

Functional safety in the process industry

FESTO



SIL certified

You want that feeling of security.
You require uninterrupted production.
We bring you safety and reliability.

→ **WE ARE THE ENGINEERS
OF PRODUCTIVITY.**



Page 3

SIL – Safety Integrity Level

Page 4

SIL in concrete terms

Our
expertise

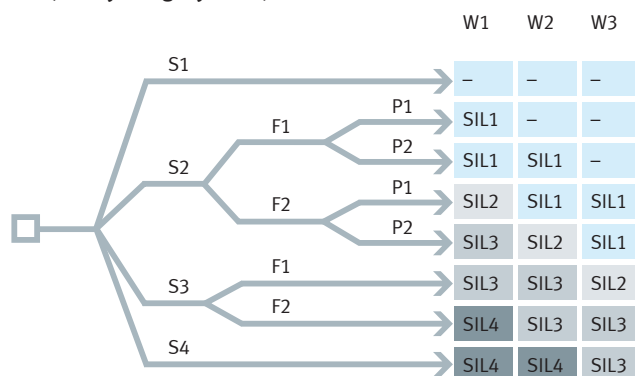
**Your
advantage**

SIL – Safety Integrity Level

Safety equipment in process plants aims to reduce the hazards presented by processes for people, the environment and property to the lowest possible, acceptable level. Depending on the potential hazards, plants are assigned a Safety Integrity Level (SIL1 to SIL4). SIL1 represents the lowest risk and SIL4 the highest acceptable risk with catastrophic consequences.

As a general principle, the more hazardous the plant, the more reliably its safety equipment must operate in case of an emergency. Once a plant is assigned a SIL level, specific installation principles must be observed, e.g. redundant design. This enables the risk to be reduced to the greatest possible extent in the event of a malfunction.

SIL (Safety Integrity Level)



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 several 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

Page 6

Components for safety-related applications

Page 9

Redundant system conditions for safety-related applications

Page 12

Solutions for safety-related applications

SIL in concrete terms

The standards:

The basic standard for functional safety is IEC 61508, entitled "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems". IEC 61511, entitled "Functional Safety – Safety Instrumented Systems for the Process Industry Sector" applies to process automation.



IEC 61508 describes the method for assessing risks (using a riskograph) and the measures required to design suitable safety functions, ranging from sensors and logic circuits to actuators.

A safety circuit, or SIS – Safety Integrated System – normally 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

IEC 61511 describes the specific implementation of IEC 61508 for the process industry. The focus here is on applications with a low demand mode. In process plants, this represents most safety functions.

Important to know

The requirement for failure probability 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 can.

Relevant characteristic values for calculating SIL

• PFD (Probability of Failure on Demand):

Probability that a safety function will fail in low demand mode (demand rate/year < 10)
Low Demand

• PFH (Probability of Failure per Hour):

Probability that a safety function will fail during continuous use (demand rate/year > 10)
High Demand

• SFF (Safe Failure Fraction):

Proportion of safe failures out of the total number of failures

• HFT (Hardware Failure Tolerance):

Ability of a requested function to continue to perform during errors and deviations

HFT0: An individual error can lead to the loss of the safety function, e.g. 1oo1 connections

HFT1: At least 2 errors must occur simultaneously in order to cause a failure of the safety function, e.g. 1oo2 connections

HFT2: At least 3 errors must occur simultaneously in order to cause a failure of the safety function, e.g. 1oo3 connections

• λ (Failure rates):

S : Total failure rate for safe failures

SD: Failure rate for safe, identifiable failures

SU: Failure rate for safe, unidentifiable failures

D: Total failure rate for dangerous failures

DD: Failure rate for dangerous, identifiable failures

DU: Failure rate for dangerous, unidentifiable failures

• MTBF (Mean Time Between Failure):

Mean time between two successive failures




• Device type A:

Device for which the failure behaviour of all components and the failure characteristics are adequately determined, e.g. through operational reliability.

• Device type B:

Device for which the failure behaviour of at least one component and the behaviour in the event of a failure are not adequately determined.

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

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}					

Defined by the manufacturer
To be determined by the system operator

What does SIL mean for operators?

A company that erects and operates a system which represents a potential hazard for employees, local residents or the environment must minimise the risk presented by the process under fault conditions.

To achieve end, both IEC 61508 and IEC 61511 essentially require the following steps to be carried out:

1. Risk definition and rating

according to detailed failure probabilities for everything from sensors to controllers and actuators for the entire service life of the components.

2. Definition and implementation of measures

to minimise residual risk.

3. Use of suitable equipment

(evaluated or certified)

4. Periodic tests and inspections

to ensure correct observation of the safety functions.

Target: $SIL \geq SIL_r$

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	$3 \times 10^{-6} \leq PFH < 10^{-5}$	One risk of failure every 1,250 days	HFT 0				HFT 1	HFT 0			$10^{-2} \leq PFD < 10^{-1}$	Once every 10 years
	$10^{-6} \leq PFH < 3 \times 10^{-6}$	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	HFT 2		
(per hour)												

Components for safety-related applications

The product range presented here is used in systems for safety-related applications in the chemical and petrochemical industries. Products with a SIL3 compliance or higher require certification to IEC 61508 by an autonomous organisation; for products up to SIL2 the suitability can be declared by the company itself. The characteristic values required to calculate the achievable SIL level of an SIS system are detailed in the relevant certificate or user documentation.

Components with SIL certificate

Pilot valves VOFC



For safety-related systems up to SIL3 in redundant circuits or up to SIL2 in single-channel circuits for low demand, high demand and ESD (Emergency Shut Down) applications.

- Design principle: pilot operated
- Explosion protection to IEC Ex: EPL Gb/ EPL Db
- Explosion protection to ATEX: II 2 G / II 2 D
- Types of ignition protection, solenoid coils: Ex ia, Ex me, AEx-m
- IP65 housing protection
- Surface finish: aluminium (Ematal coated) – stainless steel
- Operating conditions: indoors/outdoors



Pilot valves VOFD



For safety-related systems up to SIL3 in redundant circuits or up to SIL2 in single-channel circuits for low demand, high demand and ESD (Emergency Shut Down) applications.

- Design principle: direct acting
- Explosion protection to IEC Ex: EPL Gb / EPL Db
- Explosion protection to ATEX: II 2 G / II 2 D
- Types of ignition protection, solenoid coils: Ex me, Ex d, AEx-d
- IP65 housing protection
- Surface finish: Aluminium (Ematal coated) – stainless steel
- Operating conditions: indoors/outdoors



Quarter turn actuator DFPD



Double- and single-acting for activating process valves in safety-related systems up to SIL3 in a redundant design or to SIL2 in single-channel design in low demand and high demand applications.

- Temperature range: –50 ... + 150 °C
- Explosion protection to ATEX: II 2G c T4 X / II 2 D c 125 °C X
- Rotation angle up to 180°
- Surface finish: stainless steel shaft, housing with epoxy coating



Sensor box SRBC



For the electronic and visual position indication of automated process valves in safety-related systems up to SIL2 for low-demand and high-demand applications.

- Housing protection IP67/NEMA 4/4X
- Type of ignition protection: Ex ia
- Explosion protection to ATEX: II 2G c X / II 2D c X
- cCSAus: ordinary location
- Operating conditions: indoors/outdoors



Sensor box SRBE



Visual position indication and electrical position sensing of automated process valves in safety-related systems up to SIL2 for low-demand and high-demand applications.

- Housing protection IP67/NEMA 4/4X
- Types of ignition protection: (A)Ex d, (A)Ex tb
- Explosion protection:
 - To IEC Ex: EPL Gb / EPL Db
 - ATEX: II 2G / II 2D
 - CSA:
 - Class I, Div 1; Class I Div 2
 - Class II, Div 1; Class III, T4A
 - Class I, Zone 1; Class I, Zone 21
- Operating conditions: indoors/outdoors



How to find the SIL certificates/declarations

1st step:

→ www.festo.com/supportportal

2nd step:

Enter the product type or part number

Search

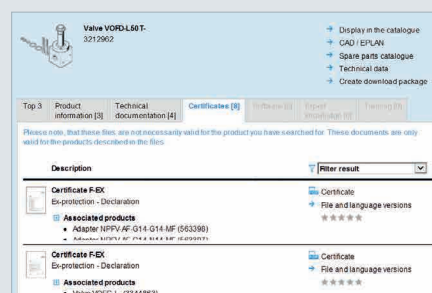
VOFD

Find

Help

3rd step:

Click on the Certificates tab



4th step:

SIL certificate/declaration



Components with SIL manufacturer's declaration

Pilot valves VSNC



With changeable seal for 3/2- or 5/2-way function, 5/2-way double solenoid and 5/3-way design. For safety-related systems up to SIL2.

- Design principle: pilot operated
- Types of ignition protection, solenoid coils:
Ex ia, Ex m, Ex na, AEx-m
- IP65 housing protection
- Surface finish: aluminium
- Operating conditions: indoors



Pneumatic linear actuator DLP



Double-acting opening/closing linear actuator to activate process valves in safety-related systems up to SIL2.

- High corrosion resistance (CRC 3) for outdoor installations
- Contactless position sensing
- Port pattern to Namur VDI/VDE3845 for mounting solenoid valves
- ATEX certification: II 2 GD



Pneumatic valve terminal MPA



Maximum function integration, many electrical connection options, multi-pin plug, Festo I-Port, fieldbus and a comprehensive diagnostics concept. Suitable for use in safety-related systems up to SIL2.

- Different manifold block materials
- Optimised variants with increased flow rate
- Fast-switching valves available
- IP20 variant ideal for control cabinet solutions



Pneumatic valve terminal CPV



Intrinsically safe valve terminal with pneumatic multiple connector plate with wall through-feed, for use in safety-related systems up to SIL2.

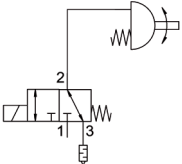
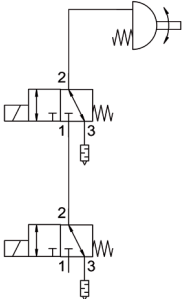
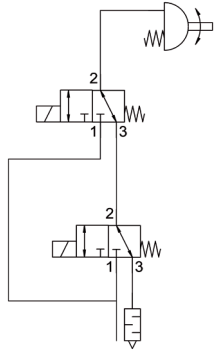
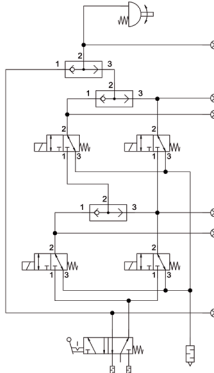
- Protection class to IP65
- Protection class IP65 also in conjunction with pneumatic multiple connector plate for control cabinet assembly
- CE marking
- Can be directly installed in Ex zone 1/21



Redundant system conditions for safety-related applications

Process safety and reliability are always at the forefront when using redundant systems. 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.

The functions in the circuit diagram

1oo1 (One out of One) 	1oo2 (One out of Two) 	2oo2 (Two out of Two) 	2oo3 (Two out of Three) 
<p>A single failure can lead to an unsafe condition.</p>	<p>Safety If a fault is detected in a valve, the entire system is exhausted. This leads to an unsafe condition and the system moves to a safe position.</p>	<p>Increased uptime Only when both valves fail is the correct function no longer ensured and this leads to an unsafe condition.</p>	<p>Safety and reliability At least three failures must occur simultaneously to cause an unsafe condition.</p>

To provide redundancy in the event that a valve fails, the above mentioned systems are installed in safety- or process-critical systems. Their compact design reduce the cost of the piping and simultaneously the potential for leaks in a system. This reduces assembly and operating costs of the plant.

Most widely used redundant systems at field level

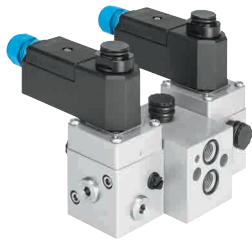
Safety (1oo2)

With enhanced safety (1oo2), two valves are connected in series. Both valves are energised during operation. Should a valve or a solenoid 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.

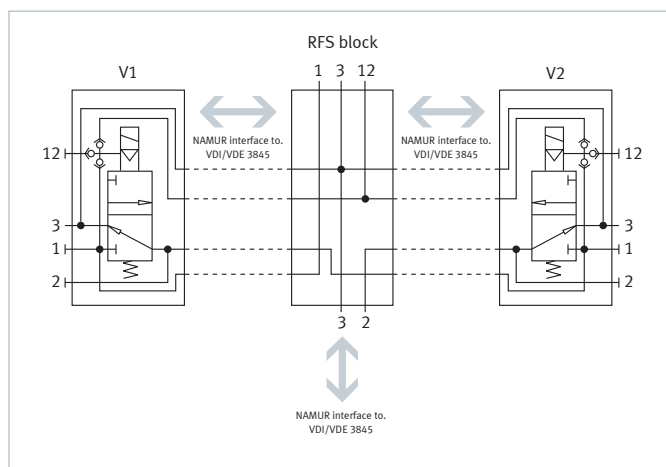
Increased uptime (2oo2)

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

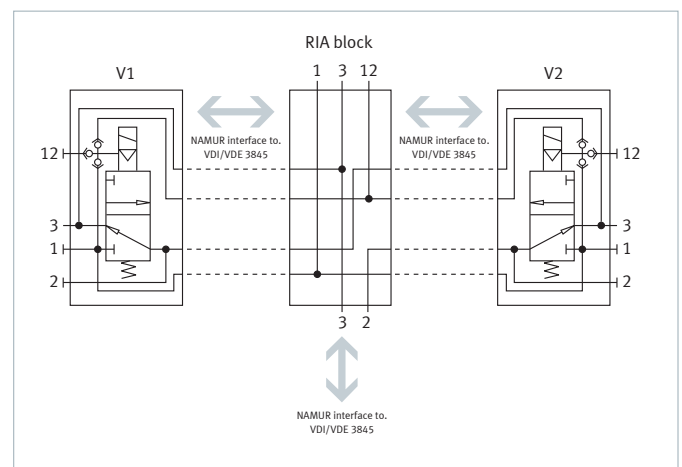
Redundant NAMUR block (1oo2 & 2oo2)



- The NAMUR block enables the installation of two solenoid valves VOFC or VOFD. The NAMUR interfaces make redundancy easy to implement. The advantages: low warehousing costs and easy replacement of solenoid valves.
- Both solenoid valves are redundantly interconnected and provide a redundant function for automated process valves. The blocks are available in fail-safe function (1oo2) or with increased uptime (2oo2)
- The NAMUR block can be mounted directly on quarter turn actuators using the standardised interface. Separate installation with suitable piping is also possible.
- With 1oo2 and using the additional auxiliary power terminal, the NAMUR block can also be used with piloted solenoid valves on actuators that have a positioner for fail-safe functions.
- High flexibility due to the available types of ignition protection and global certification of the solenoid coils.
- Available with G and NPT connections.



Redundant Fail Safe – 1oo2



Redundant Increased Uptime – 2oo2

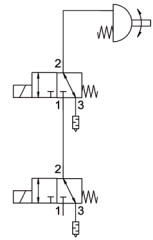
Redundant INLINE valves (1oo2 & 2oo2)



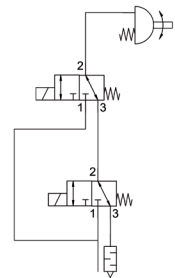
With these compact systems, Festo is drawing on the tried and trusted technology (proof-in-use) of the valves VOFD and is combining this in one housing. Thanks to the Ematal coating, these valves meet the highest safety standards in process engineering and can withstand the toughest of ambient conditions. Available types of ignition protection: Ex me, Ex d.

- Simple replacement of individual valve installations.
- The valve's redundant circuit ensures a redundant fail-safe function (1oo2) or provides increased uptime (2oo2) for automated process valves.
- High flexibility due to the available types of ignition protection and global certification of the solenoid coils.
- Compact and robust housing for installations in harsh ambient conditions.
- Available with G and NPT connections.

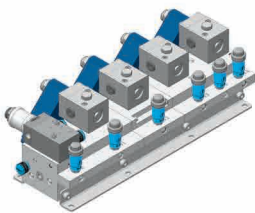
1oo2 (One out of Two)



2oo2 (Two out of Two)



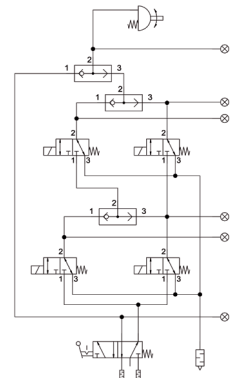
Safety and reliability Inline/ Namur (2oo3)



There is a combination that provides maximum safety and reliability at the same time. This so-called 2oo3 system combines both technologies and meets the highest demands of a system. The block is an inline variant and is integrated in your system. The built-in standard valves are mounted on the block via the NAMUR interface. This opens up the opportunity for diversity in the design. It also means that individual valves can be easily replaced. 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.

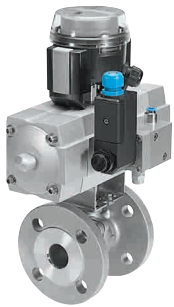
The mechanical pressure indicators or pressure gauges, mounted directly on the valve block, always give a reliable and swift indication if a valve is pressurised. In addition, the mechanical displays can be replaced with electronic pressure sensors in order to reflect the status in the control system.

2oo3 (Two out of Three)



Solutions for safety-related applications

1. Actuator units from Festo – ready to install



Complete actuator units, whether single- or double-acting, save you time and money. We will build your ready-to-install and tested actuator unit in accordance with your requirements – including for safety-related systems. To do this, we use automated process valves based on certified components with a corresponding SIL manufacturer's declaration.

- Fully assembled to your specifications
- Costs and time saving
- Ready to install
- SIL or ATEX assessment of the actuator with the corresponding manufacturer's declaration possible
- Designs for low temperatures

2. Panel and control cabinet solutions for safety-related applications



Piped pneumatic control systems

Festo offers a broad spectrum of pneumatic control systems. Our offer encompasses all stages of the value chain, from initial planning and engineering up to assembly, testing and delivery of the ready-to-install panels.

Control cabinets for the process industry

Control cabinet solutions tailored to your specifications and requirements protect the components used against environmental factors, fluids and foreign matter. You decide whether tubing or piped connections are more suitable for your purpose.



Regardless of whether you are using pneumatic, electric or electropneumatic components, you will receive a control cabinet that is completely in line with your requirements. On request, we can subject the entire cabinet to a SIL assessment. For explosion protection, we also manufacture control cabinets in a 2GD or 3GD design with international approvals and in accordance with the U.S. NEC standard.



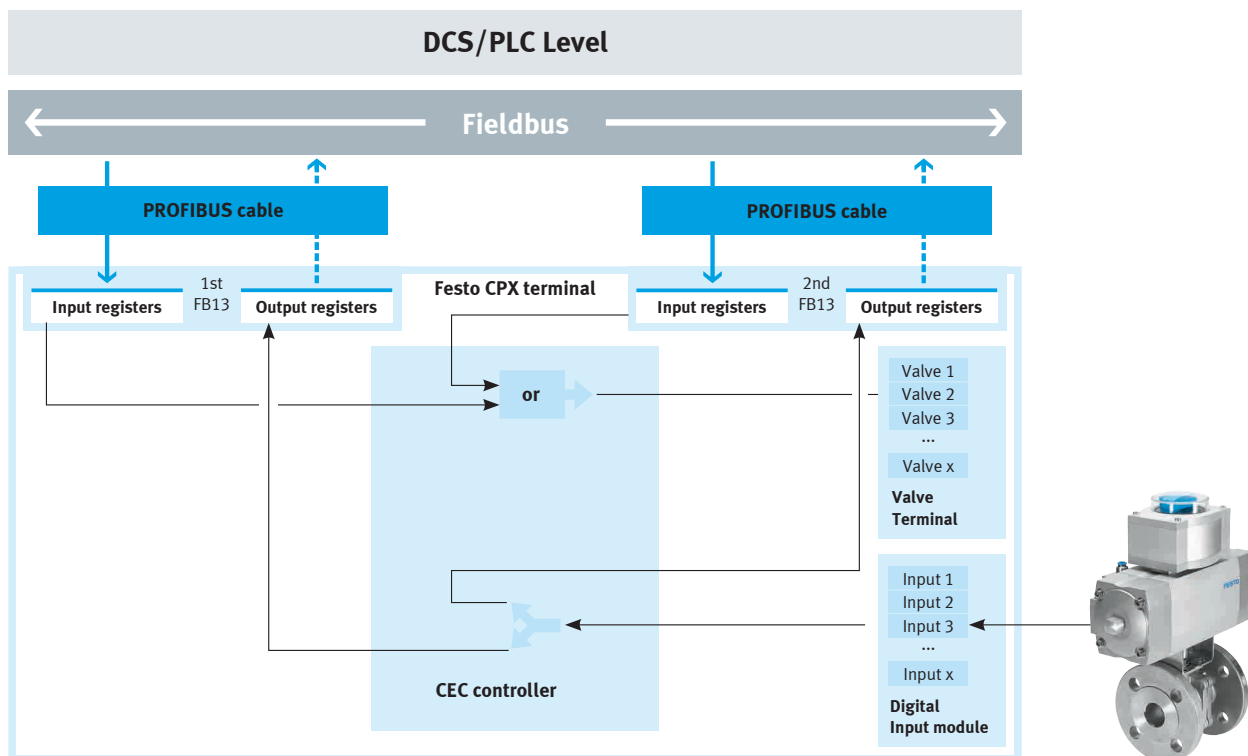
3. Current solutions for batch processes

3.1 PROFIBUS redundancy

Festo uses a redundant PROFIBUS solution 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. This reliably sends and receives the control system protocols.

It has the further benefit that you can access the remote I/O directly on site via a controller with Ethernet interface and parameterise or implement additional processes. The tried-and-tested technology of the CPX-P, with its input modules for connecting NAMUR sensors, reliably takes over the tasks of the control level.

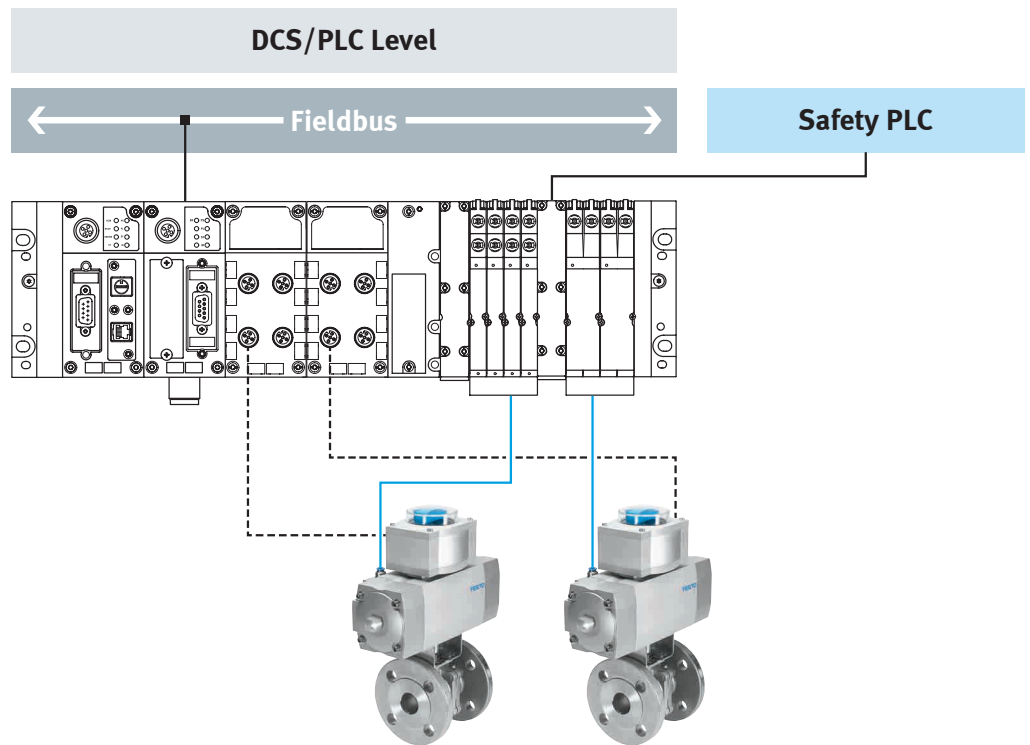
The modular terminal CPX together with the SIL2-rated valve terminal MPA is a compact alternative.



3.2.1 CPX/MPA with safety PLC

Valve terminal with integrated safety shutdown to control separate actuators.

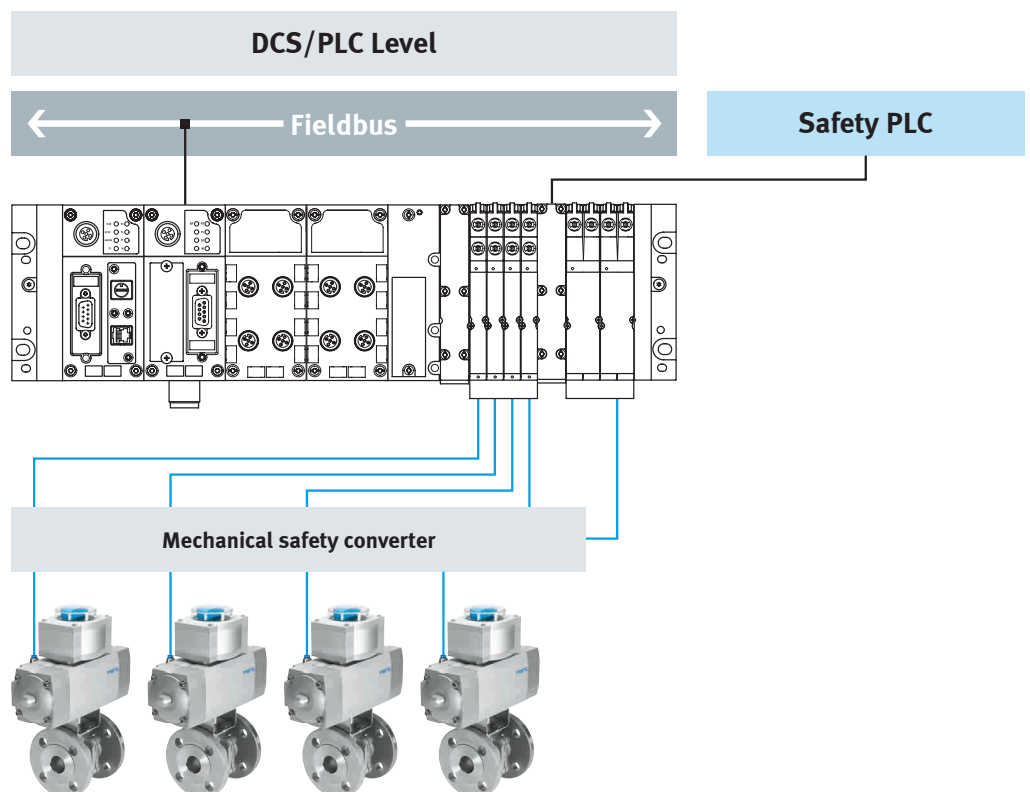
In the operating mode, the valve terminal is activated via a fieldbus and switches actuators in the process. In addition, the valve terminal has a separate supply to the safety PLC, which actuates the valves on the valve terminal for the safety shutdown. The actuators for the operating mode and the actuators for the safety shutdown are connected in series. This solution is suitable for SIL2 circuits. To increase the safety level, there is also an option of interconnecting the valves redundantly.



3.2.2 CPX/MPA with safety PLC

Valve terminal with integrated safety shutdown to control actuators for operating and safety mode.

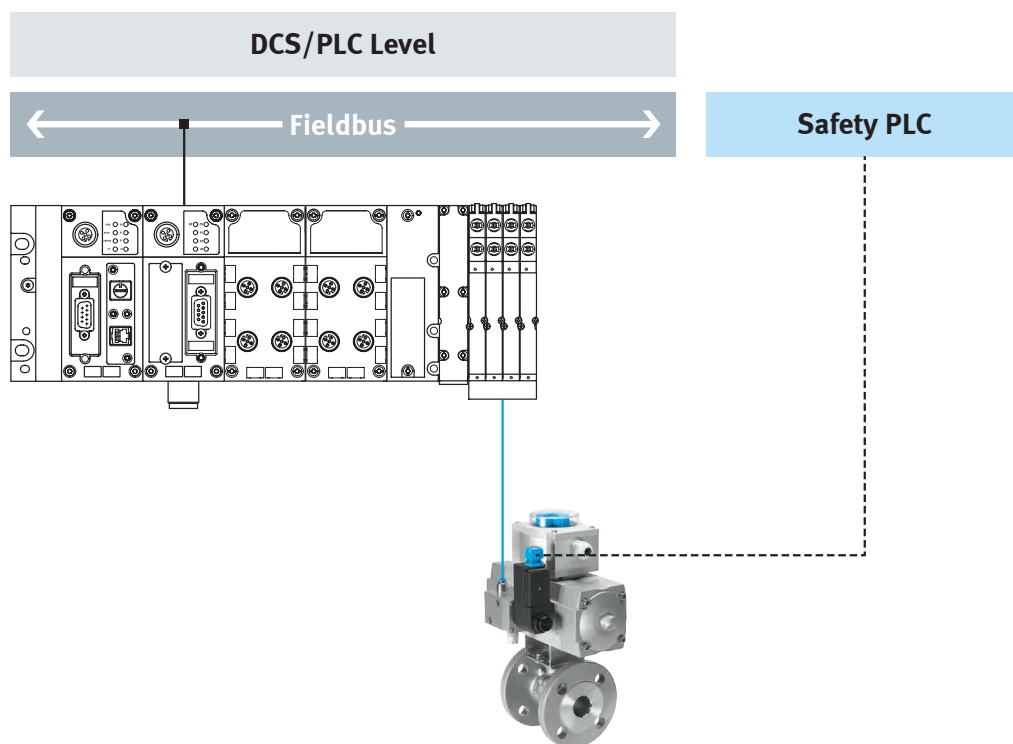
In operating mode, the valve terminal is actuated via a fieldbus and switches actuators in the process. In addition, the valve terminal has a separate supply to the safety PLC, which actuates the valves on the valve terminal for the safety shutdown. It also activates the same actuators in order to shut down the process safely. This solution is suitable for SIL2 circuits. To increase the safety level, there is an option to switch the valves redundantly.



3.3 VOFC/D as a safety valve

Valve terminal plus individual valve for safety shutdown.

The operating mode is controlled via the fieldbus and the valve terminal and is used to switch 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.





Productivity

Maximum productivity is a question of ambition

Do you share this attitude? We would be happy to help you achieve this goal with our four outstanding qualities:

- Security • Efficiency • Simplicity • Competency

We are the engineers of productivity.

Discover new dimensions for your company:

→ www.festo.com/whyfesto