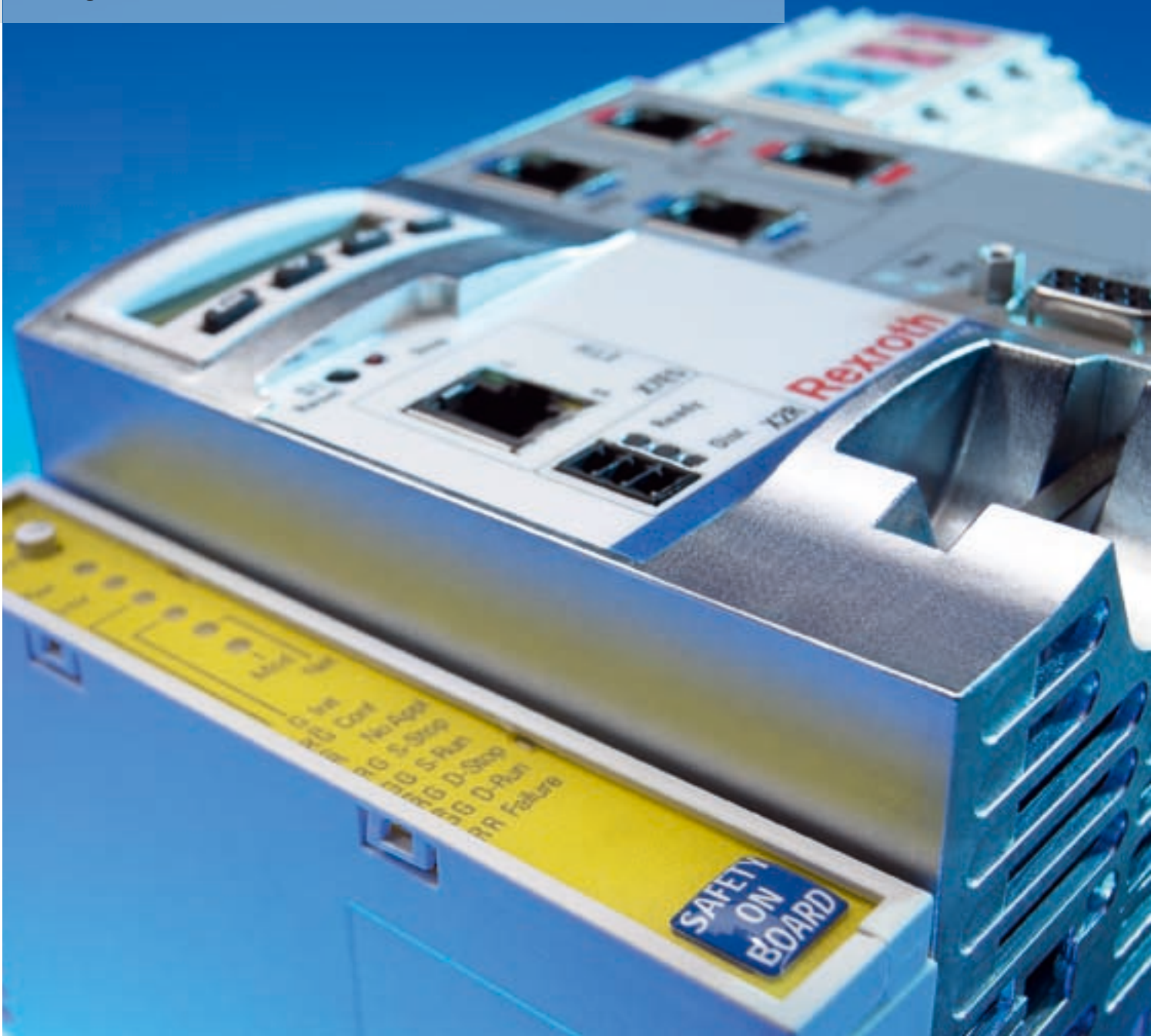


# Safety on Board Functional Safety in Automation Technology

Integrated, certified and consistent



# Safety on Board – integrated, certified and consistent

Whether the task involves machine tools, packaging and printing machines, assembly, handling or robot applications, the protection of personnel, machines and tools is absolutely paramount. In order to meet these expectations, modern safety concepts have to comply with demanding requirements such as “safe motion”, “safe processing of peripheral signals” and “safe communication”. Safety on Board from Rexroth meets all these requirements and is a synonym for well thought-out and intelligent safety solutions from the Automation House.



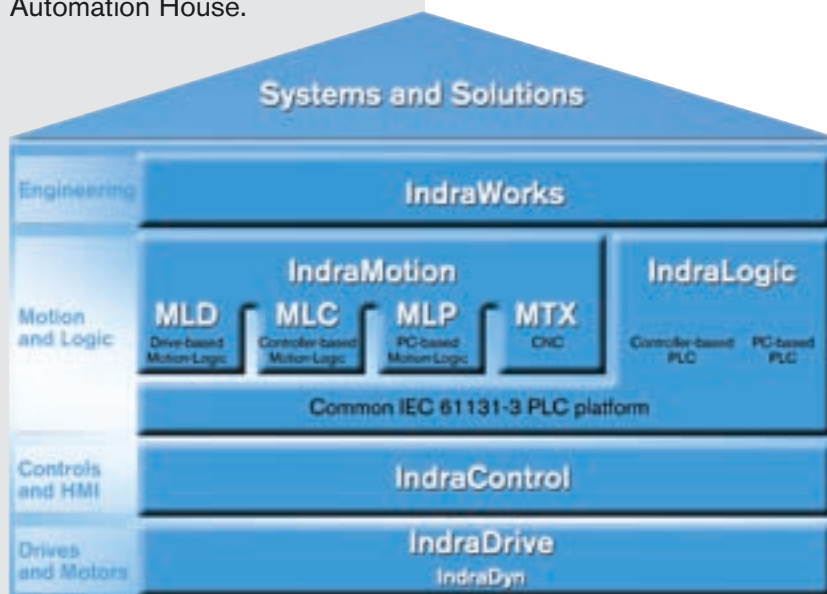
SafeMotion, the drive-based safety solution from Rexroth, means much more than just the “safe stop”

of machinery. Rather, SafeMotion is the first step in the realization of safe machine concepts. SafeMotion allows the operator to have access to the process without danger, increases availability by reducing downtimes and therefore increases productivity.



SafeLogic, the controller-based safety solution from Rexroth, replaces inflexible wired safety

relays with flexible, programmable safety software. With the consistent IndraWorks engineering framework, the system of processing signals from peripherals can be quickly and easily adjusted to a wide variety of machine concepts. SafeLogic can help to reduce start-up and validation times drastically, while a high-performance diagnostics tool delivers guaranteed maximum plant availability.



Our Automation House is a unique modular toolkit which gives you everything you need to create leading-edge automation solutions. From drive and control systems to the high-performance software framework for standardized engineering and user-friendly operation. This innovation gives you all the privileges associated with modern automation technology – integration, intelligence and investment for the future.

### **Integrated**

Maximum protection for personnel, reduced downtime, increased availability and simplified start-up and validation – these are just some of the advantages of integrated safety technology from Rexroth. By integrating safety functions in standard components, we upgrade them to full-fledged safety components. These can be used as stand alone components or as part of our system solutions.

### **Certified**

Safety on Board provides the machine manufacturer with a guarantee of maximum safety and reliability on the basis of components and system solutions which are tested and certified in accordance with the latest safety standards. This minimizes the cost and effort involved in the validation of plant and machinery and gives the manufacturer assurance – both in functional and legal terms.

### **Consistent**

From the drive to the controller – SafeMotion and SafeLogic merge perfectly to form a comprehensive safety concept. To enable safety data to be exchanged between the controller and the drive, SERCOS has been extended to include the CIP Safety based SERCOS safety protocol. The control communication system transfers both standard data and safety data, eliminating any other interfaces and offering major potential for savings.

The standardized IndraWorks engineering framework for configuration, programming and diagnosis increases plant availability and drastically cuts start-up times.

### **Safety on Board –**

**From the drive to the control system, Rexroth offers safety solutions that can be optimally scaled.**



Safety peripherals can be integrated with the help of SERCOS safety or PROFIsafe - either directly or via safe I/O modules. This makes SafeLogic the first safety controller to support two safety protocols simultaneously.

It goes without saying that SafeMotion is also available as a stand alone component. The drive-integrated safety technology is capable of being integrated in every kind of system architecture via discrete, two-channel control systems or safe bus systems.

# SafeMotion – Safe stop and more



**Safe drive technology from Rexroth means more than just safe stopping.** Above all it is safe motion functions that give you the means of protecting your personnel effectively, increasing productivity and realizing new safety concepts.

Whenever operators have to work inside the machine either for commissioning purposes or for process-related reasons, it is a requirement of the Machinery Directive that the machine manufacturer has made provision for special safety precautions, because any uncontrolled movements can be a danger for persons in the event of a malfunction. Rexroth has these malfunctions fully under control and as a pioneer of drive-integrated

safety technology, with many years of experience in the field. “Safety on Board” was introduced to the market by Rexroth as early as 1999 and has been continually expanded with the addition of further functions ever since.

### Expanded range of functions

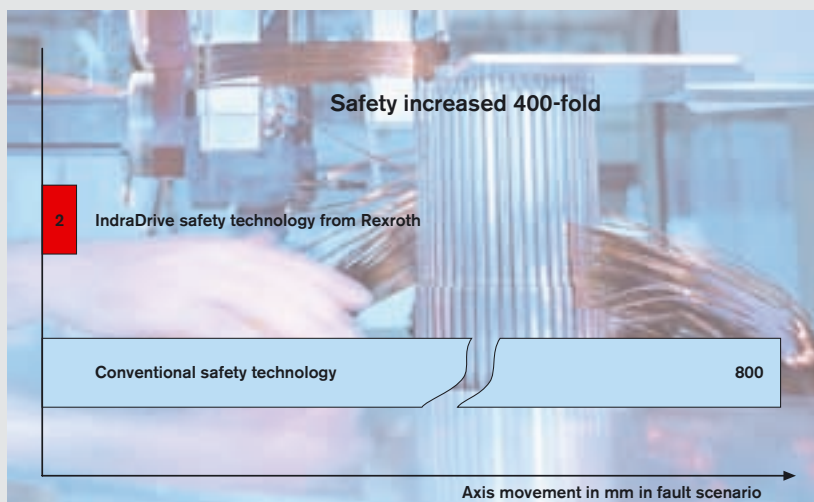
In addition to the traditional safe stop and motion functions, IndraDrive also supports more than 18 safety functions, such as

safety door locking, various safely limited positions and a safe braking and holding system to prevent vertical axes from falling.

### Convincing advantages:

- Increased machine productivity as a result of shorter special mode times
- No unnecessary idle times because the line circuit breaker does not have to be opened
- No need for re-synchronization of coupled axes
- High reliability thanks to certified and integrated safety functions
- Savings on limit switches, measurement and analysis units and control cabinet size
- Reductions in time and money spent on certification
- Online-self-monitoring instead of forced offline-checking-procedure, i.e. no periodic machine shutdown needed for fault detection

### Axis movements minimized thanks to ultra-short response times

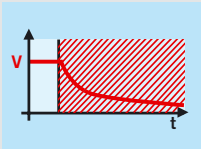


Before a user in the protected area reacts to an error with an acknowledgement linked to contacts, a linear axis with a ball screw has already traveled 100 to 200 mm,

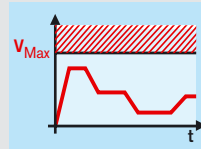
linear motors have already traveled 400 to 800 mm. IndraDrive safety technology finds the error within 2 ms and the axis moves only 2 mm.



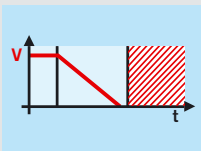
# SafeMotion – Certified safety functions



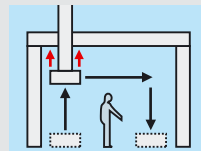
**Safe Torque Off (STO)**  
Safe Torque Off  
Stop category 0 in accordance with IEC 60204-1:  
Safe drive torque cut off



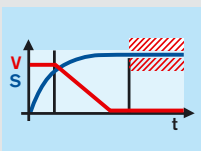
**Safe Maximum Speed (SMS)**  
The maximum speed is safely monitored irrespective of the mode of operation.



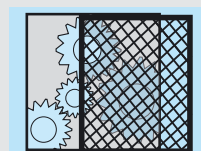
**Safe Stop and Safe Drive Interlock (SS1)**  
Safe Stop 1  
Stop category 1 in accordance with IEC 60204-1:  
Safely monitored stop, control or drive controlled with safe drive torque cut off



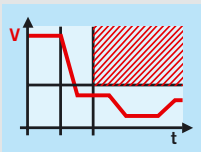
**Safe Braking And Holding System (SBS)**  
The safe braking and holding system controls and monitors two independent brakes



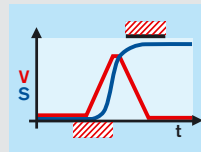
**Safe Operating Stop (SS2, SOS)**  
Safe Stop 2, Safe Operating Stop  
Stop category 2 in accordance with IEC 60204-1:  
Safely monitored stop with safely monitored standstill at controlled torque



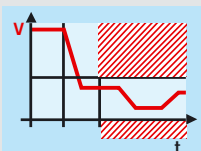
**Safe Door Locking (SDL)**  
When all the drives in one protection zone are in safe status, the safety door lock is released



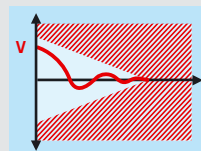
**Safely Limited Speed (SLS)**  
If enable signal is given a safely limited speed is monitored in special operating mode



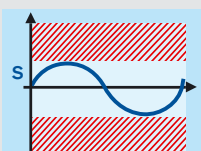
**Safely Limited Increment (SLI)**  
If enable signal is given a safely limited increment is monitored in special operating mode



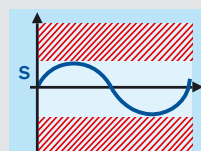
**Safely Monitored Direction (SDI)**  
A safe direction (clockwise, counterclockwise) is also monitored in addition to safe motion



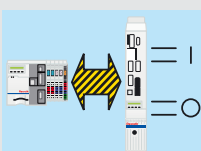
**Safely Monitored Deceleration (SMD)**  
Safely monitored deceleration ramp when stopping



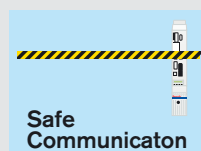
**Safely limited Position (SLP)**  
A safely limited position range is also monitored in addition to safe motion



**Safely Limited Position Switch (SPS)**  
Monitoring of safe software limit switches



**Safe Inputs/Outputs (SIO)**  
Dual-channel safety peripherals can be connected to the drive and made available to the controller via the safety bus



**Safe Communication (SCO)**  
Selection/deselection of safety functions and transfer of process data (e.g. actual position values) via safety bus

All safety functions are certified as compliant with standards ISO 13849-1:2006 <sup>1)</sup>, IEC 61800-5-2:2007 <sup>1)</sup>, IEC 61508:1998-2000 <sup>1)</sup>, IEC 62061 <sup>1)</sup>, ISO 13849-1:1999, EN 954-1:1996, ISO 13849-2:2003, IEC 60204-1:1997, EN 50178-1:1997, IEC 61800-3:2004, UL 508C R7.03, C22.2 No. 0.8-M86 (R2003), CAN/CSA C22.2 No. 14-95, NFPA 79:2007 ER1 through TÜV Rheinland, TÜV Rheinland North America Inc. and SIBE Switzerland. <sup>1)</sup>Currently in preparation

# SafeMotion – Fast, autonomous, reliable



## Fast

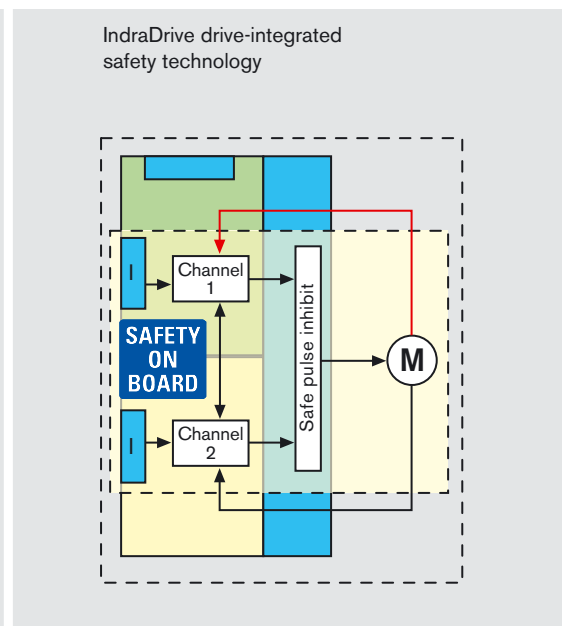
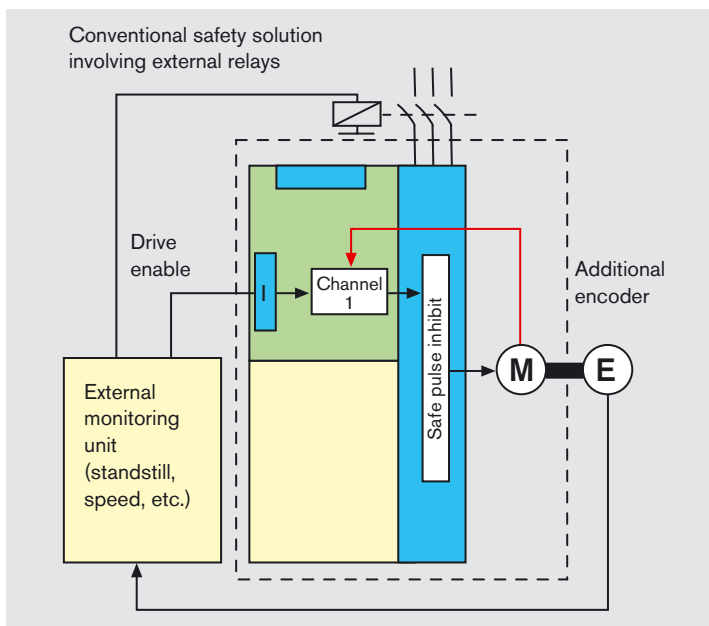
The drive-integrated safety technology in IndraDrive monitors movements where they are generated. The results are very rapid response times of just 2 ms upon triggering of the internal monitors. This is particularly important for high-dynamic drives because otherwise there is a risk of impermissibly large residual distances. The drives remain in position control during any intervention work on the machine, which eliminates the need to disconnect from the mains power supply and re-synchronize coupled axes. Reducing these special mode times leads to significant improvements in plant productivity.

## Stand alone

IndraDrive with integrated safety technology can be used as a stand alone component because two redundant and diverse monitoring channels are directly integrated in the drive. The safety peripherals such as mode selectors or enable switches, for example, can be connected directly to the drive so that the safety functions can be switched active. In contrast to conventional safety technology there is no need for additional external measurement and monitoring devices. This results in space-saving, low-cost solutions.

## Reliable

The safety functions in IndraDrive are tested by independent certification bodies and are compliant with the latest safety standards. You can rely on the certified safety of IndraDrive and therefore reduce the need to organize certification yourself. Since the complete monitoring system is integrated in the drive you can be sure of maximum safety without possibility of tampering.



**Simple start-up**

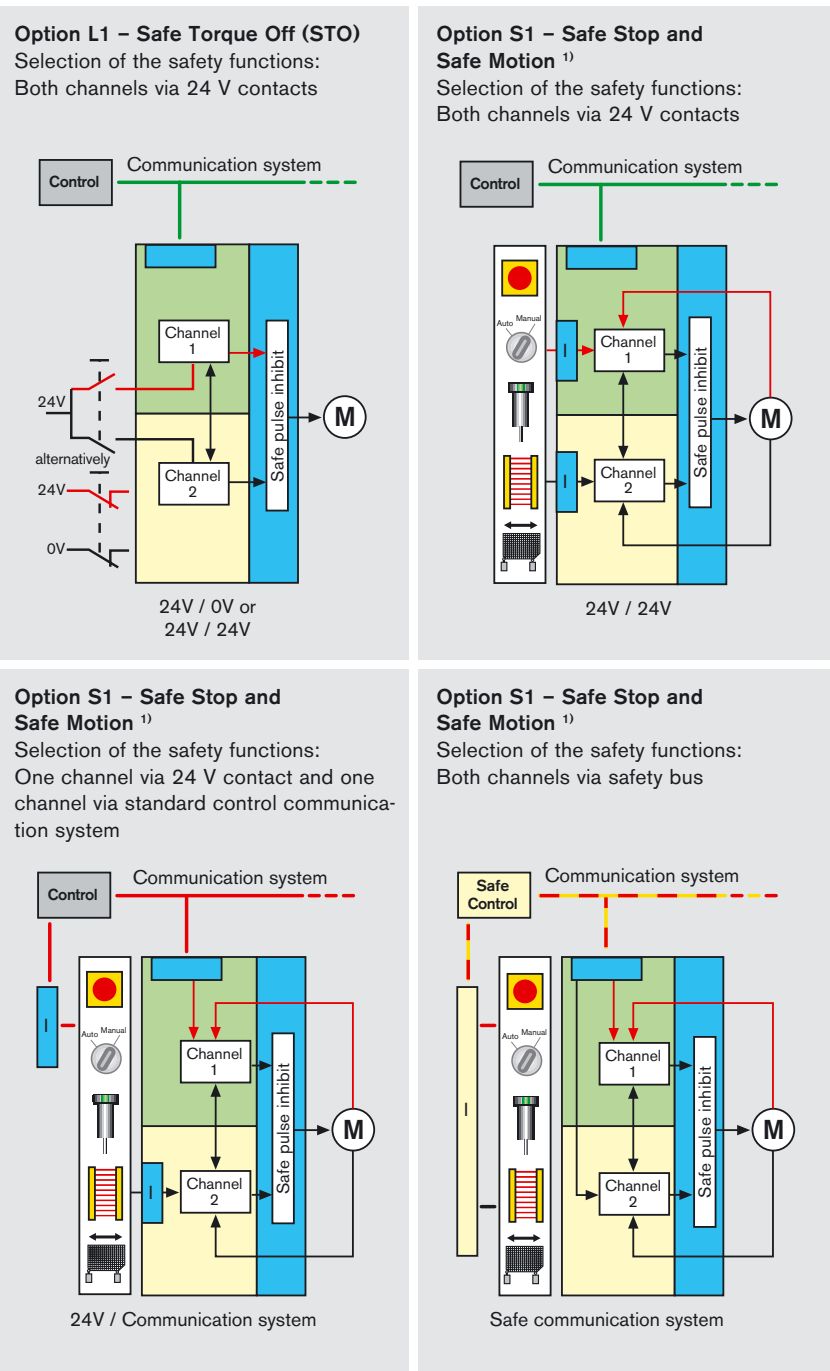
The safety parameters – such as a monitored, limited speed, for example – are parameterized in a simple menu-guided start-up procedure. With removable memory cards, reproducing the safety parameters in series production machines is simplicity itself, as is re-importing whenever a switch of drive controller is made.



**Simple service handling**

For servicing, the safety parameters are simply imported to a new device. All that has to be checked is the identification of the drive (manufacturer, machine type, axis). There is no need for the validation procedures to be repeated again on-site.

**There are different ways in which the dual-channel selection of the required safety functions in the drive can be realized:**



<sup>1)</sup> IndraDrive drives with Option S1 support all the safety functions shown on page 5.

# SafeMotion – The safe braking and holding system

Rexroth is the first company in the world to integrate a safe braking and holding system in its drives for preventing vertical axes from crashing. This redundant concept provides maximum safety even after the power has been shut off.



Personnel frequently have to carry out work in the machining areas of plant and machinery – be it for commissioning, rectifying faults or as part of process optimization. Particular caution is required here if any axes are under the load of gravitational force in the area of access. Vertical or inclined axes can be a danger in particular when disconnected from the power supply because of the risk of falling unintentionally. Possible causes include holding brakes that are soiled, oily or damaged as a result of mechanical wear, or faults in the brake controls.

The Rexroth safe braking and holding system provides protection against such dangers through three independent channels – sensing the motor torque and two redundant brakes.

## Safety for man and machine

- Certified in accordance with EN 954-1, Category 3 for maximum safety
- Prevents axes under the load of gravitational force from falling
- Lightning response in the event of a malfunction thanks to drive-integrated monitoring
- Two independent brakes – separately controlled and monitored
- Redundant holding of the vertical axis even after the power supply has been switched off, e.g. in the event of an emergency switch-off or emergency stop
- Escalation strategy with graduated impact of the three braking forces minimizes the stress on the mechanical system
- Open for various different electrically released brakes – can also be installed on the load-side





### Open for different brake systems

Different machines use different brake systems, which is why the safe braking and holding system is open and can also integrate products from other suppliers with ease. It is even possible to use hydraulically or pneumatically actuated rod or guide rail brakes.

Both brakes have to be released electrically and comply with the specification for the control signals. For motors with housings the holding brake integrated in the motor is normally used as the first brake. The second brake takes the form of a brake fitted either directly to the motor flange or to the transmission exit end or on the load-side. This offers the advantage of ensuring that any failures in mechanical transmission elements are also reliably controlled as well. For direct drive motors, underlying principles mean that only load-side

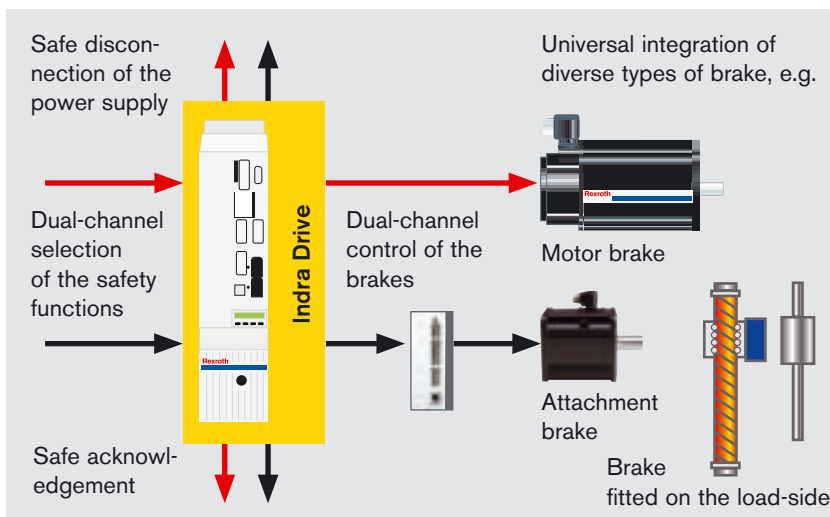
brakes can be used. The second channel brake control is provided by an external control unit monitored by the drive. There are no safety-specific requirements for the individual brakes.

### Detecting dormant faults

To detect dormant faults (e.g. oily holding brakes) the brakes have to be tested at regular intervals. First the current load torque caused by the gravitational force has to be determined.

The brakes are then applied in sequence and subjected to a load from the drive in both directions, the load in each case being 1.3 times the maximum weight load of the application. At the same time the positional information is monitored by two channels on the basis of a parameterizable tolerance range. An “overrunning” axis, caused for example by an oily

brake, would be reliably detected and intercepted by this solution. Once both holding systems have successfully passed the brake test, the internal brake status for a parameterizable time is set to “Ok”. Within this time it will be permissible to enter and remain in the area beneath the vertical axis without the need for a new brake test.



The safe braking and holding system is based on two independent brakes which are separately controlled and monitored by the redundant and diverse channels in the drive.

# SafeLogic – Safe logic processing simply programmed

**SafeLogic from Rexroth – programmable, functional safety up to SIL 3, certified in accordance with IEC 61508.**

As an integral component of standard control systems it allows the user to program both standard and safety applications together on a control system with the same IndraWorks engineering tool. The applications are completely decoupled from each other so that any changes to the standard application have no influence on the safety application.

## Functional principle

SafeLogic is available for controller and PC-based control systems. This involves upgrading standard control systems with an optional function module. This function module provides all the resources required for safe logic processing.

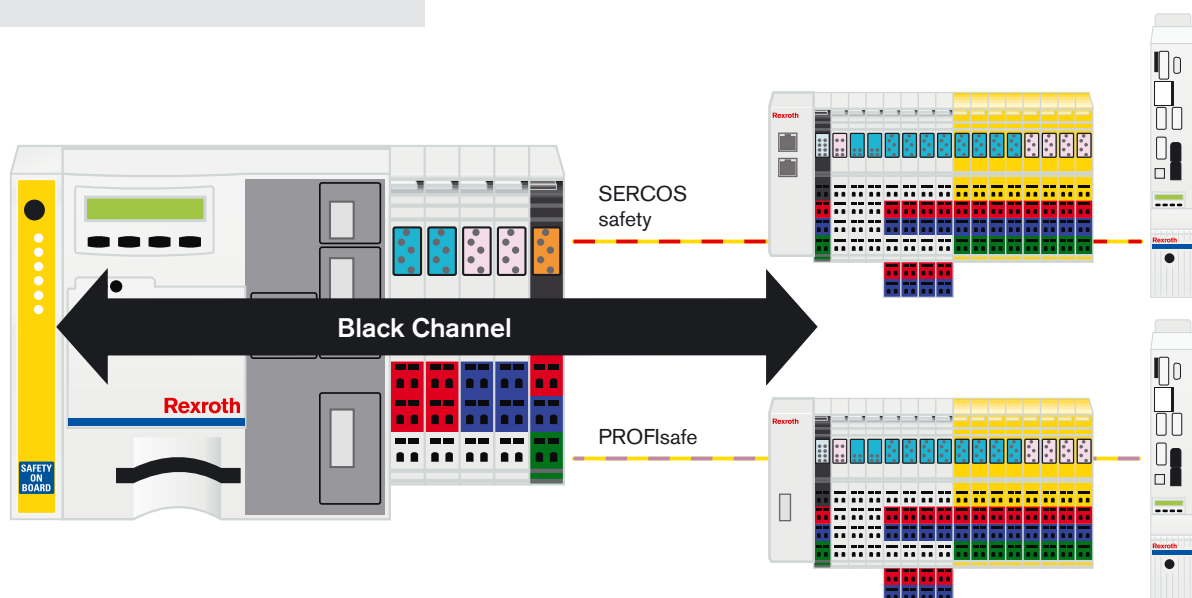
The information exchanged between the participants in a data connection, i.e. between the producer and the consumer, is exchanged in the form of safe data telegrams. If the consumer determines that the received data is incorrect or if there is an error in transmission, it switches to a predefined, safe error status.

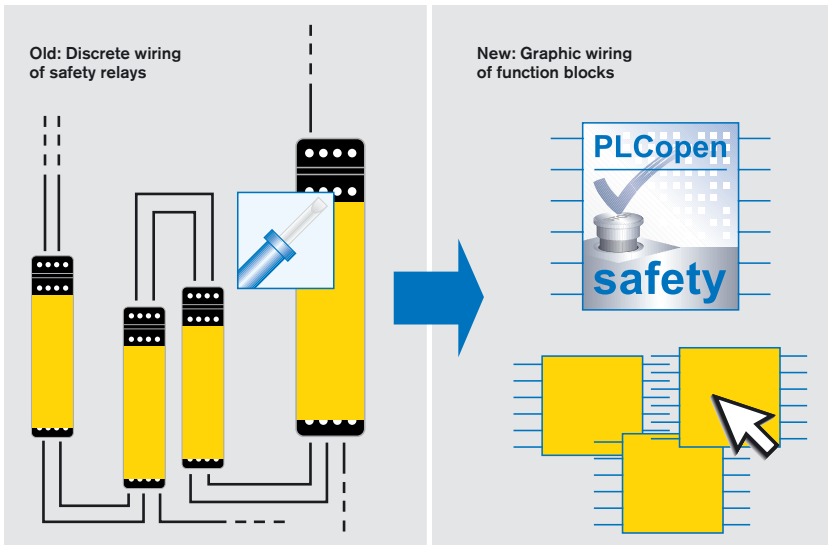
The transmission path therefore becomes a “Black Channel” and has no impact on safety – irrespective of the medium or transmission path selected.

## Communication

For the communication interface it is possible to use either the SERCOS and/or PROFIBUS interface on the standard controller. Both networks are run simultaneously and serve both the standard and the safety components in a mix.

To this end, not only is SERCOS safety supported but the PROFIsave V2 protocol for connecting intelligent third-party safety components as well.





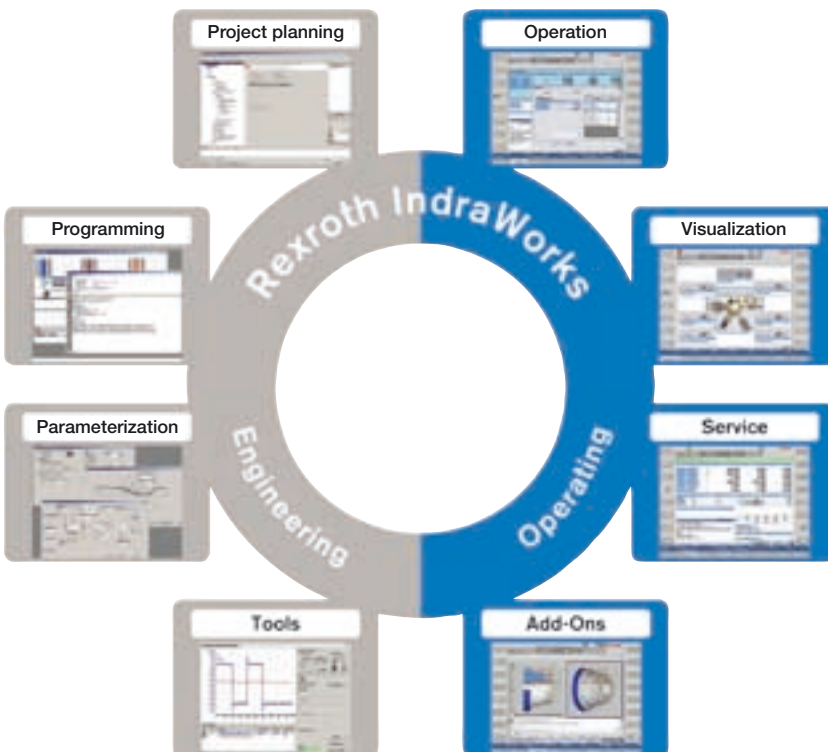
### Programming

The safety application is created with the IndraWorks SafetyManager. Programming is in accordance with the principles of the PLCopen-Safety specification. The principle is that the programming is configured along similar lines to the wiring of discrete safety relay. Certified function modules take the place of the relay and graphic connections (programming) between the function modules replace the discrete wiring.

At an organizational level a distinction is made between two user groups:

- The basic level user only connects up the function blocks along the same lines as the discrete wiring. The resultant program reduces to a minimum the cost and effort involved in the validation process.
- For the extended level user the more extensive functionality allows user-defined function blocks to be created.

However, the effort involved in the validation of these function blocks is considerably higher. On the other hand, once they have been verified they are suitable for use in the basic level, with the aforementioned advantages. This therefore provides a simple means of implementing organizational measures associated with functional safety management.



# SafeLogic – Safe peripherals without limits

**Safe peripherals are integrated via the standard bus systems SERCOS III and PROFIBUS DP, with PROFINET IO to be available in the future as well.** When used together with the controller-based IndraControl L, safe I/O modules can be integrated directly via the local bus – with any order of standard and SafetyIO modules possible.

## Safe interlinked machinery

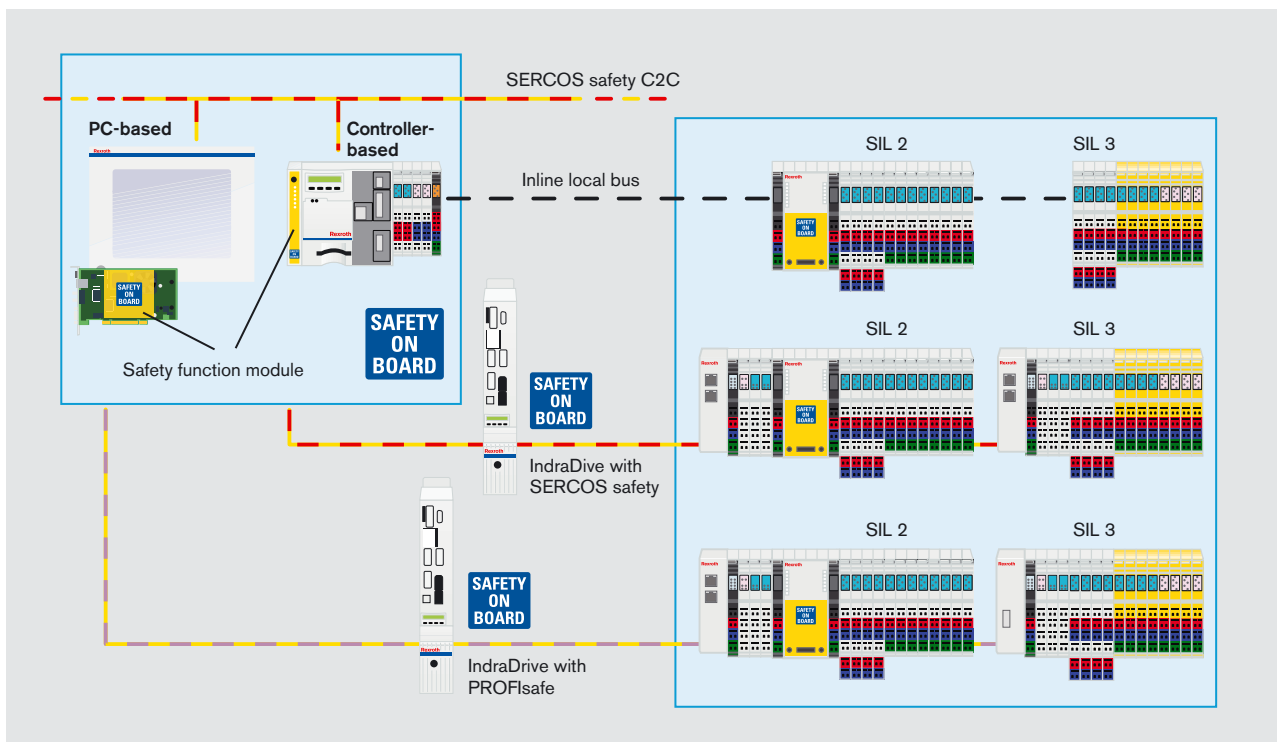
The safe exchange of data between the individual safety controllers for machine linkages is also via SERCOS safety and the C2C transport mechanism of SERCOS III.

## Safe drive technology

The IndraDrive drive-integrated safety technology can be integrated in networks via SERCOS III for interpolation drives. It is also possible to integrate drives in positioning block mode via PROFIBUS DP, with integration via PROFINET IO also available in future as well.

## Safe inputs and outputs

To meet requirements for safety integrity, Rexroth Inline SIL 2 and SIL 3 SafetyIO modules are available for safety peripherals signal inputs and outputs. The I/O modules can be run on SERCOS, PROFIBUS DP and the local bus regardless.

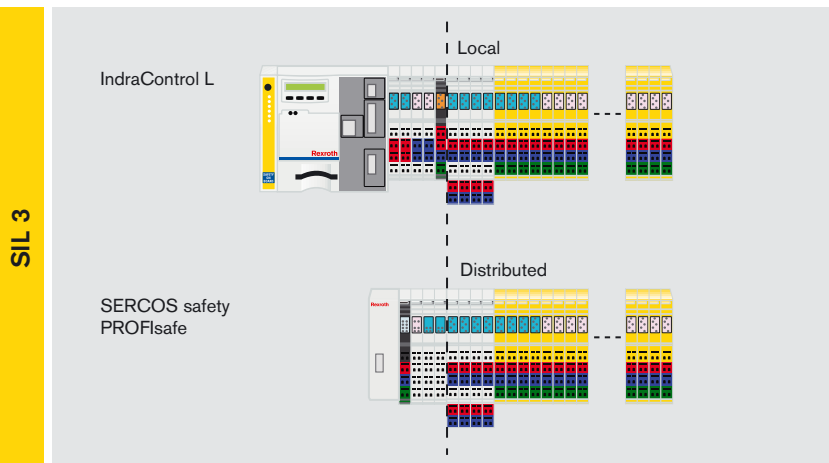
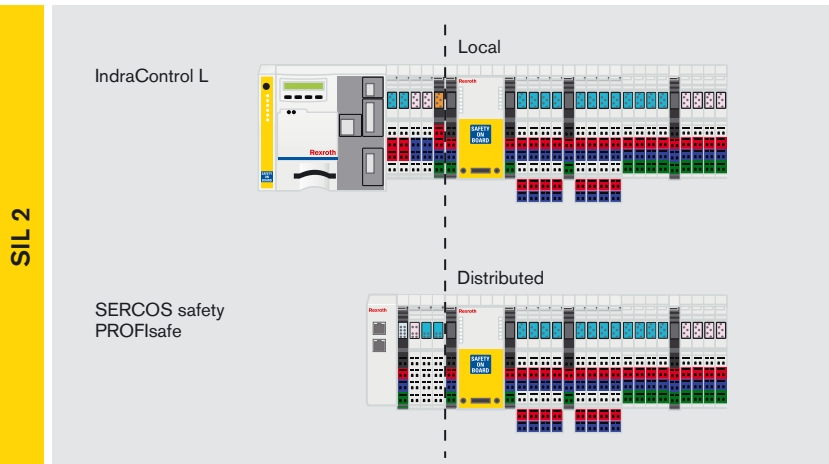




## SIL 2

For SIL 2 requirements (PL d) the Rexroth Inline DI8, DI16 and DO8 standard I/O modules can be used. A SafetyIO converter containing all the safety-related measures is positioned upstream of the “safe” I/O modules. Here, one SIL 2 input is generated from input channels assigned in pairs to two standard input modules. The required test pulses can be directly picked off the module. Both mono and complementary NC and NO combinations can be connected.

All stuck-at faults and crossover faults are detected. A SIL 2 output is designed in such a way that one physical output can be used to switch two redundant contactors. The contactor is monitored directly in the SafetyIO converter via the self-monitoring external device monitoring inputs.



### The advantage

This offers average savings of 40% compared to SIL 3 modules, depending on the expansion option. The range of types is also reduced since they are used as standard modules as well.

### SIL 3

The requirements of SIL 3 (PL e) apply only in exceptional cases. Rexroth Inline supplies special SIL 3 SafetyIO modules for these applications.



# SafeLogic – Technical data



Safety function module		
Platform	IndraControl L	20 x 120 x 70 mm (W x H x D)
	IndraControl P	PCI-format
Protocols	SERCOS safety	yes
	PROFIsafe V2	yes
Number of safety participants		64
Telegram memory		max. 2 kByte
Fail-safe I/O		> 500
Cycle times	Processing time per 1k of instructions	0.5 ms
	Protocol cycle time	min. 1 ms
	Safety cycle time	type 10 – 30 ms
Ambient conditions		5 – 55 °C
Voltage supply		internal

SIL 2 SafetyIO converter		
SafetyIO converter per station		1
Interfaces	PROFIBUS DP	yes
	SERCOS III	in preparation
	Local bus (Rexroth Inline)	in preparation
Digital inputs	SIL 2-channels (PL d/Cat. 3)	max. 32
	Test signals	2
Digital outputs	SIL 2-channels (PL d/Cat. 3)	max. 16
	Output current	0.5 A
Device monitoring		16
Filter groups		4
Discrepancy time groups		4
Group switch-off		yes
Ambient conditions		5 – 55 °C
Voltage supply		24 V (max. 8 A)
Current load	Actuator supply	6 A
	$U_{T1}, U_{T2}$	0.7 A each
	$U_L$	260 mA

SIL 3 SafetyIO module		
Input channels	SIL 2-channels (PL d/Cat. 3)/SIL 3-channels (PL e/Cat. 4)	8/4
	Cycle signals	2
Output channels	SIL 3-channels (PL e/Cat. 4)	8
	Output current	2 A
Ambient conditions		5 – 55 °C

# SERCOS safety – for safe communication worldwide

Safe data transmission up to SIL 3 in accordance with IEC 61508 – SERCOS safety combines the advantages of the SERCOS III Ethernet-based communication system and the internationally established safety protocol CIP Safety. This permits real time, safety and standard IP data to be exchanged via the same medium and beyond the boundaries of individual networks. CIP Safety offers worldwide market acceptance and allows interoperability between CIP Safety-based networks and components.

**SERCOS safety means:**

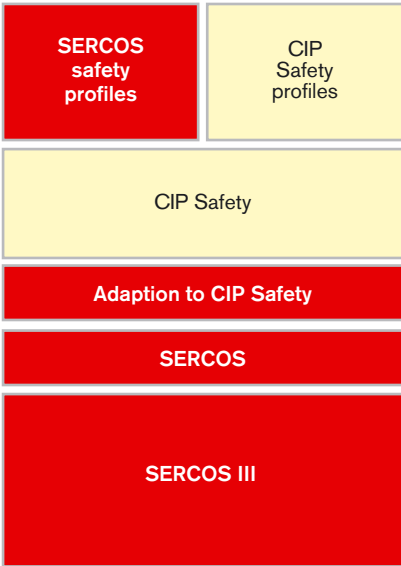
- The use of the CIP Safety <sup>1)</sup> mechanisms for protocol security
- Adaptation of SERCOS on CIP Safety
- SERCOS-specific Safety profile

**SERCOS safety offers the following:**

- Simple realization of safety applications up to SIL 3 in accordance with IEC 61508, even for ultra-short cycle times
- Drastic reduction in topology costs compared to current solutions
- Drive-integrated safety functions incorporated in the machine control system to optimum effect, increasing plant productivity in the process
- Realization of homogeneous safety solutions in which the control system, drive, data transmission and I/O peripherals all merge to optimum effect
- Implementation of central and distributed architectures to meet the highest requirements in terms of performance and deterministic

**SERCOS III**

Direct cross-communication permits data exchange between two safety slaves without the safety master having to route the data. SERCOS III can therefore be used to create structures which work without any central safety control system whatsoever and which allow ultra-short response times.



SERCOS safety – integrated safety



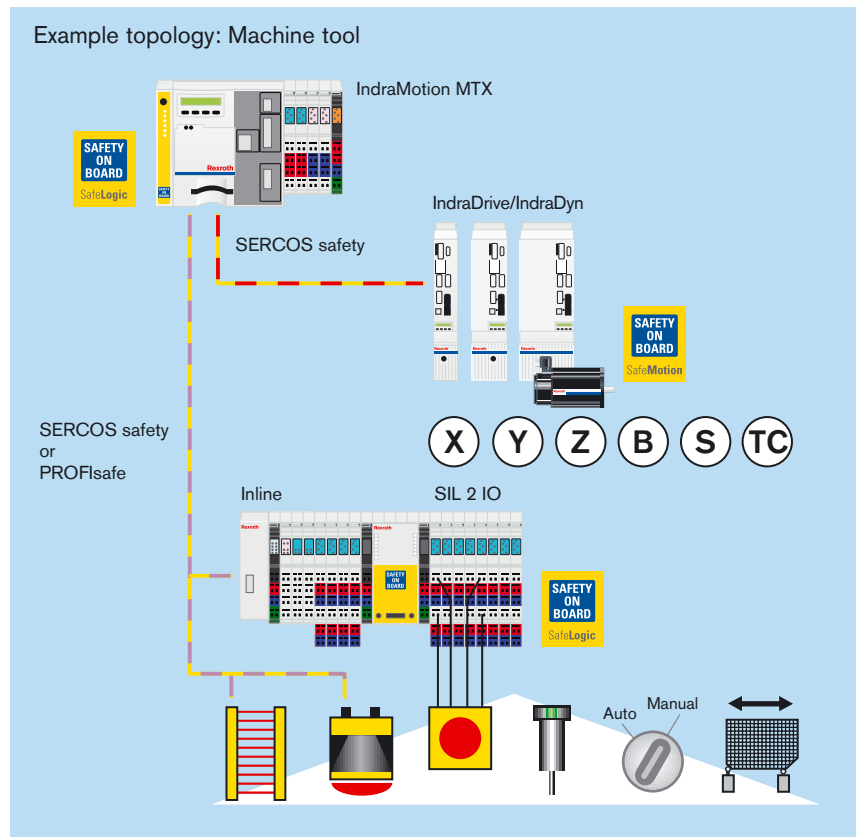
<sup>1)</sup> CIP Safety is a registered Trademark of the ODVA (Open DeviceNet Vendor Association)

# Safety on Board – In machine tools

C standard	Machine type	Safety-related control functions acc. EN 954-1:1996			
		Enable device	Reduced speed	Interlocking of guards	Emergency stop
EN 12417: Mar 2007	Machining centers	Category 3	Category 1 and verification, Category 3	Category 3	Category 3
EN 12415: May 2003	Turning lathes	Category 3	Category 3	Category 3	Category 1 (contact-based) Category 3 (electronic)
EN 14070: Jan 2006	Transfer and single-purpose or special-purpose machines	Category 3	Category 1 and verification, Category 3	Category 3	Category 3

When it comes to setting up tools and probes, carrying out control measurements or clearing faults, the SafeLogic and SafeMotion control and drive-integrated safety functions ensure that applications can be configured safely and easily, in accordance with EN 12415, EN 12417, EN 14070, for example.

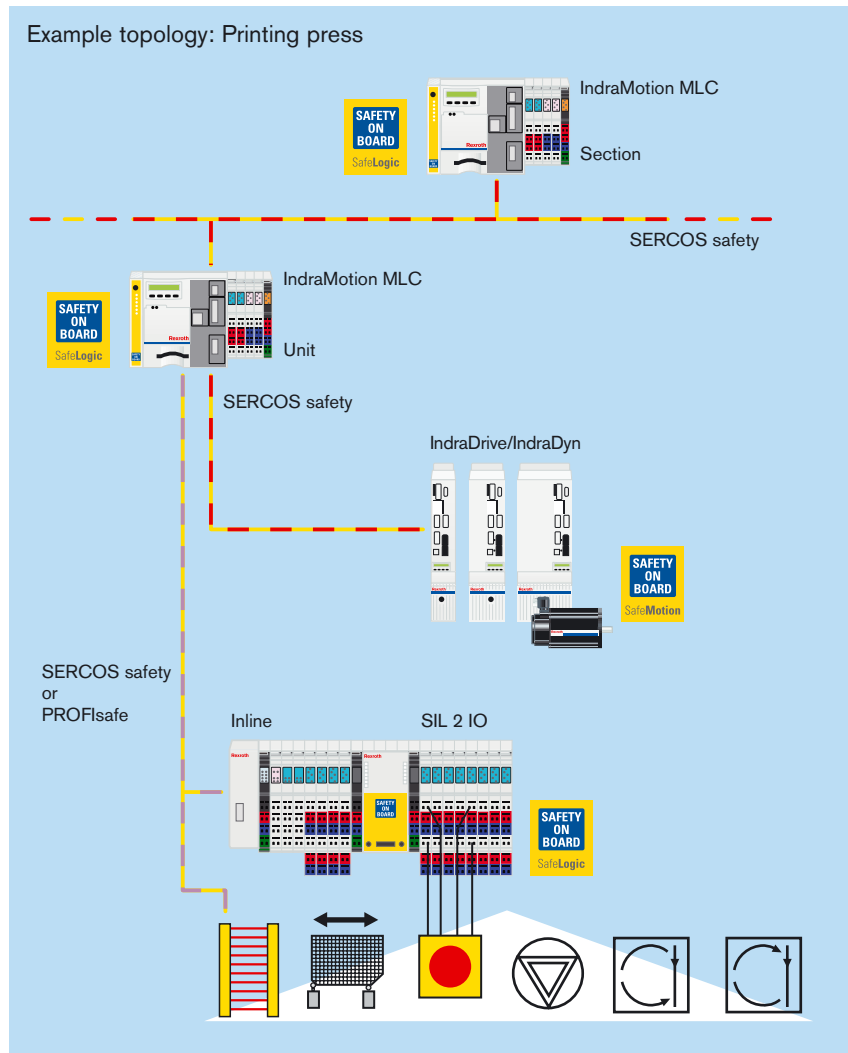
As long as the guard doors are closed the machine produces at full speed. In special mode the doors are allowed to be opened and, depending on the protection area, various safety functions are active which, for example, monitor the safe operating stop or permit operation at limited speed. In automatic mode it is possible to have the process monitored with higher safely monitored speeds.



# Safety on Board – In printing and converting machines

C standard	Machine type	Safety-related control functions acc. EN 954-1:1996	
EN 1010	Safety requirements for the design and construction of printing and paper converting machines	Without regular access as part of operations	With regular access as part of operations
EN 1010-1: Mar 2005	Common requirements	Category 3	Category 4
EN 1010-2: Jan 2006	Printing and varnishing machinery including pre-press machinery	Refer to EN 1010-1	Refer to EN 1010-1
EN 1010-3: Dec 2002	Cutting machines	Refer to EN 1010-1	Refer to EN 1010-1
EN 1010-4: Sept 2004	Bookbinding, paper converting and finishing machines	Refer to EN 1010-1	Refer to EN 1010-1
EN 1010-5: Oct 2005	Machines for the production of corrugated board and machines for the conversion of flat and corrugated board	Refer to EN 1010-1	Refer to EN 1010-1

Whether for changing plates or offset blankets, washing the rollers or changing the reels, SafeLogic and SafeMotion have everything needed for safe printing and paper conversion in accordance with the requirements, for example, of EN 1010. The safety functions such as the monitoring of protection areas, for example, or limited speeds or safe direction of rotation, are certified functions which are available in the controller and the drive. These safety functions are easy to integrate in the application with the help of function blocks, enabling safety and standard applications to be merged with each other to optimum effect.

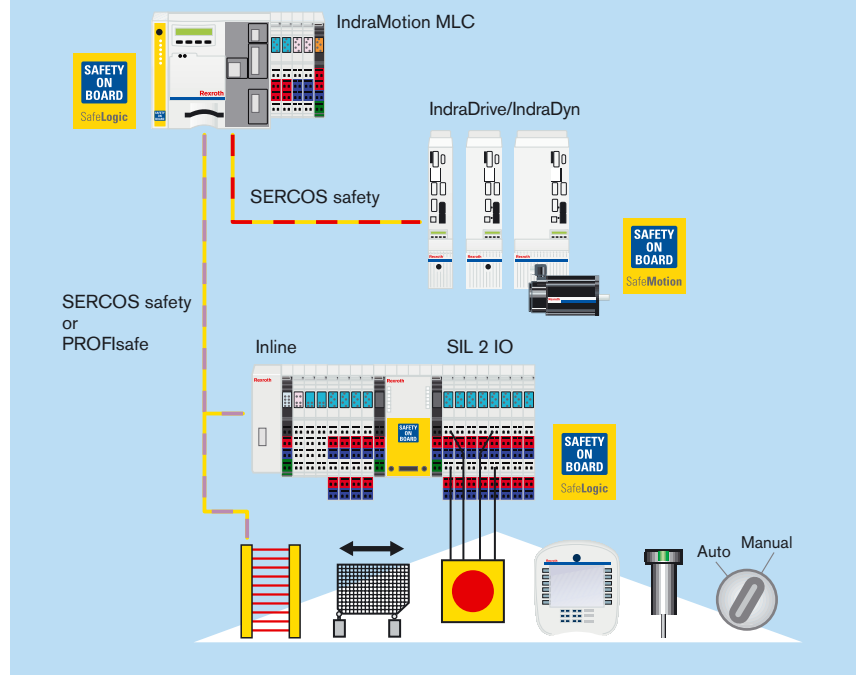


# Safety on Board – In packaging machines

C standard	Machine type	Servo-drive systems: Safe Operating Stop	Safety-related control functions
EN 415-2: Oct 2000	Pre-formed rigid container packaging machines		Category 2
EN 415-3: Oct 2000	Form, fill and seal machines		Category 1 or 2
EN 415-4: Aug 1997	Palletizers and depalletizers		Category 1 or 2
EN 415-5: Oct 2006	Wrapping machines		Refer to IEC 61508
EN 415-6: Oct 2003	Pallet wrapping machines	Category 3	Category 3
EN 415-7: Oct 2006	Group and secondary packaging machines	SIL 2	SIL 1
EN 415-8: Jan 2005	Strapping machines	Category 3	Category 1 to 3

Be it during forming, filling, closing, multi-packing or palletizing – if a product or wrapper becomes jammed for example, then the operator will need to access the inside of the machine safely in order to rectify the fault quickly. SafeLogic and SafeMotion enable a safe torque cut-out or a safe operating stop that does not entail switching off electromechanically the power and therefore does not result in a time-consuming machine restart. Overall equipment effectiveness (OEE) can thus be significantly increased. The requirements imposed by standards such as EN 415 for packaging machines can be met with SafeLogic and SafeMotion.

Example topology: Food processing and packaging machine



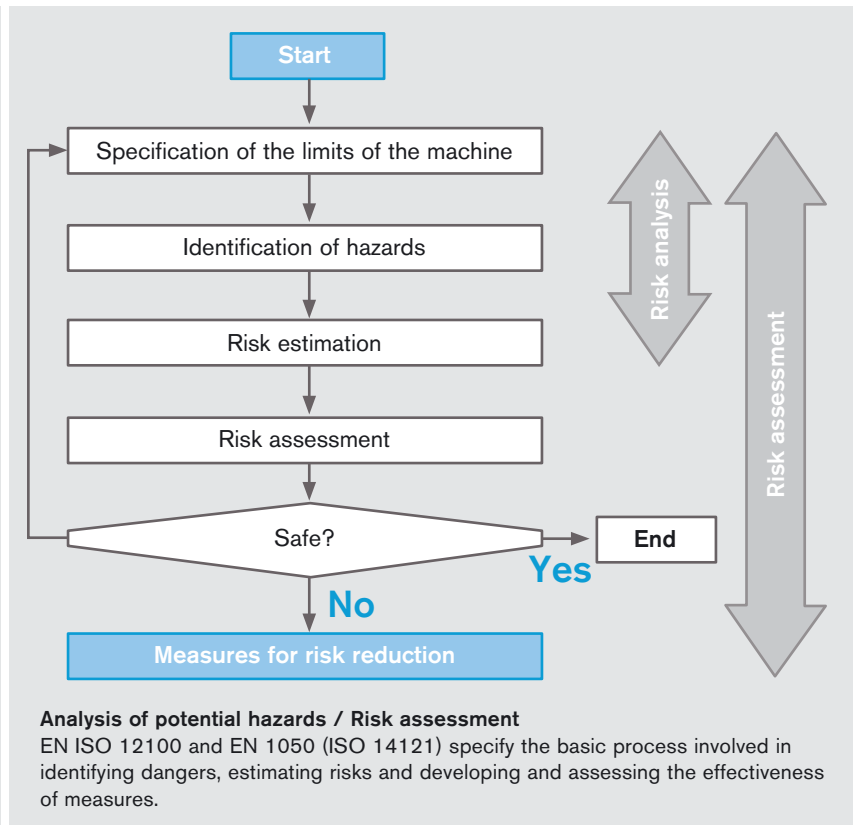




# Functional safety – Not just a question of standards

With the CE Mark of Conformity the manufacturer declares that his plant and machinery meet basic safety requirements. Standards help to provide the basis for verifying that this is actually the case. Does this mean that safety technology is simply a question of standards?

Certainly they cover basic requirements but they do not absolve the manufacturer from his responsibilities in respect of risk assessment and the implementation of measures.



## The European Machinery Directive

Manufacturers of plant and machinery are required to carry out an analysis of potential dangers and a risk assessment before construction is permitted. This is stipulated in the European Machinery Directive 98/37/EC, or the revised version of 2006/42/EC. The Machinery Directive has been incorporated in the national legislation of all the countries of Europe, which means that it is legally binding. The European Commission draws attention to the fact that the requirements of 2006/42/EC, ensuing as a consequence of the new Machinery Directive, can and should be complied with as of now in the development and manufacture of machinery.

However, up until Dec. 29, 2009 it is still permissible for Declarations of Conformity to refer to 98/37/EC only.

## CEN/CENELEC

The harmonized standards organized by CEN/CENELEC provide the manufacturers with help with verification because it can be assumed that in applying them the manufacturer will be conforming with the requirements of the Machinery Directive at the same time. However, in legal terms they are not binding.

## C standards

C standards stipulate specified requirements for certain types of machine such as, for example, machining centers, printing presses and paper converting machinery and presses. Machine types covered by C standards have had a risk analysis carried out and the standards also specify concrete measures for the reduction of risks for those machine types.

For those machines or parts of machines which are not included in the C standards, the manufacturer is responsible for undertaking the analysis of potential dangers and the risk assessment himself.

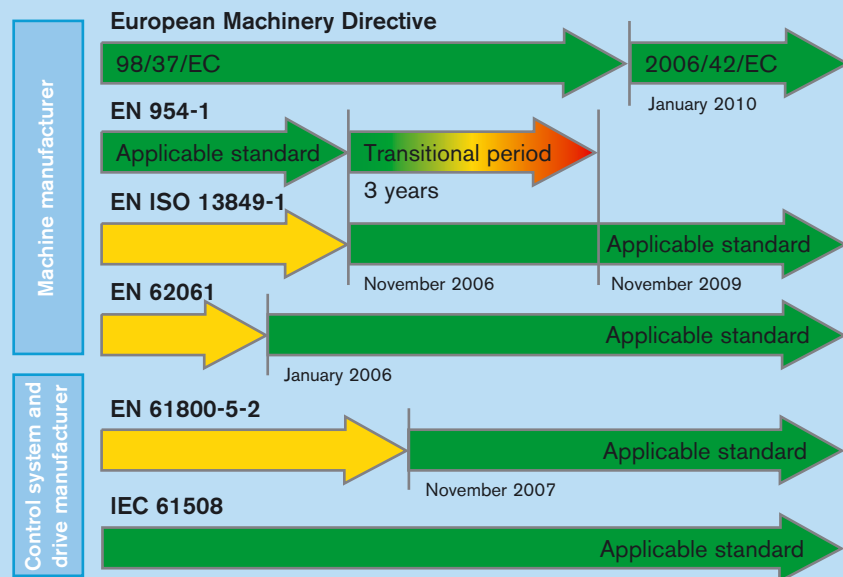
### Standards in a state of change

Up to now the safety-related components of machine control systems have had to be designed in compliance with EN 954-1. As from November 2009 the only applicable standard will be its successor, EN ISO 13849-1. This means that EN 954-1 may only be used for a transitional period for machines brought into circulation before the deadline of October 2009.

### Accounting for failure probabilities

EN 954-1 takes a deterministic approach which is largely defined by hardware-oriented structures and categories. With the growing importance of programmable electronics, in particular, in safety technology, it became necessary to adjust the simple error model to account for advances in technology and take account of modern concepts as well.

The new safety standards therefore take account of a probabilistic approach. Instead of considering the failure of a safety function in absolute terms it is assessed in terms of probability. Depending on the potential risk, the safety measure has to demonstrate a certain level of reliability, i.e. there must only be a certain probability of it failing. The entire product life-cycle is taken into account because many systematic "faults" occur early on in the planning stage. From the specifications and implementation to modifications and taking out of operation, requirements are made of all the phases in the life-cycle. Implementation is checked by means of verification and validation which has to be planned in concrete form in advance as part of a "Functional Safety Management Process" designed to ensure that quality is guaranteed.



### IEC 61508

The IEC 61508 standard is the "mother" of all safety standards which take a holistic probabilistic approach. It classifies the probabilities of failure in Safety Integrity Levels (SIL) 1–4, with the requirements of SIL 4 being the highest. As a general rule this standard is used by manufacturers of safety devices as a test standard. For machine builders, however, the requirements and measures are specified on a user-oriented basis in standards IEC 62061/ IEC ISO 13849-1.

### IEC 62061:2005

Since Jan. 1, 2006 the IEC 62061 standard can be taken into account as a harmonized standard for electrically and electronically programmable safety technology in machines. It is based on IEC 61508 and applies the level restricted to SIL 1–3 for classification. In order to simplify the calculation of reliability for the safety function, it specifies 4 sub-system architectures. In terms of the programming of the safety application, the requirements of IEC 62061 are

more limited than those of IEC 61508 in relation to the graphic programming languages line ladder diagram (LD) or function block diagram (FBD).

### ISO 13849-1:2006

ISO 13849-1 is based on the well-known hardware-oriented structures and categories in EN 954-1 but also combines them with failure probabilities. Unlike the IEC 62061 standard, ISO 13849-1 can also be applied to non-electrical/non-electronic systems. The requirements are grouped in 5 performance levels (PL). ISO 13849-1 is also restricted to simple graphic programming languages.

### IEC 61800-5-2:2007

The IEC 61800-5-2 standard is a product standard for electrical drives with integrated safety functions. The requirements are based on IEC 61508 and are also expressed in Safety Integrity Level (SIL) 1–3.

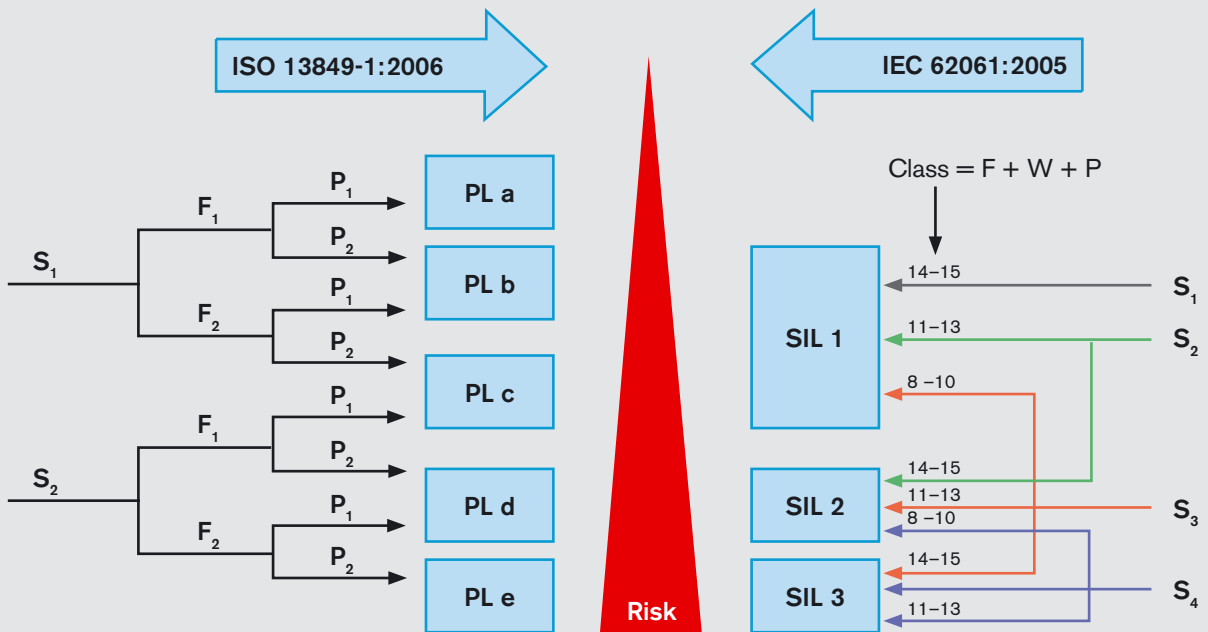
The required reliability of a safety function is determined with reference to severity (S), frequency (F) and potential for prevention (P). The required performance level (PL) is determined in accordance with ISO 13849-1 on the basis of classifications.

In contrast, IEC 62061 allocates points [1 - 5] for the evaluation of the influencing factors and takes the likelihood of occurrence into consideration (W). The sum of F+W+P therefore determines the required SIL in dependency on the severity (S).

For the evaluation of the achieved level of safety integrity, IEC 62061 stipulates a simplified mathematical procedure for predefined system structures. ISO 13849-1 on the other hand specifies the estimation of reliability (PL) as being dependent on the hardware-oriented structure (category), the determined mean time to dangerous failure (MTTFd) and the diagnostic coverage (DC) of a safety function.

	Performance Level (PL) ISO 13849-1:2006	Probability of dangerous failure per hour (1/h)	Safety integrity level (SIL) IEC 61508
<b>ISO 13849-1:2006</b>	a	$\geq 10^{-5}$ to $10^{-4}$	–
	b	$\geq 3 \times 10^{-6}$ to $10^{-5}$	1
	c	$\geq 10^{-6}$ to $3 \times 10^{-6}$	1
	d	$\geq 10^{-7}$ to $10^{-6}$	2
	e	$\geq 10^{-8}$ to $10^{-7}$	3
	–	$< 10^{-8}$	4
			<b>IEC 62061:2005</b>

Relationship between PL and SIL and the probability of failure in accordance with ISO 13849-1:2006

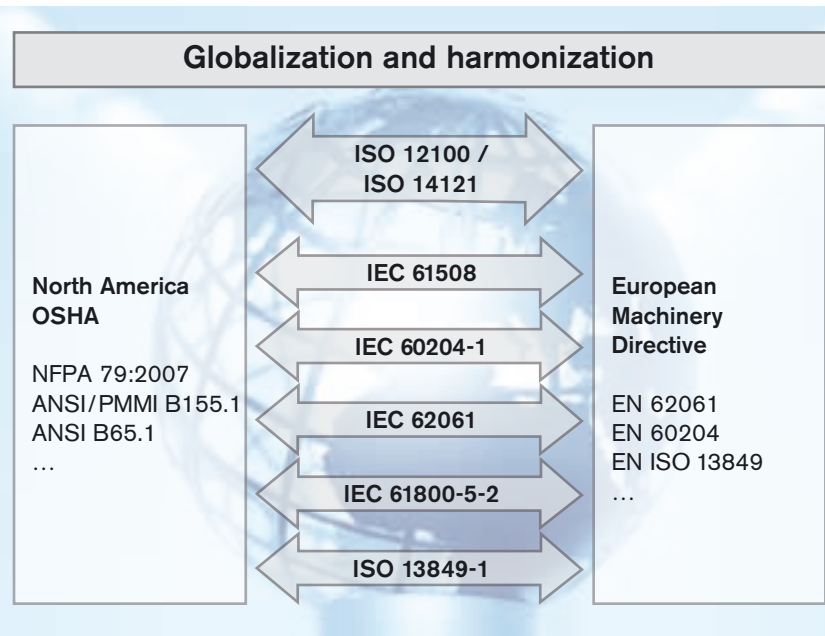


- S Severity of injury
- F Frequency and/or exposure a hazard
- P Possibility of avoiding the hazard or limiting the harm
- W Probability of hazardous event

# Standards for functional safety – European and worldwide

## Other countries, other regulations:

Country-specific regulations generally make it necessary to develop different, country-specific machine concepts. However, the precondition for international business, in particular, is a standardized approach to the requirements of functional safety throughout the world.



## Safety standards in the USA

The 1970 Occupational Health and Safety Act requires that safety has to be guaranteed for all work on plant and machinery. In particular, if the owner/operator of the machine knowingly allows his personnel to be exposed to preventable hazards, he can expect to pay penalties running to millions of dollars in the event of an accident. The Occupational Safety and Health Administration (OSHA) issues higher authority standards, but also often refers to “standards” of the “American National Standard Institute (ANSI)”, which can be applied in a similar way to the European presumptive effect.

User organizations and associations such as the NFPA, NEMA, PMMI, RIA, etc., also produce additional machine-specific standards which are often incorporated in an ANSI standard.

## International harmonization of standards

The introduction of the IEC 61508 standard and other standards derived from it such as IEC 62061 and ISO 13849-1 is a further step towards the international harmonization of the relevant safety standards. These standards have already had an influence on many American standards and/or compliance with the standards is made a condition for the use of safety-related components. The ANSI/PMMI B155.1 (2006) standard, for example, harmonized the process for risk analysis in accordance with ISO 12100 / ISO 14121 and refers to IEC 61508, IEC 62061 and ISO 13849-1, among others. The 2007 edition of the NFPA 79 takes account of drive systems which have been tested as acceptable in accordance with IEC 61508 and/or IEC 61800-5-2.

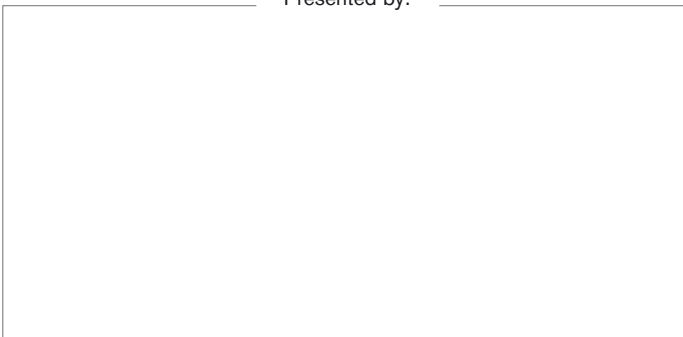
## NRTL Listing

The OSHA designates testing organizations as “National Recognized Testing Laboratories (NRTL)”. Even where these institutions make use of IEC 61508, for example, as the basis for testing and the results of the test correspond to those carried out by a testing organization certified in the EU, many North American companies still insist on a test by an NRTL. Bosch Rexroth therefore works with TÜV Rheinland North America Inc. as it is a testing organization which has NRTL-certification from the OSHA.



Bosch Rexroth AG  
Electric Drives and Controls  
P.O. Box 13 57  
97803 Lohr, Germany  
Bgm.-Dr.-Nebel-Str. 2  
97816 Lohr, Germany  
Phone +49 9352 40-0  
Fax +49 9352 40-4885  
[www.boschrexroth.com](http://www.boschrexroth.com)

Presented by:



The data specified above only serve to describe the product.  
As our products are constantly being further developed, no statements concerning a certain condition or suitability for a certain application can be derived from our information. The information given does not release the user from the obligation of own judgment and verification. It must be remembered that our products are subject to a natural process of wear and aging.

70 067 AE/2008-03 – A1 – HW  
R911323724  
© Bosch Rexroth AG 2008  
Subject to revisions!  
Printed in Germany