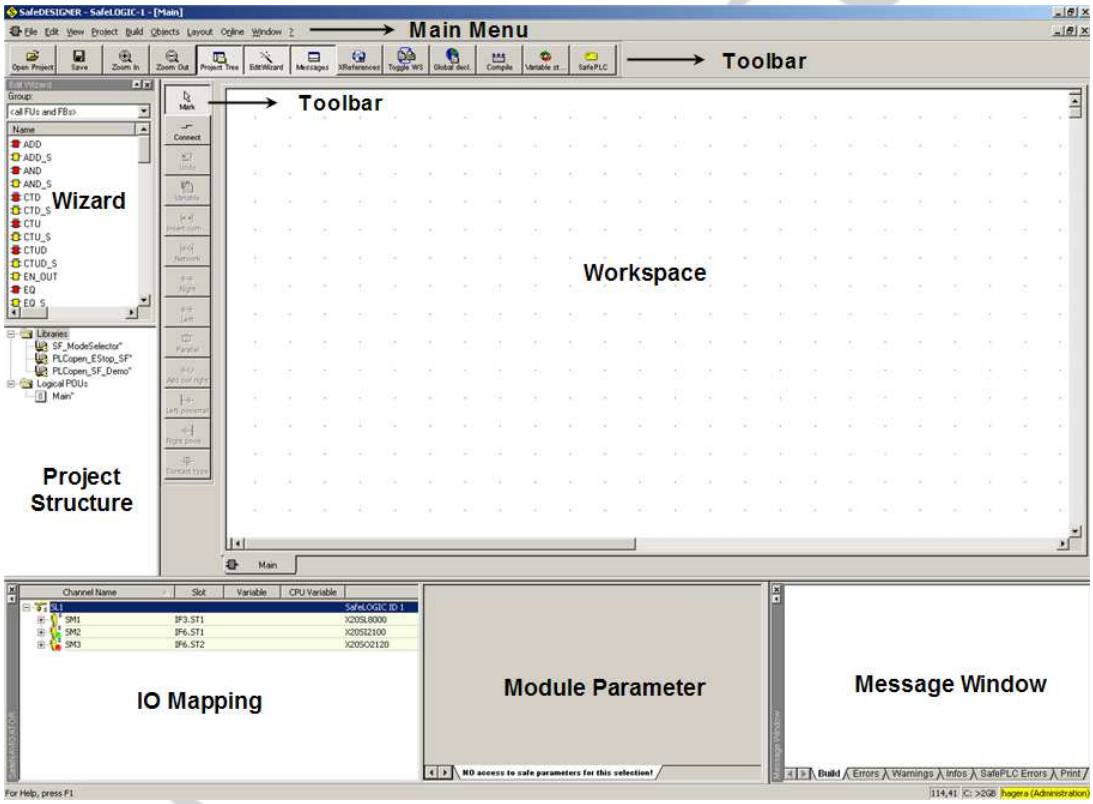


Fig. 48: SafeDESIGNER Overview

The Automation Studio user interface consists of the following elements:

- Main Menu
  The main menu offers access to all available functions.
- Toolbars
  The toolbars contain buttons that provide fast access to a wide selection of commands and functions.
- Wizard
  The wizard allows Drag & Drop addition of new function blocks in the desired positions.
- Project Structure
  The project structure displays the inserted libraries for the project as well as the different worksheets.
- IO Mapping
  Variables can be connected to the channels of safety-relevant modules using the IO mapping window.
- Workspace
  A graphic editor for configuring safety applications.
- Module Parameter
  This window is responsible for managing relevant security parameters. Reaction times that must be maintained for safety reasons and the use of machine options can be configured here. The access concept protects parameters from unauthorized or unintended changes.
- Message Window
  Delivers messages to the user.

5.5.1 Safety application programming

As mentioned above, a **graphic editor** is available for programming safety applications. The possible **programming languages FBK and LD** may be chosen freely or can also be mixed. Easy application development is possible using Drag & Drop and Copy & Paste functions. In the background, the system monitors the plausibility of the planned safety application.

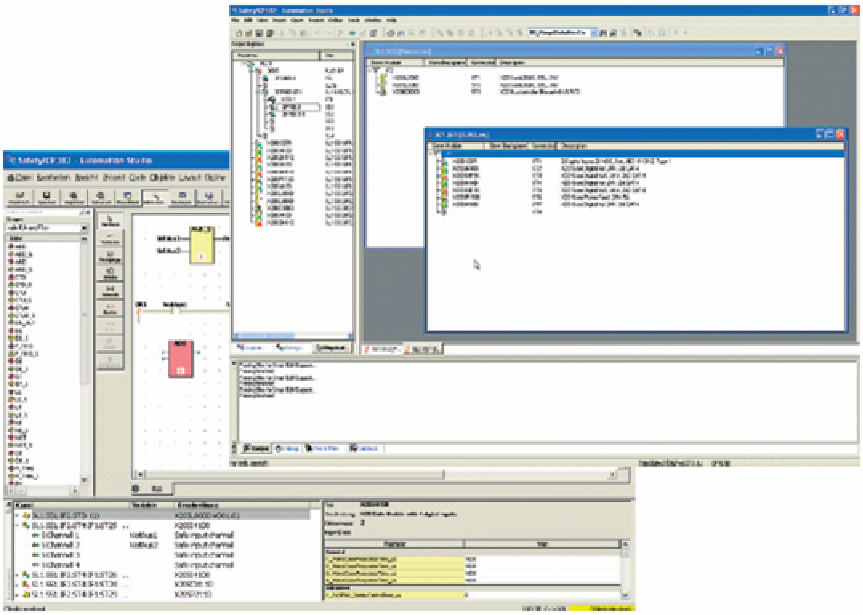


Fig. 49: Programming

With the use of the PLCopen Safety Library, the procedure more closely resembles **virtual wiring** than programming.

I/O data points make it easier for the user because more safety-relevant hardware modules are shown in SafeDESIGNER.

Transparent and non-reactive access to secure data in the standard application is a big advantage. Communication channels between the standard CPU and SafeLOGIC can also be configured to enable data exchange.

The application is processed by **two different compilers** in order to ensure the highest security.

With SafeDESIGNER, **documentation** and safety application version history can be **managed** simultaneously.

5.5.2 PLCopen Safety Library

The function blocks for safety-oriented applications standardized in the **PLCopen** package revolutionize the development of safety applications. All of the available **function blocks** are **certified** and reduce the complexity of the safety applications.

Fig. 50: PLCopen Safety Library

The PLCopen Safety Library can be divided into four main areas:

- Function blocks for sensors
- Function blocks for actuators
- Function blocks for muting
- Function blocks for motion

The function blocks for **sensors** involve:

- Equivalent
- Antivalent
- Mode selector
- Emergency stop
- Electro-Sensitive Protective Equipment (ESPE)
- Two-Hand Control Type II
- Two-Hand Control Type III
- Safety guard monitoring
- Testable safety sensors
- Enable switch

Fig. 51: Function block for emergency stop

The function blocks for **actuators** involve:

- Out control
- External device monitoring
- Safety request
- Safety guard interlocking with locking

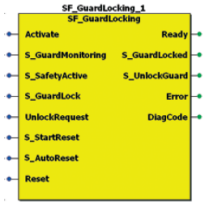


Fig. 52: Function block for safety door

The function blocks for **muting** involve:

- Sequential muting
- Parallel muting
- Parallel muting with 2 sensors

Fig. 53: Function block for sequential muting

The function blocks for **motion** involve:

- Safe stop 1 (SS1)
- Safe stop 2 (SS2)
- Safe Limited Speed (SLS)

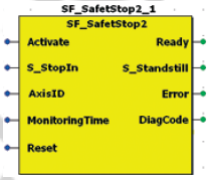


Fig. 54: Function block for SafeStop 2

6. COMMISSIONING AND SERVICE

During commissioning, the configured, safety-relevant hardware is compared with the inserted modules. The inserted hardware is then confirmed by SafeLOGIC and the **module type** as well as the **series number are saved**. This allows exchanged modules and module failures to be detected.

The following functions are available to technicians for commissioning a machine:

- Variable watch for testing sensor wiring
- Output forcing for easily checking actuator wiring
- Special "commissioning parameters" for the adjustment of safety applications for machine options

SafeDESIGNER has its own **start-up version**, in which the commissioning parameters may be changed.

Products that use integrated safety technology are equipped with extensive internal **diagnostic routines** to detect internal module errors as well as external wiring problems. Errors can be recognized by **Status LEDs** directly on the module or by analyzing the diagnostic data.

Fig. 55: Status LEDs

The X20 electronic module is removed and replaced when a **module is exchanged**. This exchange must be acknowledged by SafeLOGIC. It then automatically configures the newly inserted module. This prevents the possibility of incorrect configuration. This procedure is also executed when exchanging multiple modules. In addition, a wiring test is performed, which must also be confirmed by SafeLOGIC.

When **exchanging the SafeLOGIC** module, applying the SafeKEY from the defective device restores the safety application and all application-specific data.

7. SUMMARY

You are now familiar with the **B&R Integrated Safety Technology** concept and can apply it to your machines.

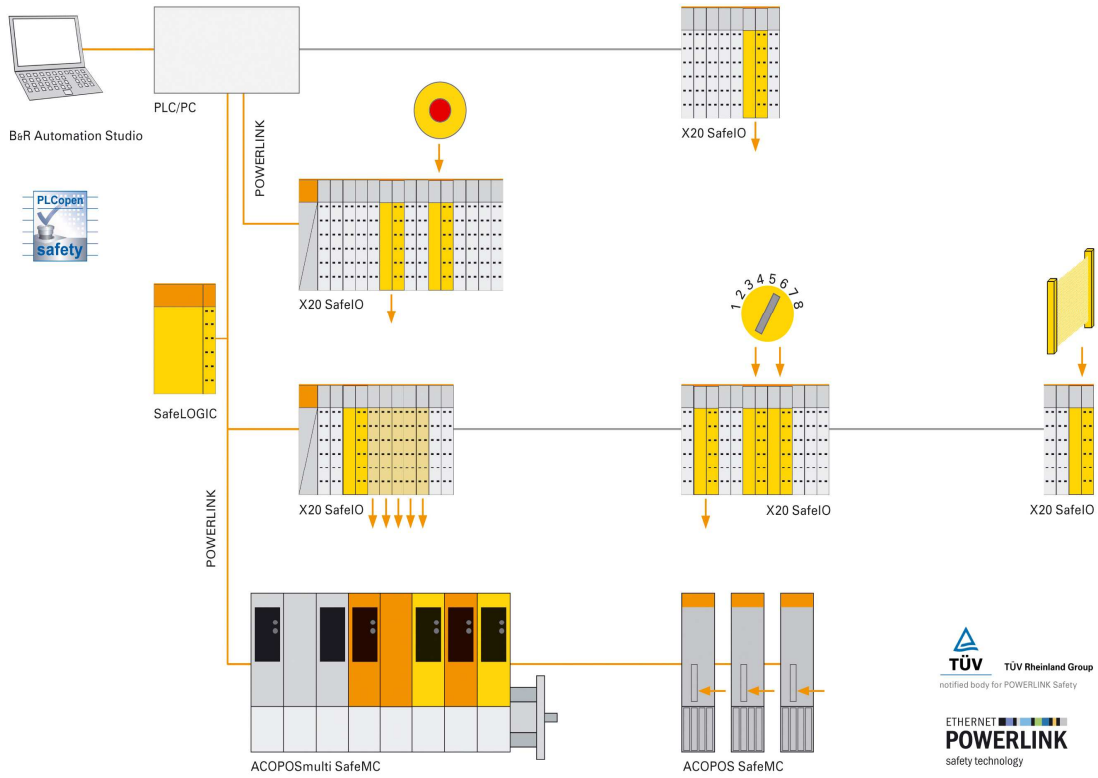


Fig. 56: B&R integrated safety technology

You also know that the available **safety components** can be optimally adjusted for your area of use. This ranges from the scaling of **SafeLOGIC**, to the use of **SafeIO modules** and the **SafeMC functions**.

You have had a brief look into the **POWERLINK Safety** bus system.

The **SafeDESIGNER** Toolset for Automation Studio allows you to create safety applications with the latest technology. The B&R philosophy "One Tool, Many Targets" is also applicable in safety technology.

You are now familiar with the **PLCopen Safety Library**, that can be used to simply and quickly configure your application through virtual wiring of certified function blocks.

Overview of training modules

TM200 – B&R Company Presentation **
TM201 – B&R Product Spectrum **
TM210 – The Basics of Automation Studio
TM211 – Automation Studio Online Communication
TM212 – Automation Target **
TM213 – Automation Runtime
TM220 – The Service Technician on the Job
TM223 – Automation Studio Diagnostics
TM230 – Structured Software Generation
TM240 – Ladder Diagram (LAD)
TM241 – Function Block Diagram (FBD)
TM246 – Structured Text (ST)
TM247 – Automation Basic (AB)
TM248 – ANSI C
TM250 – Memory Management and Data Storage
TM260 – Automation Studio Libraries I
TM261 – Closed Loop Control with LOOPCONR

TM400 – The Basics of Motion Control
TM410 – The Basics of ASiM
TM440 – ASiM Basic Functions
TM441 – ASiM Multi-Axis Functions
TM445 – ACOPOS ACP10 Software
TM446 - ACOPOS Smart Process Technology
TM450 – ACOPOS Control Concept and Adjustment
TM460 – Starting up Motors

TM500 – The Basics of Integrated Safety Technology
TM510 – ASiST SafeDESIGNER

TM600 – The Basics of Visualization
TM610 – The Basics of ASiV
TM630 – Visualization Programming Guide
TM640 – ASiV Alarm System
TM650 – ASiV Internationalization
TM660 – ASiV Remote
TM670 – ASiV Advanced

TM700 – Automation Net PVI
TM710 – PVI Communication
TM711 – PVI DLL Programming
TM712 – PVIServices
TM730 – PVI OPC

TM800 – APROL System Concept
TM810 – APROL Setup, Configuration and Recovery
TM811 – APROL Runtime System
TM812 – APROL Operator Management
TM813 – APROL XML Queries and Audit Trail
TM830 – APROL Project Engineering
TM840 – APROL Parameter Management and Recipes
TM850 – APROL Controller Configuration and INA
TM860 – APROL Library Engineering
TM865 – APROL Library Guide Book
TM870 – APROL Python Programming
TM890 – The Basics of LINUX

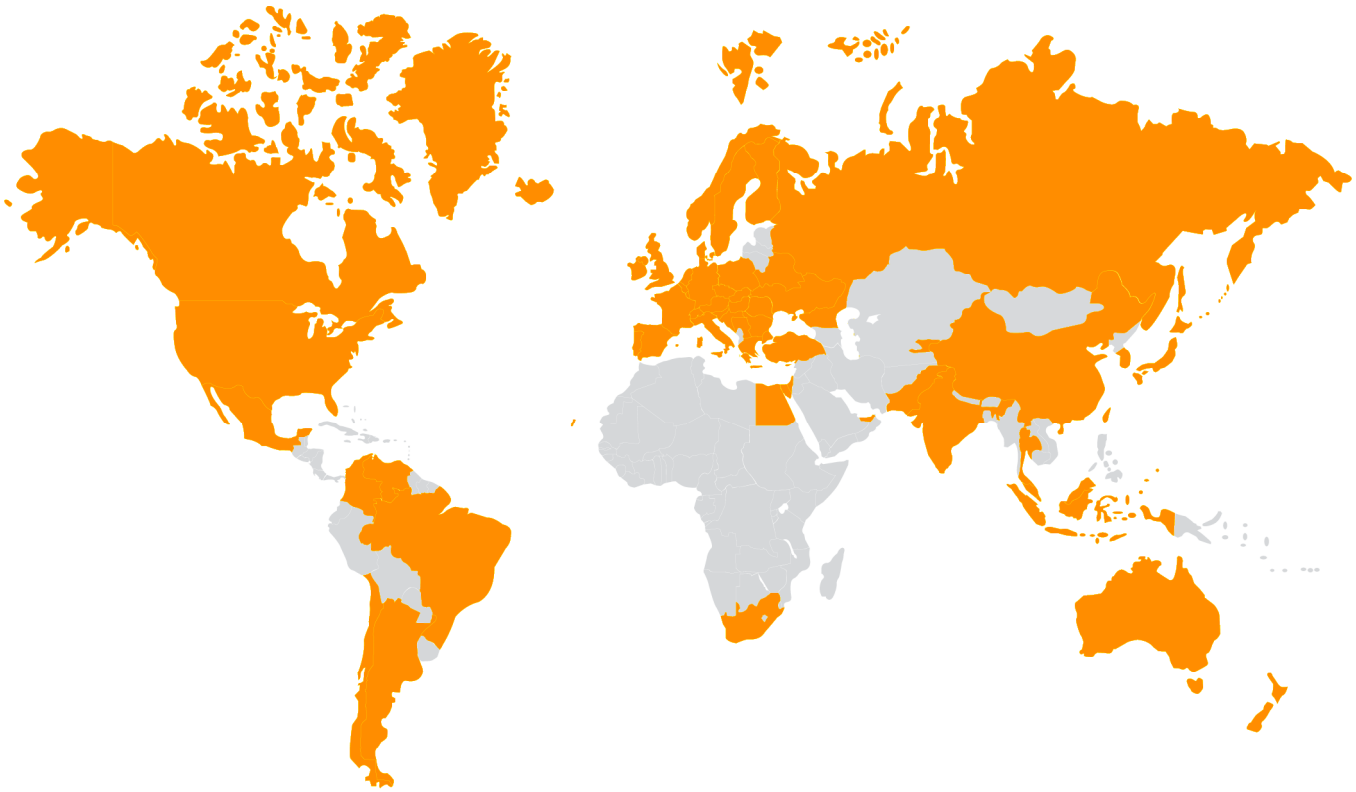
**) see Product Catalog

CORPORATE HEADQUARTERS

Bernecker + Rainer Industrie-Elektronik Ges.m.b.H.
B&R Strasse 1
5142 Eggelsberg
Austria
Tel.: +43 (0) 77 48 / 65 86 - 0
Fax: +43 (0) 77 48 / 65 86 - 26
info@br-automation.com
www.br-automation.com

TM500TRE.00-ENG 0208

140 offices in more than 55 countries - **www.br-automation.com/contact**



Australia • Argentina • Austria • Belarus • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Croatia • Cyprus
Czech Republic • Denmark • Egypt • Emirates • Finland • France • Germany • Greece • Hungary • India • Indonesia
Ireland • Israel • Italy • Japan • Korea • Luxemburg • Kyrgyzstan • Malaysia • Mexico • The Netherlands • New Zealand
Norway • Pakistan • Poland • Portugal • Romania • Russia • Serbia • Singapore • Slovakia • Slovenia • South Africa
Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • USA • Venezuela • Vietnam