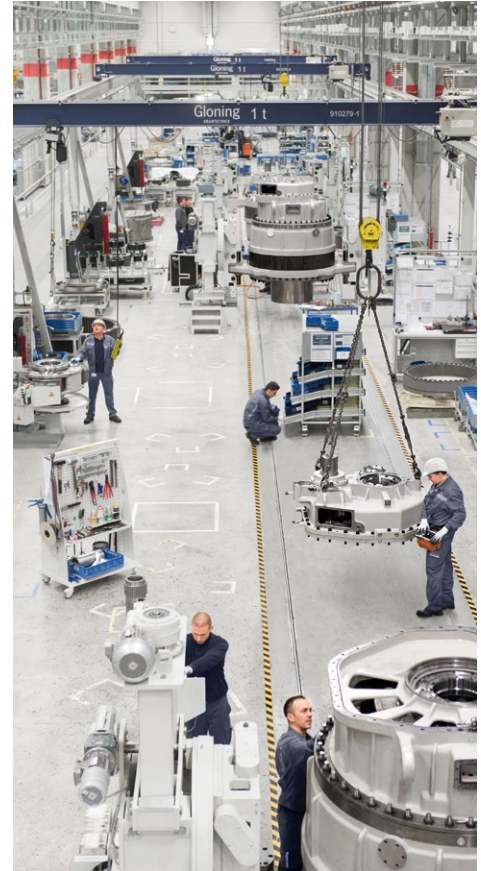


10 Steps to Performance Level



This brochure is a helpful accessory for the design of a control system based on the standards ISO 13849-1 and ISO 13849-2. It has no claim of completeness.

The statements in this document have been done carefully, but without guarantee. Only the original text from the relevant standards and directives are obligatory.



-
- 04 Realizing machine safety intelligently and economically
 - 06 Focus on Safety-Related Parts of a Control System (SRP/CS)
 - 07 Knowing what's important: Functional safety to ISO 13849
 - 08 Choose a partner who is able to join the dots.

10 Rexroth Safety on Board: More safety and productivity

- 12 1 Risk assessment
- 13 2 Identification of the safety functions
- 14 3 Determination of the required Performance Level (PL_r)
- 15 4 Category selection
- 16 5 Modeling of the block diagram
- 18 6 Faults and diagnosis
- 19 7 Determination of the PL
- 20 8 Evaluation of control system robustness
- 22 9 Software requirements
- 24 10 Verification and validation of the reached PL (PL ≥ PL_r)

-
- 25 Let us be quite clear on this ...

26 Make use of the comprehensive service. Benefit from practical training.

- 27 Benefit overview

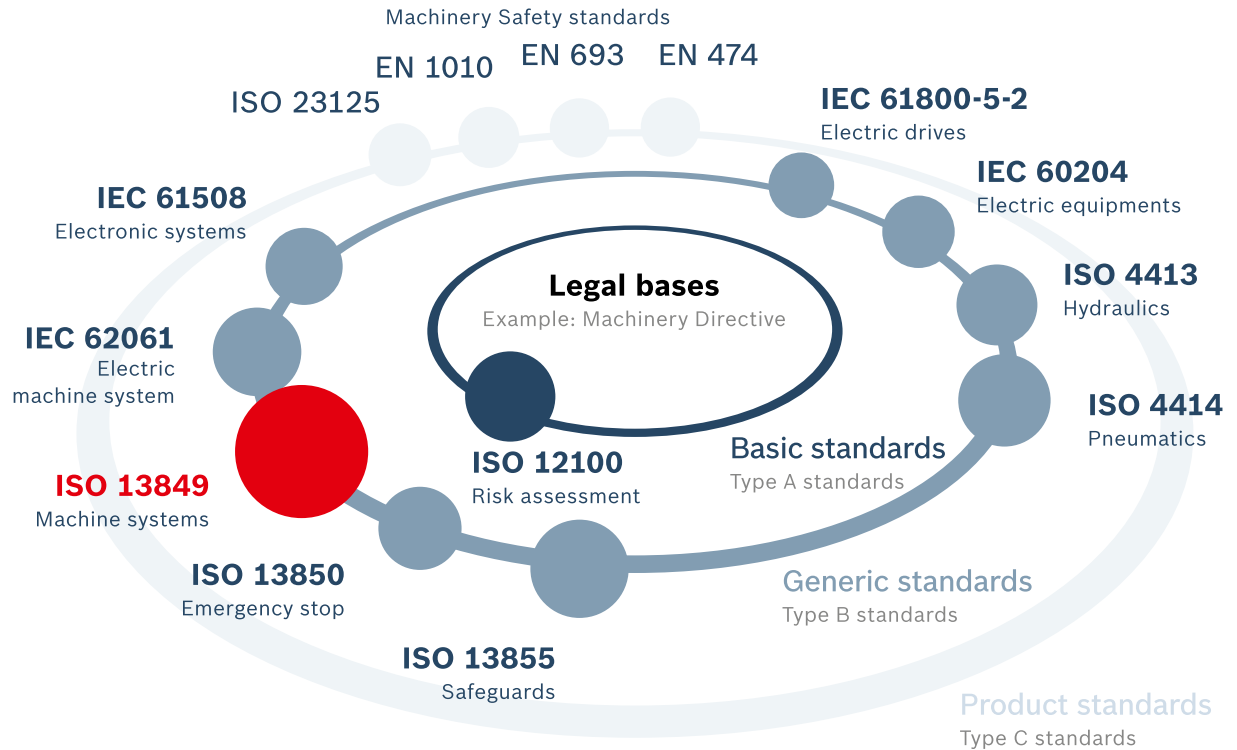
Realizing machine safety intelligently and economically

The requirements regarding safety technology are increasing worldwide. The design of modern machinery and plants is regulated by the 2006/42/EC Machine Directive in Europe as well as by the international standards ISO 13849 and IEC 62061 governing functional safety.

Machine manufacturers are obliged to provide evidence of personal protection in a comprehensive evaluation with statistical parameters, whereby all of the components and systems of control relevance used in the machine or plant are included. In the form of Safety on Board, Rexroth supports machine and plant manufacturers by providing know-how and individual consulting.

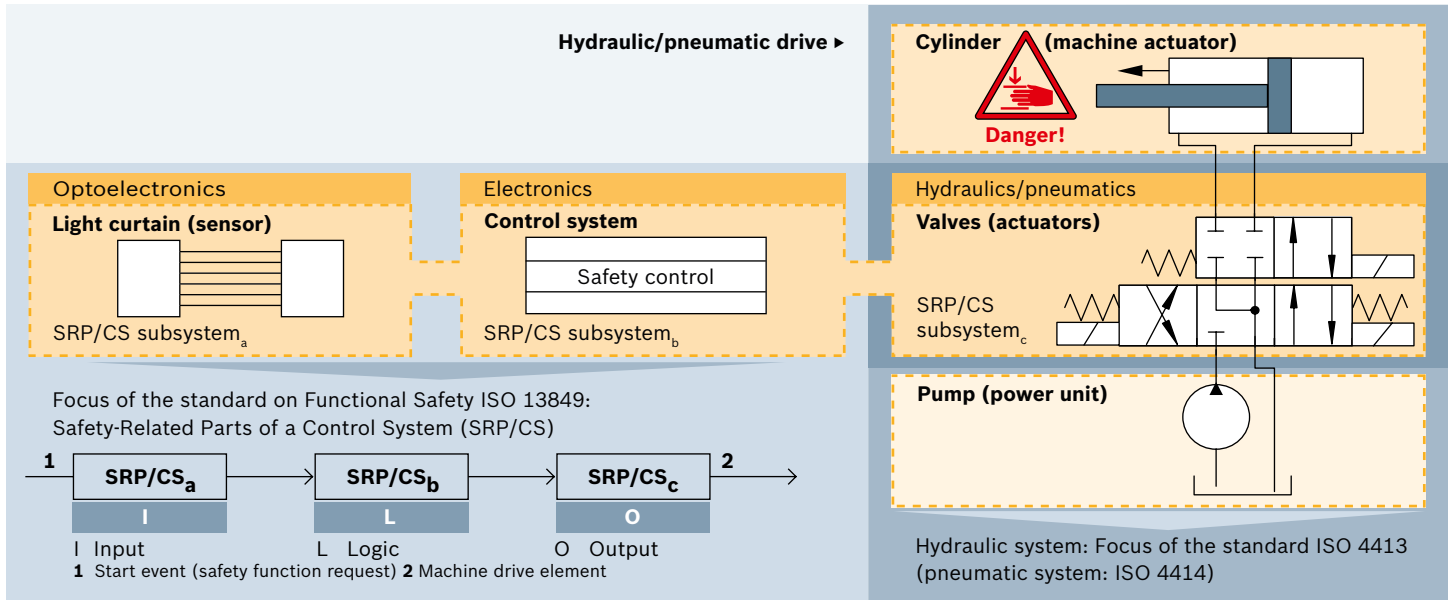
These guidelines not only help you to evaluate risks, they also show you how to design, implement, and commission the corresponding safety technology for your control systems – systematically and conformant with the respective standards.

We would be delighted to provide you with support.



Focus on Safety-Related Parts of a Control System (SRP/CS)

Control: Interaction between several systems



Knowing what's important: Functional safety to ISO 13849

ISO 13849 demonstrates how the safety requirements for machine controls are complied with. It considers the design and integration of the safety-related parts of controls (SRP/CS), regardless of whether electrical, hydraulic, mechanical, or pneumatic technologies are involved, for example. Specifications for electronic controls are also regulated by the IEC 62061.

The focus is on those parts of the control system that are of relevance for machine safety. As soon as safety is dependent on a correct control function, it is referred to as “functional safety” – with particular requirements on availability of the safety function.

More information on functional safety (ISO 13849) is available at:
www.boschrexroth.com/machinesafety



Choose a partner who is able to join the dots.

Rexroth has intensive automation expertise and international application experience. That's why we know the interactions and connections associated with systems with different technologies. Take benefit from this know-how and from our Safety on Board training offers and extensive services.

To take just one example: The design criteria and probability calculations affect the technical safety classification of components and systems – in practically all stationary and mobile machines. To this aim, suppliers must provide details concerning the reliability of all electrical, hydraulic, mechanical, and pneumatic components involved. By choosing Bosch Rexroth as a reliable partner, it goes without saying that you receive this data – along with all of the additional information you require.

Bosch Rexroth is one of the world's leading specialists in drive and control technologies. More than 500,000 customers in over 80 countries already rely on our tailored solutions for driving, controlling, and moving machines and plants.



▲ Simplify the safe operation of machine tools



▲ Ensure reliable energy generation



▲ Protect your employees from moving loads



▲ Enable safe working practices in the public sector

Rexroth Safety on Board: More safety and productivity

Divide complex tasks into clearly defined work packages: This brochure guides you from the risk assessment through to the final realization and evaluation of the safety level reached. This intelligent approach helps you to realize the state of the art for the protection of personnel and machinery in a feasible and documented manner.

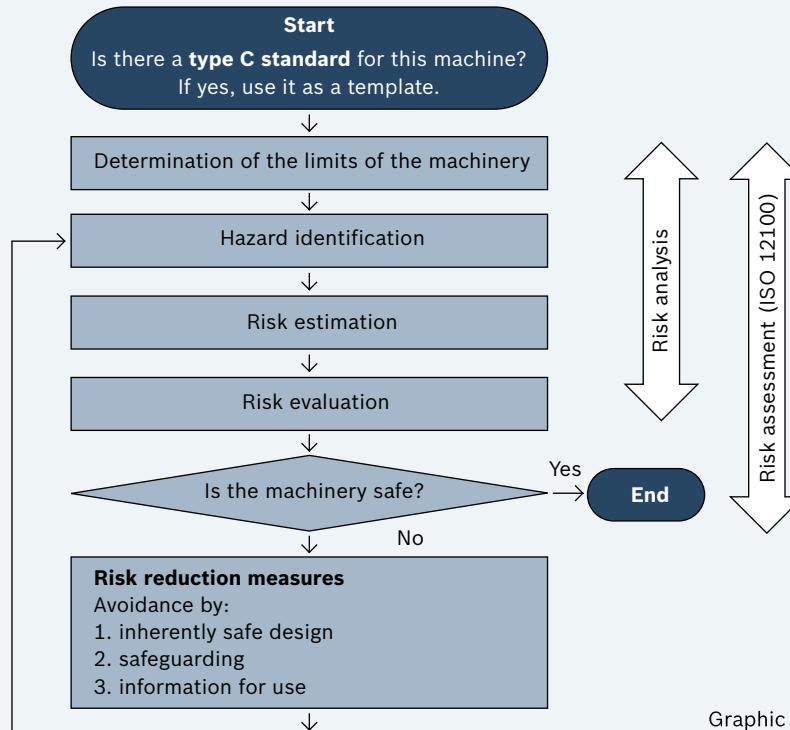
Rexroth Safety on Board also enables you to increase your machine performance. For example, you do not need to shut down the entire plant in the event of faults or when replacing tools. Simply ensure that the area in question is briefly and effectively in a safe state, enabling you to diagnose errors and eliminate them without delay.

- 1 Risk assessment
- 2 Identification of the safety functions
- 3 Determination of the required Performance Level (PL_r)
- 4 Category selection
- 5 Modeling the block diagram
- 6 Faults and diagnosis
- 7 Determination of the PL
- 8 Evaluation of control system robustness – failure avoidance
- 9 Software requirements
- 10 Verification and validation of the reached PL ($PL \geq PL_r$)



1 Risk assessment

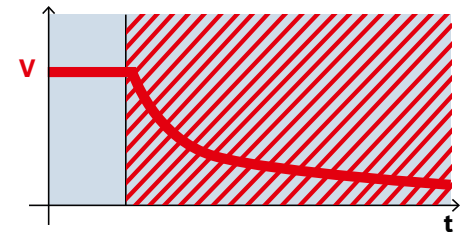
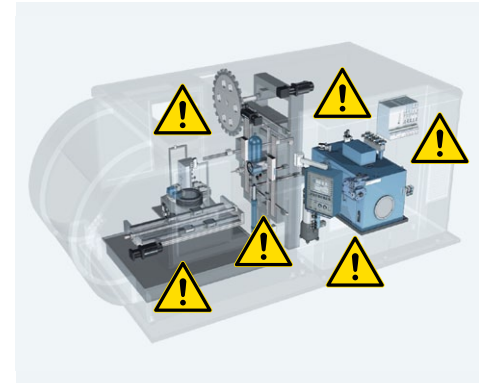
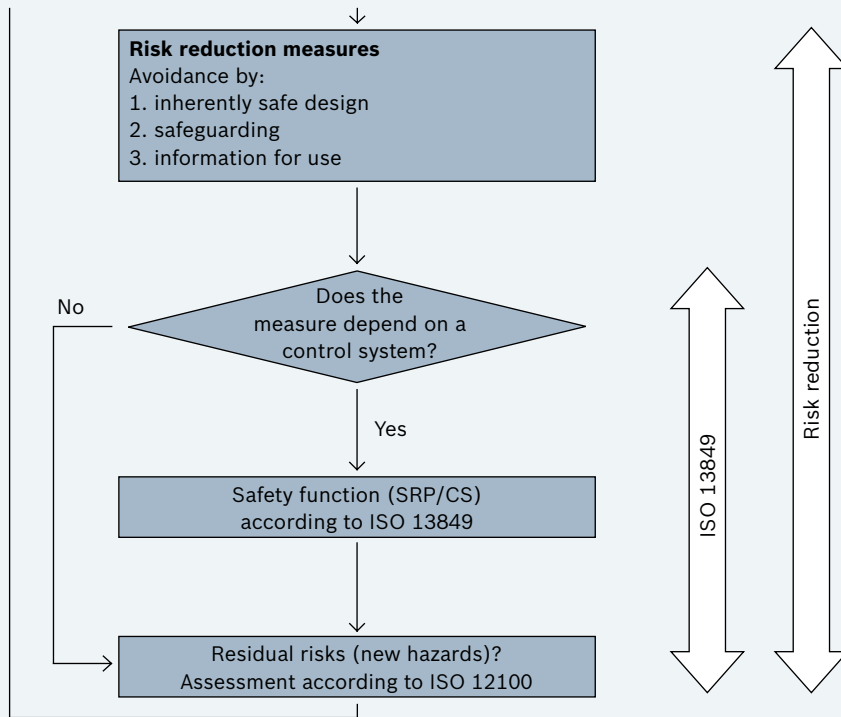
Is there a C standard for this machine? If yes, use it as a template.



Graphic continued on page 13

2 Identification of the safety functions

Graphic continued from page 12



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

Example: An unexpected startup must be avoided by opened protective door!

3 Determination of the required Performance Level (PL_r)

Performance Level (PL): A benchmark for the safety level

Severity of injury (S)

- S1 Slight (normally reversible injury)
- ✓ S2 Serious (normally irreversible injury or death)

Frequency and/or exposure to hazard (F)

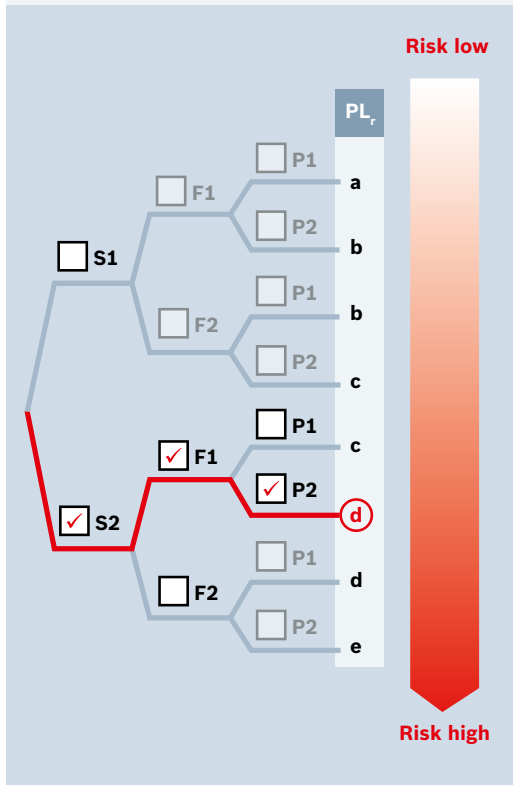
- ✓ F1 Seldom to less often and/or exposure time is short
- F2 Frequent to continuous and/or exposure time is long

Possibility of avoiding hazard or limiting harm (P)

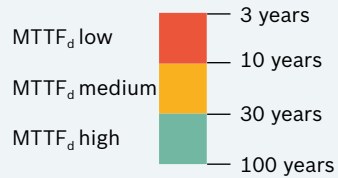
- P1 Possible under specific conditions
- ✓ P2 Scarcely possible

Example:

Functional failure can lead to fatal accidents. The operator requires access to the machine less than once per shift. In the event of a fault, they are unable to avoid the danger.



4 Category selection



Performance Level a

PFH_d: $\geq 10^{-5}$ to $< 10^{-4}$ [h⁻¹]

Performance Level b

PFH_d: $\geq 3 * 10^{-6}$ to $< 10^{-5}$ [h⁻¹]

Performance Level c

PFH_d: $\geq 10^{-6}$ to $< 3 * 10^{-6}$ [h⁻¹]

Performance Level d

PFH_d: $\geq 10^{-7}$ to $< 10^{-6}$ [h⁻¹]

Performance Level e

PFH_d: $\geq 10^{-8}$ to $< 10^{-7}$ [h⁻¹]

PFH_d: Probability of a dangerous failure per (operating) hour



I: Input
 L: Logic
 O: Output

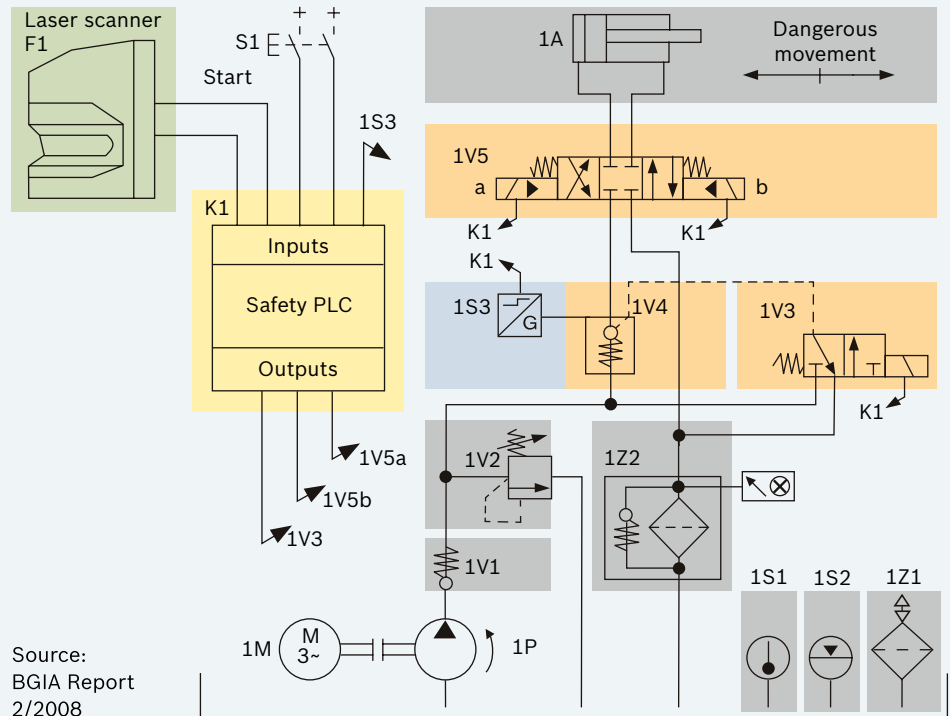
TE: Test equipment
 O_{TE}: Test equipment output
 MTTF_d: Mean time to dangerous failure

Information on the DC values under Step 6

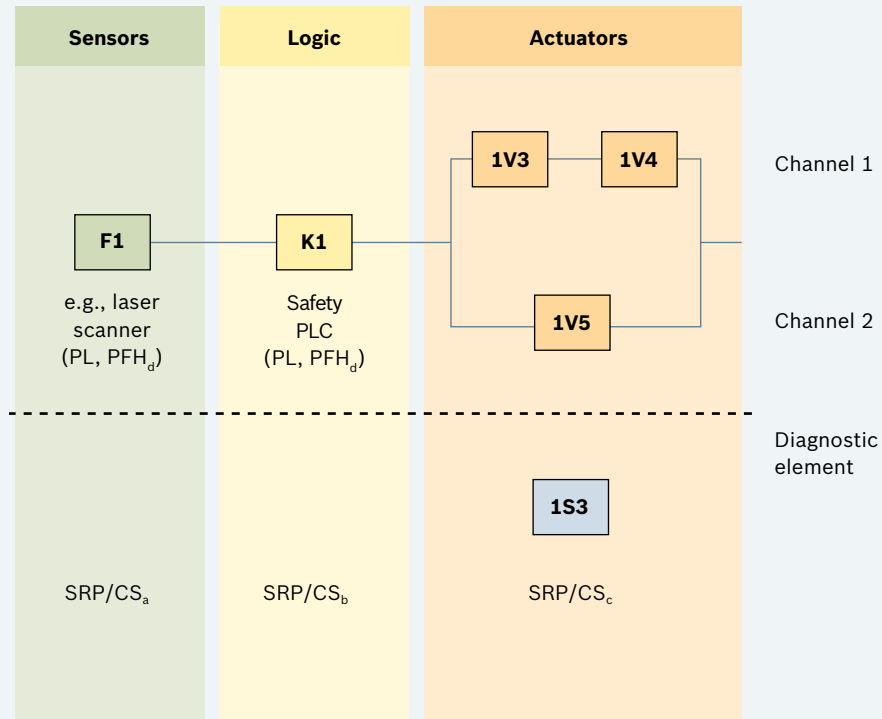
5a Modeling the block diagram

Which components are relevant for the safety function?

- Which hazards (dangerous movements) do exist?
 Cylinder!
Cylinder!
- Which components prevent it? (Stop the movements)?
 Valves!
Valves!
- What controls these components?
 Safety PLC!
Safety PLC!
- What triggers this function?
 Sensor!
Sensor!
- What tests this function, how, and how often?
 Position monitoring!
Position monitoring!
- What supports this function (safety principles)?
 Environmental conditions:
Temperature, level, pressure, filter!



5b Modeling the circuit as a block diagram



Connecting the blocks with each other (reverse analysis):

What does this element depend on?
Serial connection (dependency)

If this element fails, what takes over its function?

Parallel connection (redundancy)

Channel 1 Safe holding with valve combination 1V3 and 1V4

Channel 2 Safe holding with 1V5

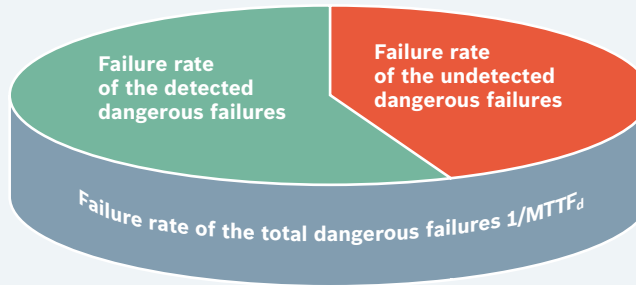
Both channels are controlled by PLC K1, which receives the request of the safety function from sensor F1.

With tests: monitoring by 1S3

6 Faults and diagnosis

Diagnostic coverage (DC) – proportion of the faults that can be detected:

Denomination	DC range
None:	$DC < 60\%$
Low:	$60\% \leq DC < 90\%$
Medium:	$90\% \leq DC < 99\%$
High:	$99\% \leq DC$



Example of design possibilities:

Measure	Technology	DC
Process (cyclic test)	Fluid technology	$0\% \leq DC < 99\%$
Cross-monitoring between 2 channels	Electronics	$DC = 99\%$
Indirect monitoring (e.g., pressure)	Fluid technology	$90\% \leq DC < 99\%$
Direct position monitoring	Fluid technology	$DC = 99\%$
Integrated self-monitoring	Safety on board	$90\% \leq DC \leq 99\%$

DC in %: Measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures ($\lambda_{d,d}$) and the failure rate of total dangerous failures (λ_d).

$$\lambda_d = \lambda_{d,u} + \lambda_{d,d}$$

7 Determination of the PL

The right parameters for different technologies

Hydraulic components



Supplier:

- $MTTF_d (B_{10})$

Machine manufacturer (OEM):

- Category
- DC
- CCF
- PL of the system

Pneumatic components



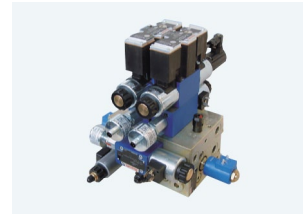
Supplier:

- B_{10}

Machine manufacturer (OEM):

- Category
- DC
- CCF
- PL of the system

Hydraulic subsystems



Supplier:

- PL_r category
- (Valve: $MTTF_d$)

Machine manufacturer (OEM):

- DC
- CCF
- PL of the system

Electronic subsystems



Supplier:

- (certified product)
- $PL (PFH_d)$
- Category

Machine manufacturer (OEM):

- PL of the system (by addition of the PFH_d values)

¹ Please also refer to ISO 13849-1 for calculating the $MTTF_d$ value from the B_{10} value.

² Calculate the PL value by adding the PFH_d values.

8a Evaluation of the system robustness




Checklist of examples of measures against CCF

CCF: Common Cause Failure

Measure	Fluid technology	Electronics	Points	Ful-filled?
Separation between signal paths	Separation in piping	Clearances and creep age distances on printed circuit boards.	15	
Diversity	e.g., different valves	e.g., different processors	20	
Protection against over-voltage, over-pressure ...	Assembly acc. to ISO 4413 or ISO 4414 (e.g., pressure-relief valve)	Protection against over-voltage (e.g., contactors, power supply unit)	15	
Components used are well tried	To be examined by the machine manufacturer for each specific application		5	
FMEA in development	FMEA in the design of the system	FMEA in the design of the system	5	
Competency/training	Qualification measure	Qualification measure	5	
Protection against contaminants and EMC	Fluid quality	EMV test	25	
Other influences (incl. temperature, shock)	Fulfillment of ISO 4413 or ISO 4414 and product specification	Fulfillment of the environmental conditions acc. to product specifications	10	
CCF total	Total number of points (65 ≤ CCF ≤ 100)			

8b Evaluation of the system robustness – safety principles

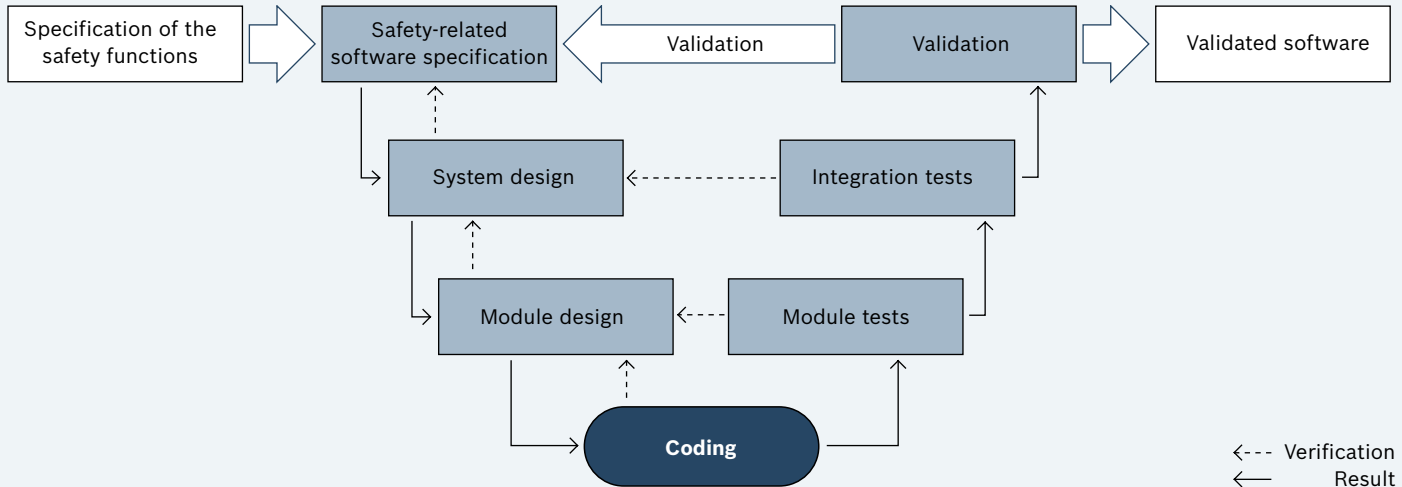
Overview of the well-tried safety principles as a checklist

	Can be used for technology				Implementation, e.g., by*			Comment (see comments in ISO 13849-2)
	Mechanical system	Pneumatics	Hydraulics	Electrical system	Component manufacturer	Machine manufacturer (OEM)	Machine end user	
Well tried safety principles								
Overdimensional/safety factor						<input type="checkbox"/>		
Safe position						<input type="checkbox"/>		
Force limitation/reduction						<input type="checkbox"/>		
Appropriate range of working conditions (environmental parameters)						<input type="checkbox"/>	<input type="checkbox"/>	
Avoidance of contamination of the compressed air						<input type="checkbox"/>	<input type="checkbox"/>	
Monitoring of the condition of the hydraulic fluid						<input type="checkbox"/>	<input type="checkbox"/>	
Minimize possibility of faults/separation						<input type="checkbox"/>		

Blue: Principle is not listed in ISO 13849-2 for the corresponding technology.

*These columns of the table serve as a basis for the machine manufactures and are to be adjusted by them.
The full chart is depicted in the handbook entitled “10 Steps to Performance Level”.

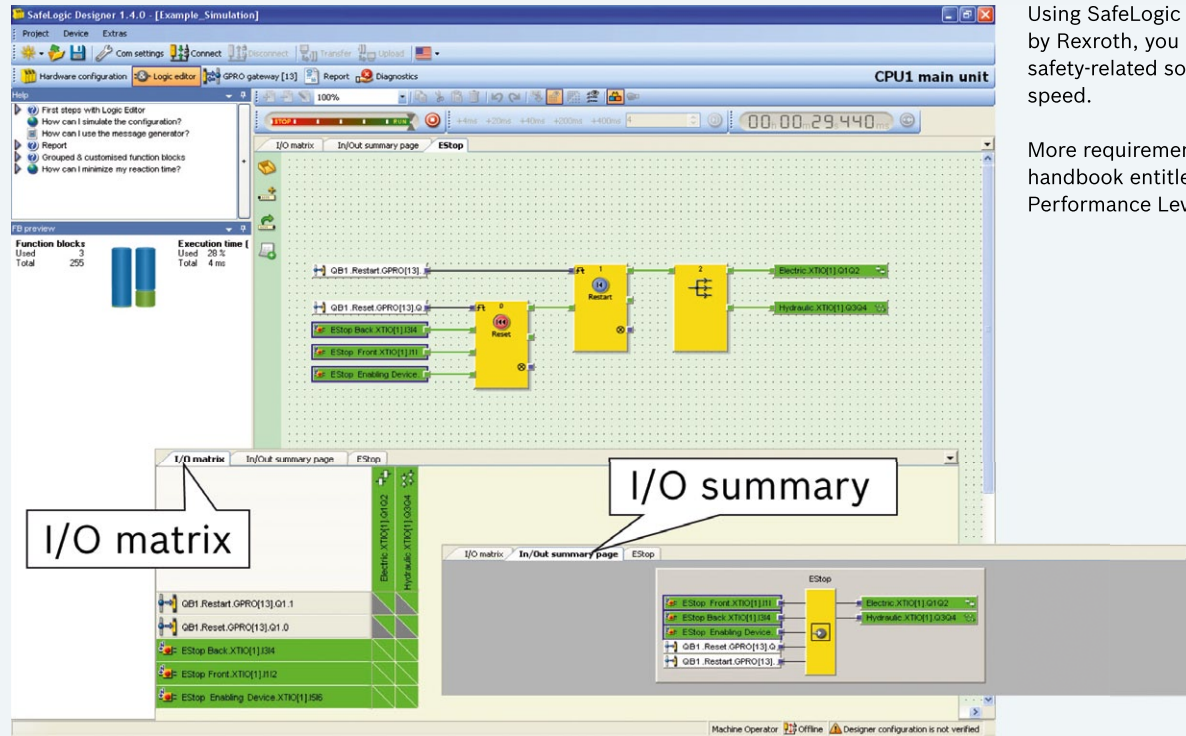
9a Software requirements



Achieve more safety using high-quality software to avoid errors – across the entire software life cycle. You receive software that is legible and comprehensible, which can be both tested and updated.

If, however, you do not use any parameterizable or programmable components, simply skip this step.

9b Safety-related software



Using SafeLogic Designer supplied by Rexroth, you can implement your safety-related software with ease and speed.

More requirements are depicted in the handbook entitled “10 Steps to Performance Level”.

10 Verification and validation of the reached PL ($PL \geq PL_r$)

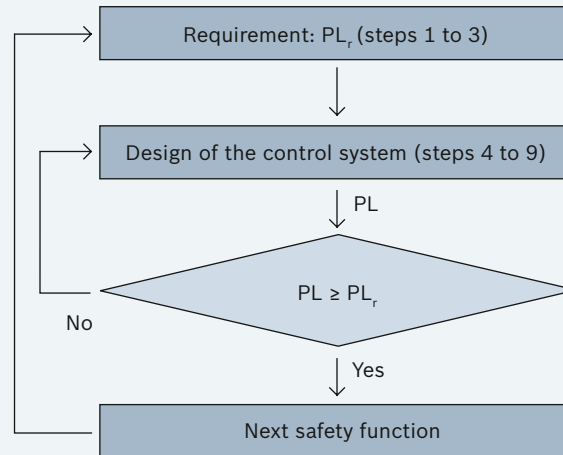
10a Verification of the reached performance level ($PL \geq PL_r$) Evaluation of the design

10b Validation of the reached performance level (machine manufacturer)

Have these requirements been met?

- Validation procedure acc. to ISO 13849-2
- Checking of implemented safety function
- Creation of technical documentation

A useful checklist is supplied in the handbook entitled “10 Steps to Performance Level”.



Let us be quite clear on this ...

The functional safety standards define clearly a set of terms and parameters. The most important ones:

PL (Performance Level): Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions [ISO 13849]

PL_r (Required Performance Level):
Required Performance Level [ISO 13849]

SIL (Safety Integrity Level): Safety Integrity Level (appropriated only for electronic control systems, see PL and IEC 62061)

MTTF (Mean Time To Failure):
Statistic expected value of the mean time to failure [ISO 13849]

MTTF_d (Mean Time To dangerous Failure):
Statistic expected value of the mean time to dangerous failure [ISO 13849]

FIT (Failure In Time): Unit used to measure the failure rate of electronic components (1 FIT = 1 x 10⁻⁹/h)

PFH_d: Probability of dangerous failure per hour (reference value for PL and SIL)

B₁₀: Statistic expected value of the number of cycles until 10% of the components have exceeded specified limits (response time, leakage, switching pressure, ...) under defined conditions

B_{10d}: Expected number of cycles until 10% of the components fail dangerously

T_{10d}: Expected value of the mean time until 10% of the components fail dangerously (maximal service time of a component)

T_M (Mission Time): Service life

DC: Diagnostic Coverage

CCF: Common Cause Failure

SRP/CS: Safety-Related Parts of a Control System

Dangerous failure:
Failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state

Make use of the comprehensive service. Benefit from practical training.

Support during the entire project term

Not every company has specialists with in-depth, up-to-date know-how concerning machine safety. As a small or medium-sized company, in particular, you can benefit from the comprehensive Rexroth service. After all, our modular services can be used individually or as comprehensive solutions from project management through to commissioning.

State-of-the-art application-oriented learning methods

Technology-specific or comprehensive learning modules communicate up-to-date knowledge on risk assessments, evaluating, project planning or commissioning of machine controls. To enable you to make the most of your time, we combine online training with practical courses and instructions on your premises. This reduces travel costs and minimizes downtimes.

Handbook for implementing functional safety

If you wish to reduce your expenses when designing safe machine controls, we recommend “10 Steps to Performance Level”, a handbook for implementing functional safety in accordance with ISO 13849.

More information on service, training and the handbook is available at:
www.boschrexroth.com/machinesafety



Benefits

- ✓ Man and machine protected
- ✓ Laws and standards satisfied
- ✓ Increased productivity, ergonomics and flexibility
- ✓ Minimized development time and effort
- ✓ Shortened reaction times and reduced space required
- ✓ Reduced Total Cost of Ownership (TCO)



The Drive & Control Company

Rexroth
Bosch Group

Bosch Rexroth AG

97816 Lohr am Main

Germany

info@boschrexroth.de

www.boschrexroth.com/machinesafety

RE 08511/01.13

Printed in Germany

© Bosch Rexroth AG 2013