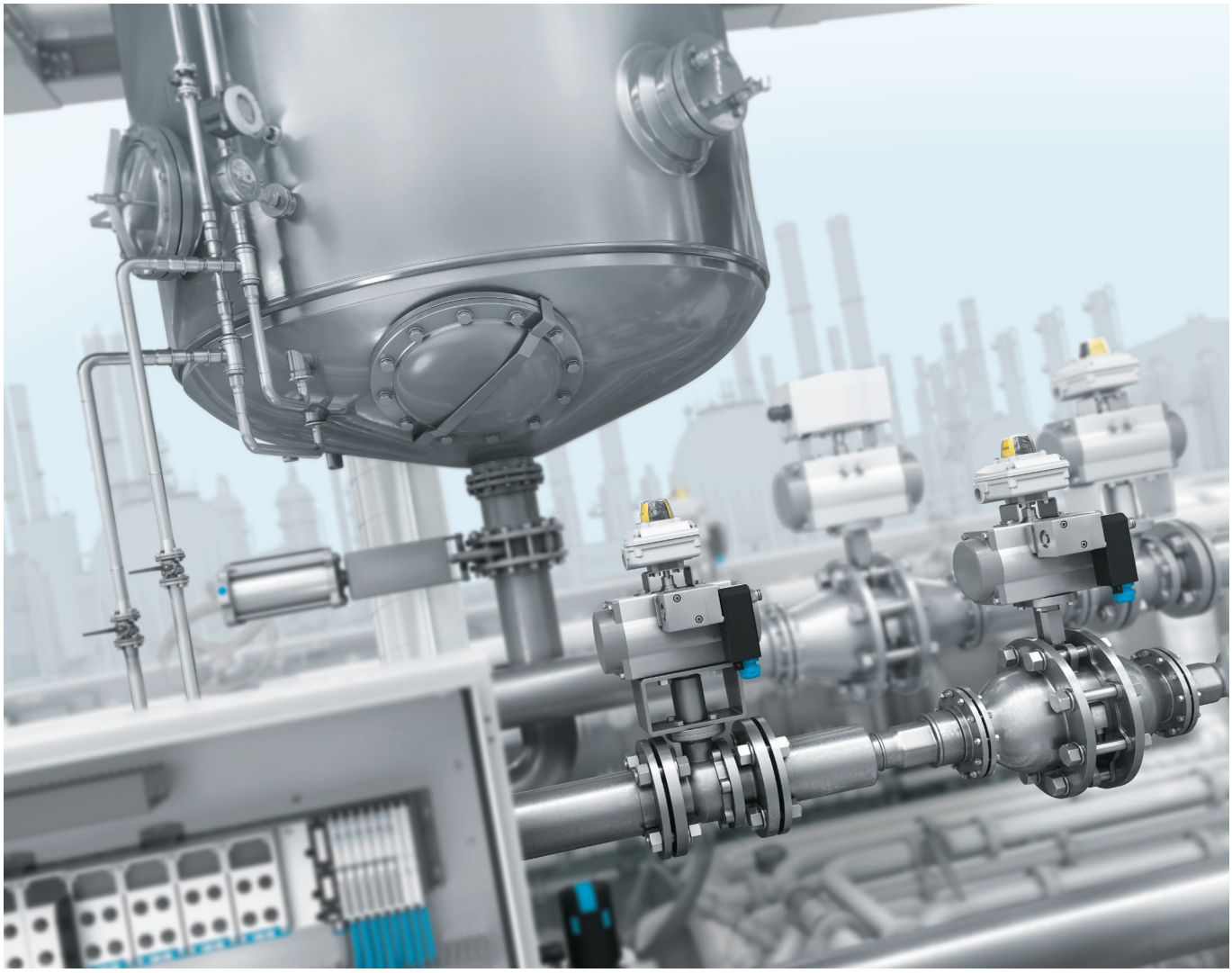
White paper
Controlling process valves and considering functional safety (SIL)



Functional safety in the process industry is a topic that has very much moved centre stage since IEC 61508 came into force. It is frequently only indicated by the abbreviation SIL. But what exactly is SIL and how can it be used to control process valves?

This white paper contains information on the following topics:

- What is SIL (Safety Integrity Level)?
- The standards
- Risk analysis
- Certificates and manufacturer's declarations
- Example of a protective device in a stirred-tank reactor
- Proven performance and extended service life using the example of a solenoid valve
- Redundant activations of actuators in the field

1. What is SIL (Safety Integrity Level)?

The aim of safety functions is to minimise the risk posed by processes for people, the environment and property. The SIL (Safety Integrity Level) describes the extent to which risk is reduced to a reasonable level. IEC 61508 explains the method for assessing risks (risk graph) and the measures required to design suitable safety functions, ranging from sensors and logic circuits to actuators for error prevention (systematic errors) and error control (random errors). This application-dependent basic standard describes the requirements for components and systems for safety functions and facilitates the development of sector-specific standards such as IEC 61511-1: "Functional safety - Safety instrumented systems for the process industry sector". IEC 61511-1 defines, among other things, the criteria for selecting components for safety functions such as operational reliability of sensors and actuators.

Important to know

The requirement for the probability of failure to IEC 61508 always refers to a complete protective device and not to individual components. A component, in and of itself, can therefore not have a SIL level; only a complete safety circuit, or SIS (Safety Integrated System), can have a SIL level.

Normally, a safety circuit consists of the following components:

- Sensors, e.g. pressure, temperature, fill level gauge
- Evaluation and output unit, e.g. a safety PLC
- Automated process valve comprising solenoid valve, actuator and process valve

Sensor ≥ 35%		Logic ≥ 15%		Actuator ≥ 50%	
PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}
SFF	λ_{SU}	SFF	λ_{SU}	SFF	λ_{SU}
HFT	λ_{DD}	HFT	λ_{DD}	HFT	λ_{DD}
MTBF	λ_{DU}	MTBF	λ_{DU}	MTBF	λ_{DU}
$SIL_{required}$ (SIL_r)					
PFD_{total}/PFH_{total}					

Typical distribution of the PFD/PFH between the sub-systems of a safety function in single-channel systems

Notified by the manufacturer

To be determined by the system operator

2. The standards

The standards for functional safety are extensive and not always easy to understand, even for experienced users. In this white paper, we will focus on the interpretation and the practical application of these standards but will not focus on them in detail.

The following standards are relevant:

- IEC 61508: "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems"

→ Basic standard for functional safety

- EN 61511 "Functional Safety – Safety Instrumented Systems for the Process Industry Sector"

→ Applies to process automation

3. Risk analysis

To minimise risk, both IEC 61508 and IEC 61511 essentially require the following steps:

- Risk definition and assessment according to detailed failure probabilities for everything from sensors through to controllers and actuators for the entire service life of the components.
- Definition and implementation of measures to minimise residual risk.
- Use of suitable devices (evaluated or certified).
- Regular tests and inspections to ensure correct observation of safety functions.

© Copyright 2017, Festo AG & Co. KG

3.1. HAZOP analysis and other methods

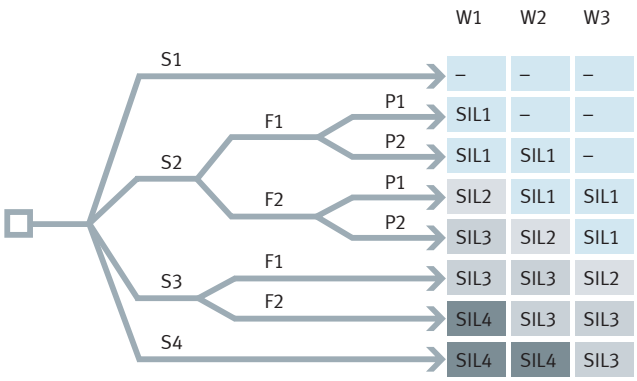
Hazards are defined as potentially critical deviations from the production process plans. In other words, hazards are dangers that pose an actual or potential threat. A HAZOP (Hazard and Operability Study) is used for systematically identifying errors and operability problems that reduce productivity. Nowadays, this method can be used for all types of systems for continuous or discontinuous production. The basic steps in a HAZOP analysis are:

1) Predict a possible result
2) Investigate causes
3) Assess the consequences
4) Countermeasures

Examples of other methods used in risk evaluation are Failure Mode and Effects Analysis (FMEA), Event Tree Analysis (ETA) or Fault Tree Analysis (FTA). These methods can be classified into three groups: inductive methods, where the causes but not the consequences are known; deductive methods such as FTA, where the consequences are known but not the causes; and exploratory methods such as HAZOP, where neither the causes nor the consequences of deviations are known. The different methods are used to find the missing information.

These methods can be further subdivided into bottom-up searches and top-down searches. Bottom-up means starting from a critical error and trying to determine the consequences (FMEA). Top-down searches involve starting with the hazardous consequences and trying to determine the causes (FTA).

SIL (Safety Integrity Level)



Risk graph: Four discrete levels (SIL1 to SIL4). The higher the SIL of a safety-related system, the lower the probability of the system not being able to execute the necessary safety functions.

S	Extent of damage	
	S1	Minor injury to a person
	S2	Severe injury to multiple persons or death of a person
	S3	Deaths of several persons
	S4	Catastrophic consequences with multiple deaths
F	Frequency and exposure time	
	F1	Seldom to relatively frequent
	F2	Frequent to continuous
P	Avoiding/mitigating the danger	
	P1	Possible under certain conditions
	P2	Hardly ever possible
W	Probability of occurrence	
	W1	Relatively high
	W2	Low
	W3	Very low

© Copyright 2017, Festo AG & Co. KG

3.2. Important terms and characteristic values

HFT
The hardware fault tolerance refers to the ability to perform the safety function even in the event of (multiple) errors and deviations. If the required SIL cannot be achieved based on these values, the SIL can be achieved via redundancies.

SFF
The SFF (safe failure fraction) determines the proportion of safe failures out of the total number of failures. Safe failures are those that do not cause a dangerous system status or that could cause a dangerous system status but are not detectable.

A product's suitability for a required SIL can be determined based on several parameters:

Low Demand
Operating mode with a low frequency of demands to activate the safety system. Demands to activate the safety system may not exceed one per year.
→ PFD (probability of failure on demand) = probability of failure on demand is event-based.

High Demand
Operating mode with a high frequency of demands or continuous demands to activate the safety system. The safety system operates continuously or demands to activate the safety system exceed one per year.
→ PFH (probability of failure per hour) = probability of failure per hour is time-based

Device type A/B
Type A: Failure behaviour of all components has been sufficiently described. This type includes simple (new) devices as well as devices with tried and tested performance.

Type B: Failure behaviour of at least one component is not fully known. This type includes complex devices as well as newly developed products.

Target: SIL ≥ SIL_r

SIL level			Device type A				Device type B					
			Safe Failure Fraction (SFF)									
	High Demand Mode	Max. acceptable failure of the safety system	‹ 60%	60...90%	90...99%	› 99%	‹ 60%	60...90%	90...99%	› 99%	**Low Demand Mode**	Max. acceptable failure of the safety system
	$10^{-5} \leq PFH < 10^{-4}$	One risk of failure every 10,000 hours										
1	$3x10^{-6} \leq PFH < 10^{-5}$	One risk of failure every 1,250 days	HFT 0				HFT 1	HFT 0			$10^{-2} \leq PFD < 10^{-1}$	Once every 10 years
	$10^{-6} \leq PFH < 3x10^{-6}$	One risk of failure every 115.74 years										
2	$10^{-7} \leq PFH < 10^{-6}$	One risk of failure every 115.74 years	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0		$10^{-3} \leq PFD < 10^{-2}$	Once every 100 years
3	$10^{-8} \leq PFH < 10^{-7}$	One risk of failure every 1,157.41 years	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \leq PFD < 10^{-3}$	Once every 1,000 years
4	$10^{-9} \leq PFH < 10^{-8}$	One risk of failure every 11,574.1 years		HFT 2	HFT 1	HFT 1			HFT 2	HFT 1	$10^{-5} \leq PFD < 10^{-4}$	Once every 10,000 years
					HFT 2	HFT 2				HFT 2		

(per hour)

Overview of failure probability and hardware failure tolerance

© Copyright 2017, Festo AG & Co. KG

4. Certificates and manufacturer's declarations
System operators require proof of the SIL classification of the components used in the SIS (safety instrumented system). According to IEC 61511, manufacturer's declarations are perfectly adequate for this. Certificates are not required by law nor are they required by the standard. A technical evaluation of the safety component to be used is needed in order to issue a manufacturer's declaration or certificate. This evaluation is frequently carried out by an independent organisation such as TÜV or Exida. If the evaluation is successful, the manufacturer can issue a manufacturer's declaration and refer to the test report of the evaluation.

Unlike manufacturer's declarations, certificates may only be issued by an accredited organisation (such as TÜV).

The safer the system has to be, the more independent the entity that evaluates functional safety and issues the evaluation must be:

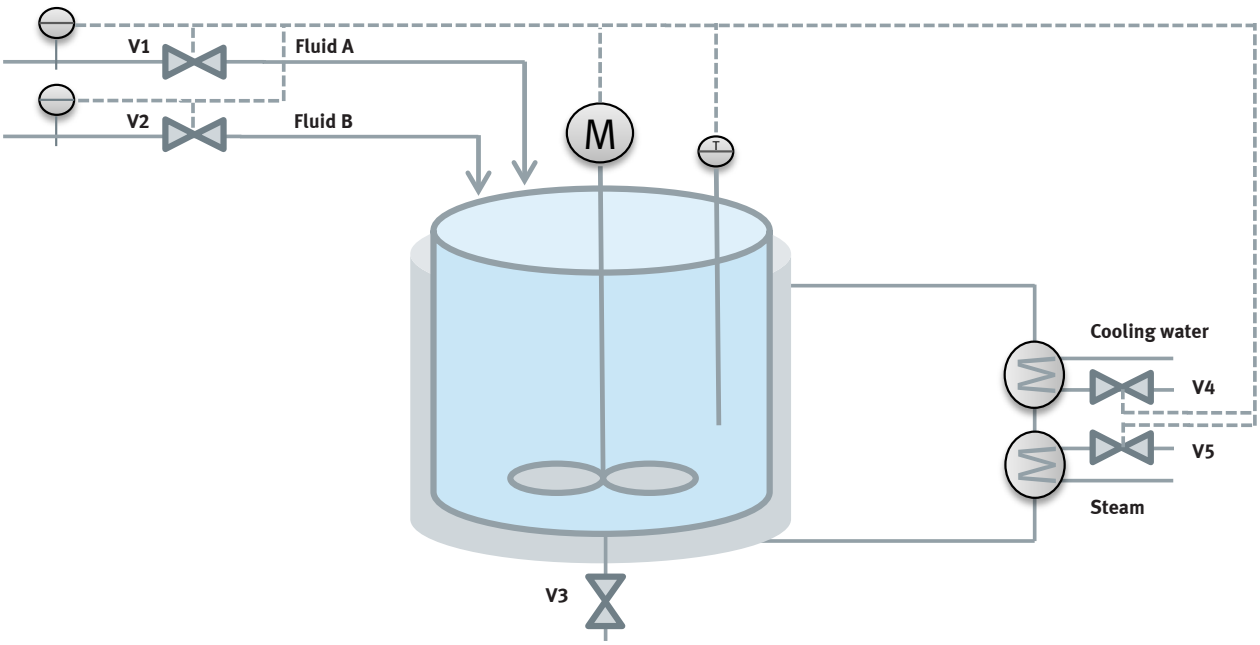
Safety Integrity Level	Evaluating entity
SIL 1	Independent person
SIL 2	Independent department
SIL 3	Independent organisation
SIL 4	Independent organisation

5. Example of a protective device in a stirred-tank reactor
In a stirred-tank reactor, different components are connected (via valves V1 and V2 in the example below) and react through heat input (endothermically) or heat release (exothermically). By stirring the contents they are thoroughly mixed. Overheating must be avoided during exothermic reactions.

In the diagram below the pressure regulation for the reaction process is an example of a function requiring a protective device. If the pressure in the reactor gets too high, heat may not be dissipated properly and cause a fault. As a result, the mixing ratio would not be correct.

This scenario would give rise to the following requirement for the protective device: close the feed valves V1, V2 and the steam valve V5 while simultaneously opening the cooling valve V4 to cool down the reactor.

There are different options for solving the above problem depending on the risk classification:

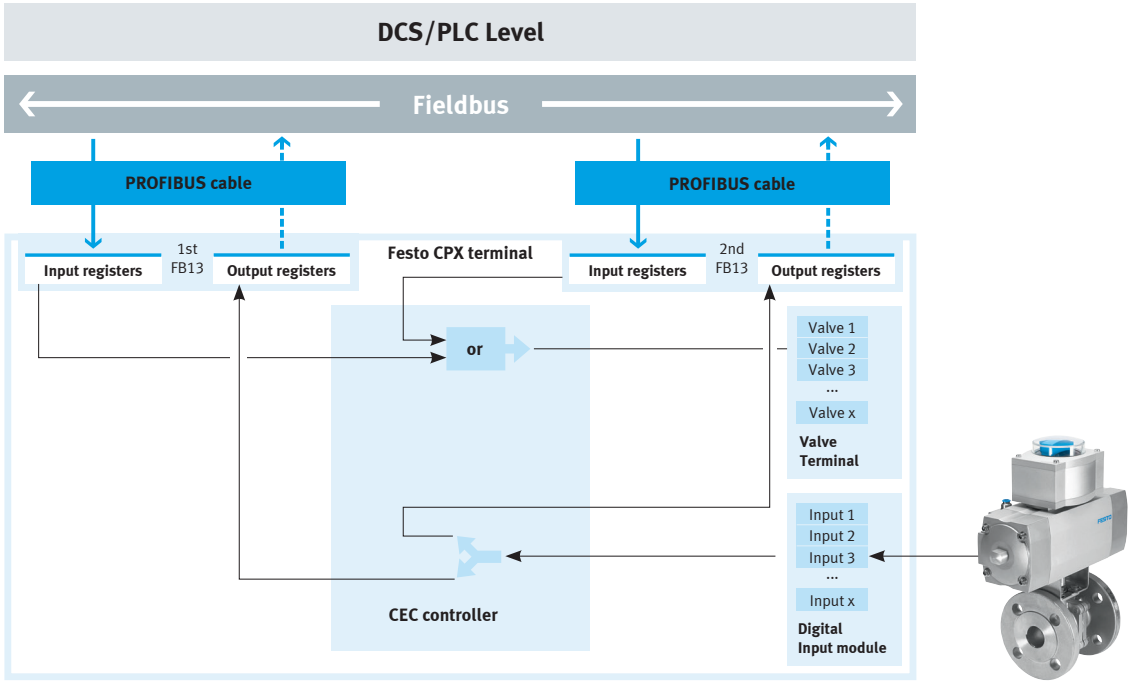


Schematic diagram of a stirred-tank reactor

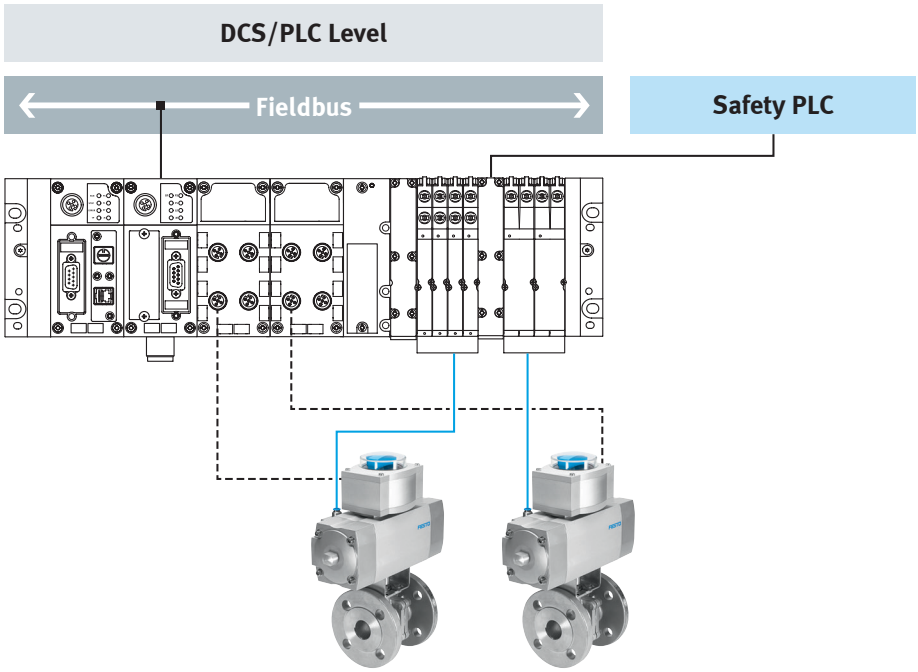
© Copyright 2017, Festo AG & Co. KG

5.1. A redundant PROFIBUS solution can be used to increase the safety between the control system (DCS) and remote I/O.
If a PROFIBUS line is removed or the PROFIBUS node is faulty, the second PROFIBUS line/node takes over. They will continue to reliably send and receive the control system protocols.

Additional advantage:
The remote I/O can be directly accessed on site via a controller with an Ethernet interface and parameterisation can be performed or additional processes can be implemented. The proven technology of the remote I/O, with its input modules for connecting NAMUR sensors, reliably takes over the tasks of the control level. The modular terminals, together with the SIL2-rated valve terminal, are a compact alternative.

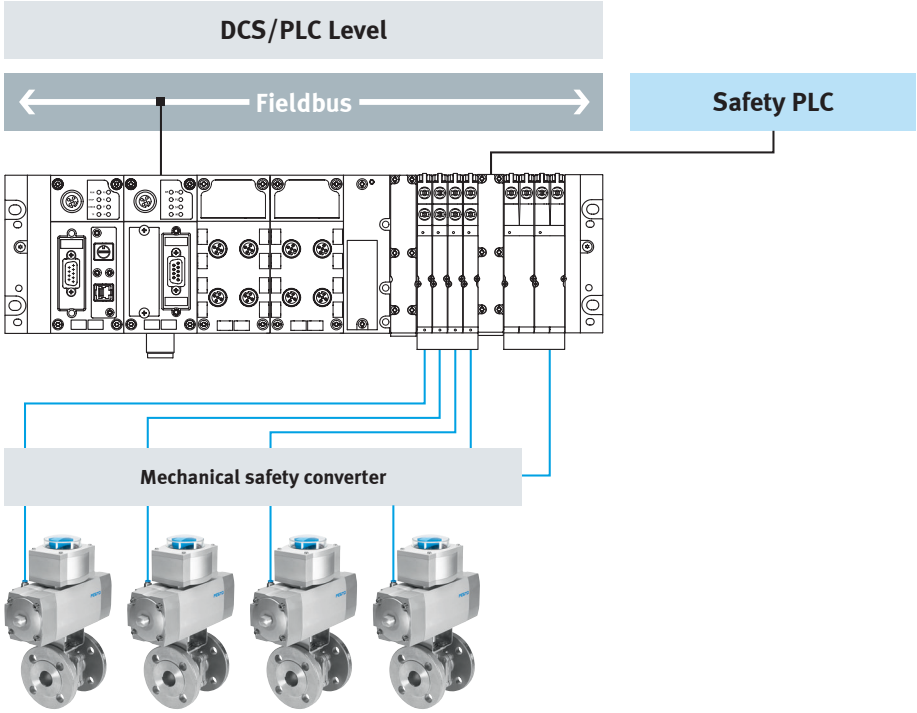


5.2. Valve terminal with integrated safety shutdown
The operating mode is activated via fieldbus modules and a valve terminal with actuators arranged in series. The valve terminal has a separate supply to the safety PLC, which actuates the separate valves. It also activates the actuators that shut down the process safely. This solution is suitable for SIL 2 circuits. To increase the safety level, there is also an option of interconnecting the valves redundantly.

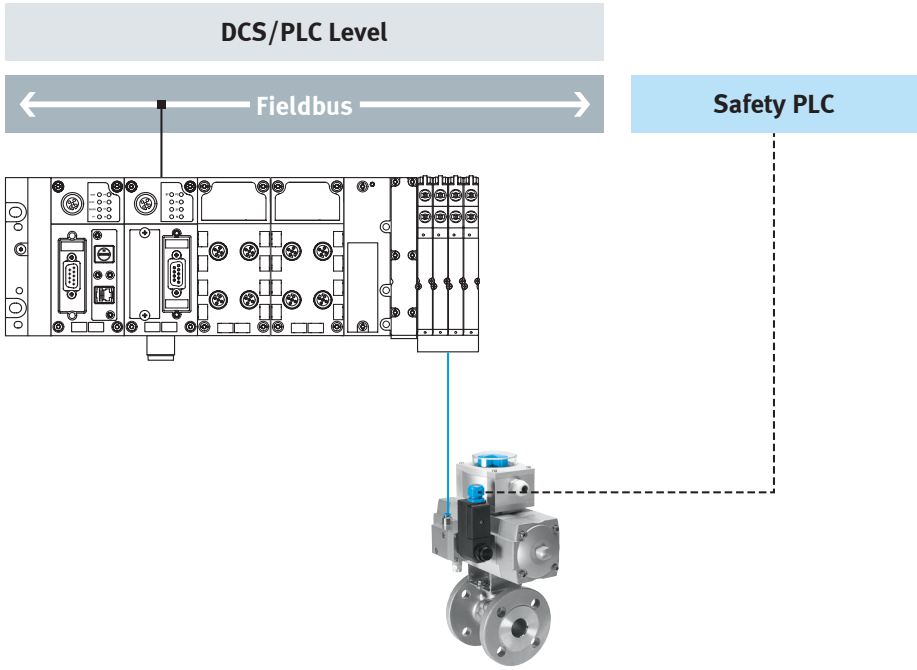


© Copyright 2017, Festo AG & Co. KG

5.3. Valve terminal with integrated safety shutdown
In operating mode, the valve terminal is activated via a fieldbus and controls actuators in the process. In addition, the valve terminal has a separate supply to the safety PLC, which actuates the valves on the valve terminal for the safety shutdown. It is exhausted via an additional 3/2-way valve, which is operated in normal mode, thus preventing the check valves installed in the branch lines from opening. In addition, by monitoring the pressure the switching position of the valve is safeguarded. It also controls the same actuators in order to shut down the process safely. This solution is suitable for SIL 2 circuits. To increase the safety level, there is an option to switch the valves redundantly.



5.4. Valve terminal plus individual valve for safety shutdown
The operating mode is activated via the fieldbus and the valve terminal, and is used to control actuators in the field. The certified individual valve mounted on the same actuator is directly actuated by the safety PLC and, if required, switches off safely. These valves can be used in safety-related circuits up to SIL3 level.



© Copyright 2017, Festo AG & Co. KG

6. Proven performance and extended service life using the example of a solenoid valve

Globalisation, especially in the chemical industry, is forcing companies to constantly increase their system performance. This is mainly to compensate for the drop in prices in the market and to stay competitive. As modern process engineering systems are highly optimised, increased levels of output can only be achieved with a reliably functioning, highly productive system without downtimes. This means reducing inspection cycles and inspection times, as well as avoiding idle times or downtimes caused by repairs carried out outside of the maintenance or downtime schedule.

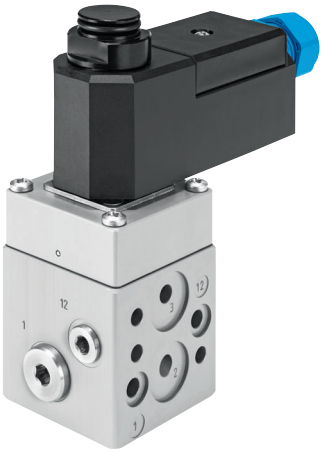
One way of achieving this is by using reliable electrical instrumentation and control technology components, such as solenoid valves, that are certified in accordance with IEC 61508.

However, even certified solenoid valves vary significantly in terms of performance and safety specifications. There are many solenoid valve solutions available on the market for safety installations, especially for low demand mode. Many of these solutions have a limited service life or have requirements in terms of downtime or the number of switching cycles required per year in order to meet safety specifications.

Increasing reliability is a prerequisite for extending the test intervals. This also means that large amounts of money can be saved. In oil refineries, it has long been common for shutdowns to take place only every five years. The high level of reliability is primarily achieved thanks to the "two from three philosophy" (2oo3) and is supported by redundant systems and devices. This more expensive option pays off thanks to the high capacity of these systems. This does not always apply to chemical plants. Nowadays, plants are trying to achieve a level of reliability similar to that of redundant components by using certified, highly reliable devices (electric motors, transmitters, controllers, solenoid valves or even process valves).

Piloted, poppet-type solenoid valves with TÜV approvals to IEC 61508 up to and including SIL 3 are available on the market. These valves, in accordance with the latest SIL classification, will guarantee a failure probability rate of 2.41 E-4. In other words, if used properly, a maximum of one faulty operation will occur in 2,410 switching cycles.

SIL-certified solenoid valves have now been in use since 2002. Solenoid valves that date from this period and have been used since then have had their original safety levels checked during laboratory tests. This means that there are now SIL-certified solenoid valves that do not need a time limitation on their certificate. When these solenoid valves were retested in the laboratory, poppet-type solenoid valves were shown to have almost the same short switching times, even after more than 12 years of use and even when compared to new valves. In addition, their sealing tightness, externally and around the sealing seat, is completely safeguarded.



3/2-way piston poppet valve with extended NAMUR port and TÜV certificate in accordance with IEC 61508

© Copyright 2017, Festo AG & Co. KG

7. Redundant activations of actuators in the field

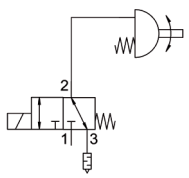
If the measures described under "6 Proven performance and extended service life using the example of a solenoid valve" are not sufficient, solenoid valves can still be redundantly interconnected (HFT1 or HFT2) as described above.

Process safety and availability are always paramount when using redundancies. Current safety circuits in process engineering are 1oo2 (One out of Two), 2oo2 (Two out of Two) and 2oo3 (Two out of Three). These are used in the production and processing of high-value and dangerous substances such as crude oil, natural gas, chemicals etc.

7.1. The functions in the circuit diagram

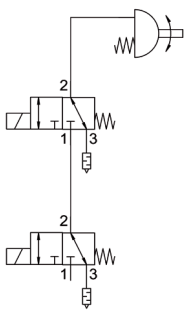
To provide redundancy in the event that a valve fails, the systems are installed in safety- or process-critical systems. Their compact design reduces the cost of the piping as well as the potential for leaks in the system. This saves costs during assembly and operation.

1oo1 (One out of One)



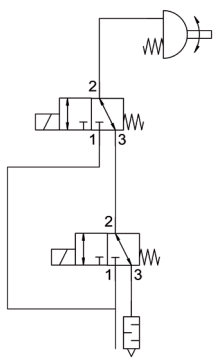
A single failure can lead to an unsafe condition.

1oo2 (One out of Two)



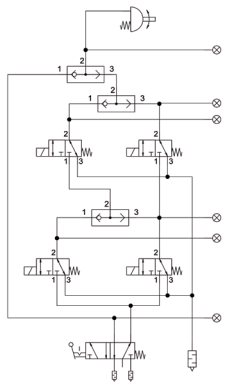
Safety
If a valve failure is detected, the entire system is exhausted. This leads to an unsafe condition and system moves to a safe position.

2oo2 (Two out of Two)



Availability
Only when both valves fail is the correct function no longer ensured and this leads to an unsafe condition.

2oo3 (Two out of Three)



Safety and availability
At least three failures must occur simultaneously to cause an unsafe condition. For function see 7.5.2

Overview of the most common redundant activations of actuators in the field

7.2. Increased safety (1oo2)

With enhanced safety (1oo2), two valves are connected in series. Both are energised during operation. Should a valve or one of the control signals fail during operation, the entire system is exhausted in order to protect it from subsequent damage. Media conveyor lines frequently require this higher level of safety.

7.3. Increased availability (2oo2)

With enhanced availability (2oo2), two valves are connected in parallel. Both are energised during operation. Should a valve or one of the two control signals fail during operation, the plant remains active and the entire system continues to work. For example, cooling circuits require this enhanced availability.

7.4. Increased safety and availability (2oo3)

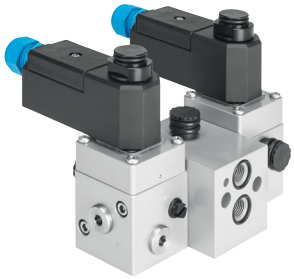
A 2oo3 circuit combines increased safety and increased availability. The advantage is that the functionality of the individual valves can be tested during operation without activating the actuator. This valve combination is also used in highly critical applications in the oil and gas industry as well as in refineries.

© Copyright 2017, Festo AG & Co. KG

7.5. Available solutions

7.5.1. Increased safety of NAMUR block (1oo2) and increased availability (2oo2)

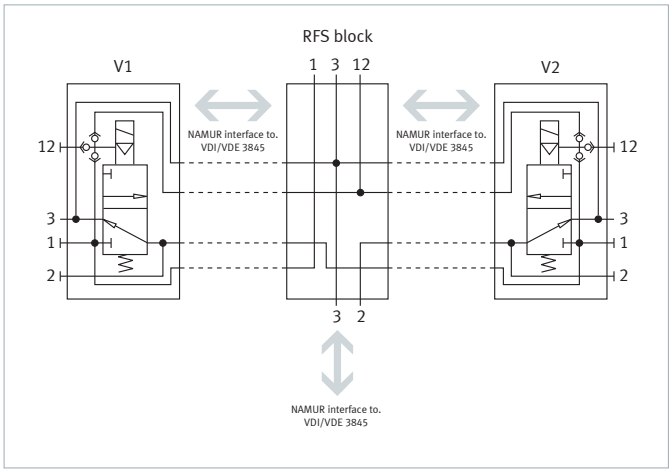
The NAMUR block enables two solenoid valves with a NAMUR port pattern to be installed. The NAMUR interfaces make redundancy easy to implement. The advantages: low warehousing costs and easy replacement of solenoid valves.



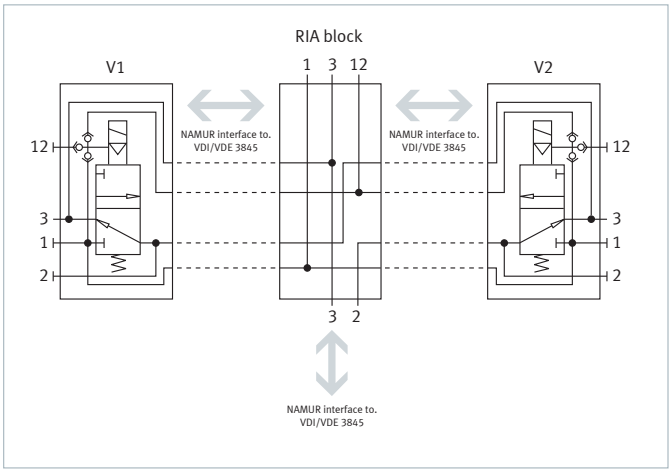
Redundant NAMUR block

The NAMUR block can be mounted directly on quarter turn actuators using the NAMUR interface. Separate installation with suitable piping is also possible.

Using the additional auxiliary power terminal, the NAMUR block can also be used with piloted solenoid valves on actuators that have positioners for fail-safe functions.



Redundant Fail Safe – 1oo2

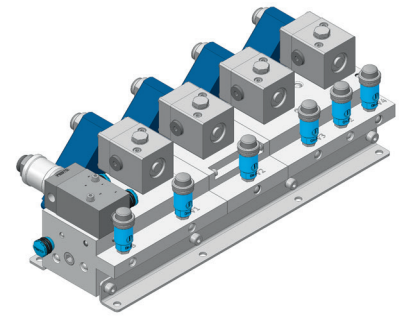


Redundant Increased Availability – 2oo2

7.5.2. Safety and availability Inline/Namur (2oo3)

There is a combination that provides maximum safety and availability at the same time. This so-called 2oo3 system combines both technologies and meets the highest demands of a system.

The valve block is an inline variant and is integrated into the system. The standard valves installed on the block are defined and mounted on the block via the NAMUR interface in accordance with VDI/VDE 3845. This combination means that the block is installed only once and the valves are only replaced via the NAMUR interface as necessary according to a service life/safety lifecycle plan. In addition, with the 2oo3 system the functions of the four valves can be bypassed. This bypass can be unlocked with a key so that maintenance can be carried out during operation. The pressure indicators, mounted directly on the valve block, always give a reliable and swift indication if a valve is pressurised.



Example of a 2oo3 function block

Author:
Reiner Laun
Industry Segment Management

Festo AG & Co. KG
Rechbergstr. 19
73770 Denkendorf, Germany
Tel.: +49 711 347 76585
reiner.laun@festo.com

© Copyright 2017, Festo AG & Co. KG