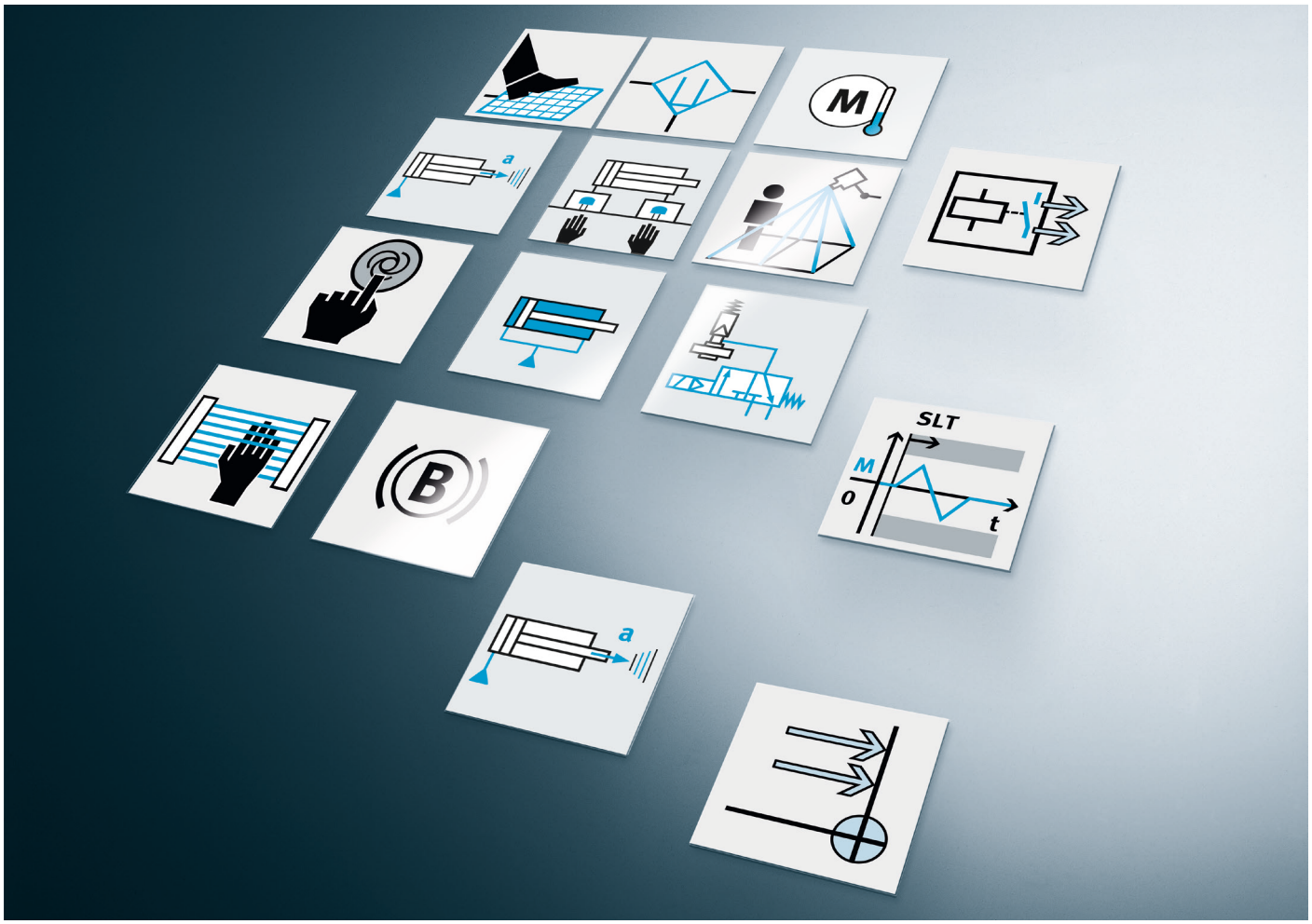
Achieving Functional Safety in Factory Automation

This white paper provides a helpful overview of functional safety, including all relevant directives and standards, for pneumatic and electrical automation systems.



Functional safety, which is part of the overall safety of a piece of equipment, reduces the risk of simple and complex systems so that they function safely even in the event of a malfunction. The objective is to prevent harm or damage to personnel, machines and the environment. Yet despite its importance in factory automation, the topic of functional safety is extensive—and you may have questions:

- Why should I use safety-related pneumatic and electric components?
- Which standards and directives apply?
- What protective measures are based on these standards?
- What are the most common protective measures?
- How can I identify the risk posed by a machine to the operator?

The goal of this white paper is to support you in implementing functional safety in pneumatic and electric automation technology in ways that comply with the EC Machinery Directive. Safety-related solutions, which can take the form of components, circuits or engineering practices, will enable you to successfully achieve your safety objectives while guaranteeing reliable machine operation in all stages of service life.

Your First Step: Perform a Risk Assessment

A well-proven method for determining machine safety requirements is to carry out a risk assessment according to the legal requirements of EC Machinery Directive 2006/42/EC. These assessments stipulate protective measures according to ISO 12100 standards, outlining safe machine design. Assessments also enable the implementation of functional safety measures according to ISO 13849, which is the safety standard that applies to the parts of machine control systems responsible for safety functions. (For a more detailed list of common machine safety standards, please see our table.)

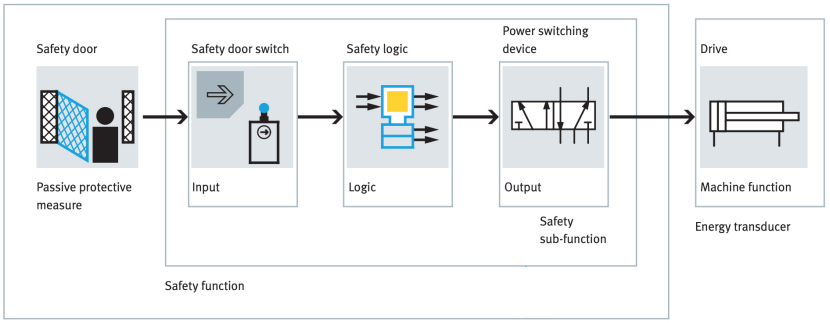
The risk assessment and analysis process involves compiling all required information, identifying the basic hazards and then estimating the risk potential. Then, on the basis of risk estimation, decisions must be made on whether or not protective measures are required for each hazard.

Overall Safety Functions for Pneumatic and Electric Components

The overall safety function is a protective measure for risk reduction that involves reaching or maintaining a safe machine state. One example is the separation of the operator from the hazard zone. To grant the operator access, the hazardous drive movement is stopped, and the drive is maintained. In this case, the overall safety function consists of a passive protective measure, the sensor (input), the logic (safety relay unit) and the valve combination (output).

Safety sub-functions, which are part of the overall safety function, are performed by a component or group of components in the safety function. A common example is the disconnection of a power switching device—such as a valve or motor controller—from the power supply.

Safety function



Some common examples of safety sub-functions in pneumatic and electric drive technology include:

- **Safe Torque Off (STO).** This function separates the power supply to the pneumatic drive, exhausting the drive's chambers and preventing the generation of a dangerous force. In electric systems, the STO function prevents force-generating energy in the electric drive and also unexpected drive startup.
- **Safe Stop 1 (SS1).** This function reduces or blocks the volumetric flow rates in and out of the pneumatic drive's two chambers, slowing down the drive's movement and bringing the drive to a stop. If the system reaches a standstill according to the

defined tolerance window, then the SS1 function reduces the pressure in the chambers, preventing dangerous forces. In electric systems, the SS1 function similarly brings the electric drive to a standstill within specific limits.

- **Safe Operating Stop (SOS).** This function prevents pneumatic drives from deviating from the stopping position by more than a specific amount. It also maintains the compressed air supply, enabling the drive to withstand the effect of external forces—for example, variable load—without any further measures. In electric systems, the SOS function supplies energy to the electric drive, enabling it to withstand external forces.

Determining Machine Performance Levels Based on the risk assessment, a Performance Level (PL) is assigned to each part of the machine. Machine performance levels specify the ability of safety circuits to execute a safety function under foreseeable conditions. They are also specified as discrete levels—PLa, PLb, PLc, PLd and PLe—and are only determined for complete safety circuits or safety devices.

Some of the quantitative and qualitative parameters that determine PL include the following:

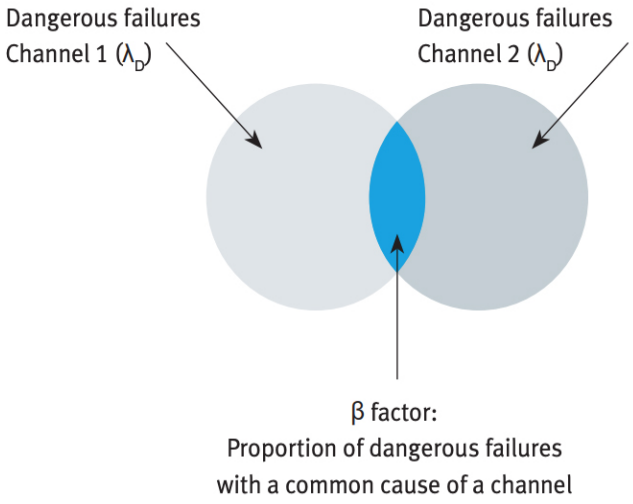
- **Circuit Structure.** The structure of a safety circuit depends on the arrangement of the components and diagnostics. These structures are divided into categories B to 4, which classify the safety circuits in terms of their resistance to faults and behavior when a fault occurs.
- **Mean Time to Dangerous Failure.** The Mean Time to Dangerous Failure (MTTFD) takes into account the reliability of the components in the safety circuits. It also specifies the portion of failure modes that poses a hazard to personnel, equipment or the environment. (For more information about calculating this value, please see our sidebar.)
- **Diagnostic Coverage (DC).** DC measures the effectiveness of the diagnostics and also specifies the proportion of identifiable and unidentifiable dangerous failures. The higher the risk, the higher the effectiveness of these diagnostics. The diagnostics of a safety sub-function must be able to monitor the safe state of the power switching component. If the safe state is exited, then the signal changes from logic 1 to logic 0. If the safe state is resumed, then the signal changes from logic 0 to logic 1. Determining Machine Performance Levels based on the risk assessment, a Performance Level (PL) is assigned to each part of the machine. Machine performance levels specify the ability of safety circuits to execute a safety function under foreseeable conditions. They are also specified as discrete levels—PLa, PLb, PLc, PLd and PLe—and are only determined for complete safety circuits or safety devices.

For power switching components with a specific normal position—for example, a spring—then the safe state is always in the normal position, and the safety sub-function is executed in the normal position. For components with no specific normal position—double solenoid valves, for example—then the possible safe state depends on maintaining the current switching position.

Common Cause Failures (CCF). CCF refers to the failures of different components due to a single event. With safety circuits from category 2 onward, the CCF must always be analyzed. This is necessary as certain causes of a fault can cause both channels to fail, disabling the safety function and compromising the required single fault protection.

ISO 13849-1 uses the beta factor model of the IEC 61508-6 standard, and has simplified it for use in machinery and systems building. This beta factor model lets you estimate the proportion of dangerous failures in a channel following the cause of the error whenever dangerous failures also appear in the second channel. The selected approach of ISO 13849-1 uses a point system with a list of measures to prevent CCF. These measures include:

- The physical separation of signal paths—e.g. the separation of wiring, as well as the detection of short and open circuits in cables by dynamics tests. Which standards and directives apply?
- Diversity—e.g. different technologies and valve designs, various switching frequencies and the integration of components with different loads. What are the most common protective measures?
- Protection against overvoltage, over-pressure, over-current and over-temperature.
- The training of designers to understand the causes and consequences of CCF.
- The environment—e.g. preventing contamination and electromagnetic disturbances.

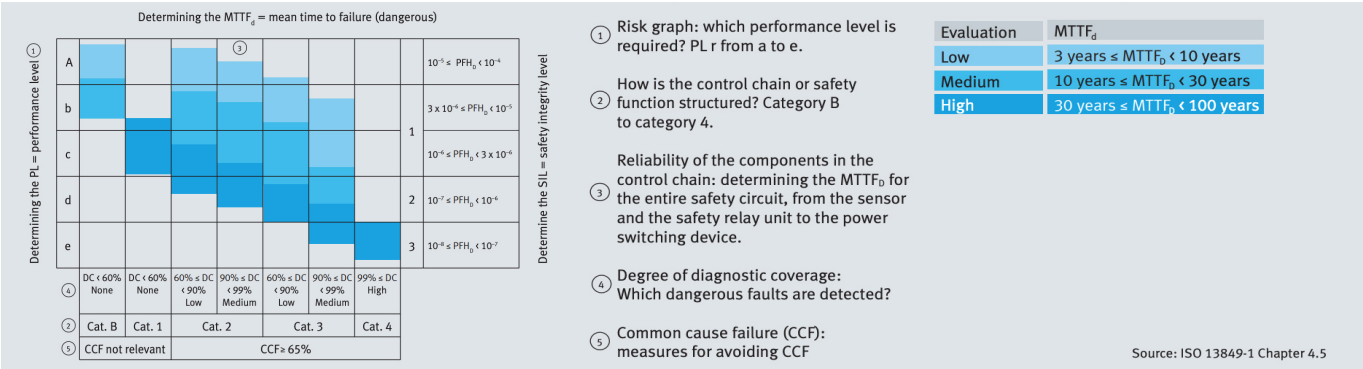


Fault Behavior. For category 2 safety circuits, you can assess fault behavior with a failure mode and effects analysis (FMEA) or fault tree analysis (FTA). Depending on your application and selected components, however, you may need to take additional measures to meet ISO 13849 requirements.

Safety-Related User Software. The product life cycle of safety-related user software must take into account the prevention of faults. The software's primary objective must be readable, understandable, testable, maintainable and preferably fault-free.

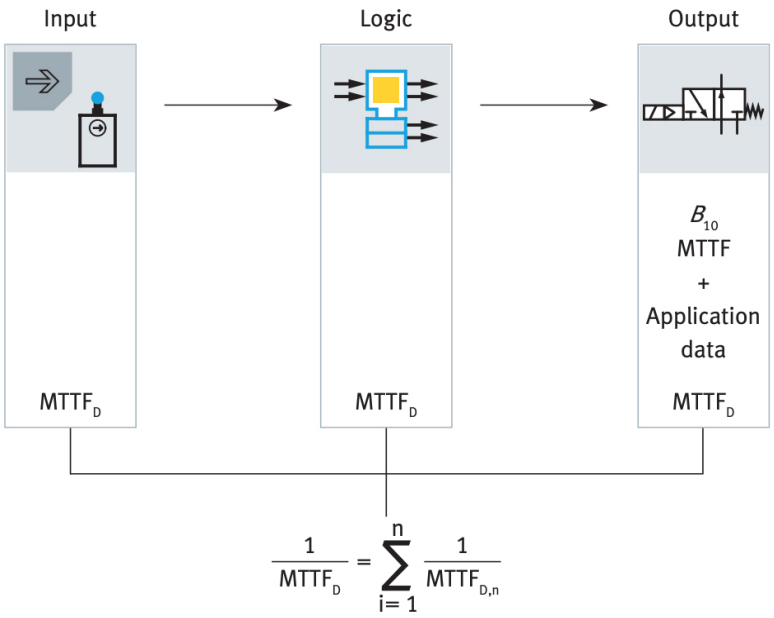
Systematic Failures—and More. These are the failures that can be traced back to a specific cause and can only be eliminated by changing the design, manufacturing process, operating behavior and documentation. Other parameters for determining PL include the ambient conditions, requirement rate and any substances affecting the materials.

The following figure depicts a simplified procedure for determining the PL of a safety function.



Learn More About Functional Safety With Festo Engineering for functional safety is one of the most important requirements in factory automation and process industry applications. At Festo, we offer products and solutions that enable you to implement functionally safe, cost-effective engineering as easily as possible.

To learn more, please download our Guideline for Functional Safety.



The Difference Between a Safety Device and Safety-related Part of a Controller

A safety device is evaluated by its manufacturer for its safety function. The manufacturer also provides characteristic values for a safety device, including the PL, safety integrity level (SIL), PFH, category, DC, CCF, etc. Examples of safety devices include light curtains, safety door switches, emergency stop command devices, safety relays and many more.

The manufacturer also provides characteristic values for standard components suitable for safety-related applications: B10 values, tried-and-tested components, compliance safety principles and fault exclusions, if required.

Determining the MTTFD For a Channel

For every channel of a safety function, you must determine the mean time to dangerous failure, or the MTTFD value. Typically, safety functions consist of a combination of input, logic and output, as well as their connections. For each of these blocks, the component manufacturer should specify the reliability information such as the probability of failure on demand per hour (PFH), MTTF or B10 values. If this information is not available, you can find the characteristic values of good engineering practices in ISO 13849-1, Table C.1.

According to ISO 13849-1, 3.1.25, you can calculate MTTF on the basis of tables—for example, according to SN 29000—or by using B10 values and their parameters of use. B10 is the expected value until 10% of the components have failed. For pneumatic components, you can determine this value using endurance tests as outlined by ISO 19973.

You can use statistical procedures to determine these values, enabling you to estimate how long it will take for a large percentage of the evaluated products to fail. In practice, you can then use this information to estimate the failure probability, time until the first repair, replacement intervals and more.

According to ISO 13849-1, for the safety-related parts of a control system, you must estimate the time until the first dangerous failure based on MTTFD or B10D values. If the dangerous proportion of the B10D value cannot be explicitly specified, then we can assume 50% of the B10D value is dangerous (per ISO 13849-1 C.4.2) using the following equation:

B10D = 2 x B10D

The MTTFD value is the expected mean time until a dangerous failure occurs with a probability of 63% (per ISO 13849-1, 3.1.25), while the B10D value specifies the number of cycles until a dangerous failure occurs for 10% of pneumatic and electromechanical components (per ISO 13849-1, Table 1).

While a detailed FMEA is necessary to determine MTTFD and B10D values, as well as those failures that might be dangerous for a given application, you can only evaluate these values if you know how the safety function is implemented—something that isn't always possible for standard products. That is why ISO 13849-1 offers a simplified option for estimating MTTFD and B10D based on the MTTF or B10 values.

Basic Standards for the Implementation of Machine Safety

Type A standard	ISO 12100	Risk assessment and risk reduction
	ANSI B 11.0	General Requirements and Risk Assessment (USA)
Type B standards	ISO 13849	Safety-related parts of control systems
	ANSI B 11.26	General Principles for the Design of Safety Control Systems Using ISO 13849-1 (USA)
	ISO 4414	Rules and requirements for pneumatic systems
	EN 60204-1	Electrical equipment for machines
	NFPA 70	National Electric Code (NEC) (USA)
	NFPA 79	Electrical Standard of Industrial Machinery (USA)
	ISO 14118	Unexpected start-up
	CFR 1910.147	Control of Hazardous Energy (Lockout/Tagout) (USA)
	ISO 14119	Interlocking devices with safety guards
	ISO 14120	Guards
	ISO 13850	Emergency stop function
	ISO 13855	Arrangement of protective devices
	ISO 13857	Safety distances
	EN 349	Minimum gaps to avoid crushing of body parts
	ISO 10218	Industrial robots
	ANSI / RIA R15.06	Industrial robots (USA)
Type C standards	ISO 16090-1	Machining centres, milling machines, transfer machines
	ANSI B11.23	Safety Requirements for Machining Centers, Milling, Drilling and Boring Machines
	EN 13736	Pneumatic presses
	ANSI B11.2	Safety Requirements for Hydraulic and Pneumatic Power Presses
	ISO 23125	Turning machines
	EN 1010	Printing and paper converting machines
	EN 422	Blow moulding machines
	EN 848	Woodworking machines
	ISO 11161	Integrated manufacturing systems
	ANSI B 11.20	Integrated Manufacturing Systems (USA)
Other standards	ISO 5598	Fluid power systems and components – Vocabulary
	ISO 1219	Fluid power systems and components – Graphical symbols and circuit diagrams
	EN 81346-2	Classification of objects and codes of classes
	EN 82079-1	Preparation of instructions for use
	EN 61508	Functional safety of safety-related electrical, electronic and programmable electronic systems
	EN 61508	Safety instrumented systems for the process industry
	EN 62061	Functional safety of safety-related electrical, electronic and programmable electronic control systems
	EN 61800-5-2	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional safety
Technical specifications	ISO/TR 14121-2	Risk assessment – Practical guidance and examples of methods
	ISO/TR 23849	Guidelines on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machines
	ISO/TR 20218-1	Robots – end effectors
	VDMA 24584	Safety functions of regulated and unregulated systems
	ISO/TS 15066	Collaborating robots
	ZVEI CB24I	Position paper classification 24-V interfaces with testing