

Minimizing risk

SIL for the chemical industry

FESTO



This white paper has the following aims:

- What is SIL, why is the topic relevant for plant operators, and what are the common misunderstandings?
- What do certificates mean and how do you read them correctly?
- To what extent do durable components offer a helpful advantage?

Executive summary

Safety devices in process-industry plants are intended to reduce the dangers posed by these plants for human beings or the environment down to a level which is as low as possible. As risk rises, it is vital to lower the probability of dangerous failure on demand at every stage of the safety chain. Depending on its danger potential, a particular plant will be assigned to a safety integrity level (SIL).

In order to achieve the required SIL, it is necessary to consider the components on the one hand and the complete safety circuit on the other. The safety values of the components are shown in certificates. However, this can lead to misunderstandings because, for example, some standard-specific details are not specifically mentioned in a certificate – being able to read and interpret certificates correctly is therefore an important prerequisite.

How often a component must be tested depends on the required SIL and the failure probability. These considerations have an important economic component. Products with a low risk of failure increase productivity. Low risk of failure means tests do not have to be carried out so frequently – or can even be completely omitted. This also means that production no longer must be stopped temporarily. An illustrative example of efficient components in SIL circuits is a piston poppet valve from Festo, which is used worldwide in the chemical industry.

Safety, risk and risk reduction

There are many facets to safety. Safety device failure can be costly at several levels: plant failures can lead to material damage, but also, depending on the industry, to injury to people and pollution of the environment. At the same time, even the smallest deviation in the process always has an economic aspect. The plant must be switched off and checked. Safety devices in process-industry plants should reduce these dangers down to an acceptable level which is as low as possible.

Depending on its danger potential, the plant or plant components will be assigned to a safety integrity level – the SIL. SIL-1 represents the lowest risk and SIL-4 the highest assumable risk with catastrophic consequences. SIL does not describe the suitability of a component, but refers to a complete safety circuit, also called SIS – safety instrumented system. This covers everything from sensor to logic and actuator technologies. However, the devices and components used for the safety circuit must be suitable for the corresponding level.

As a general principle, the greater the residual risk emanating from the process, the more reliably its safety devices must operate in case of an emergency. If a plant component is classified at a certain SIL level, the necessary passive and active protective measures must be observed. This minimizes the risk of an unsecured process. Protective devices reduce the residual risk to an acceptable level.

➤ The safety integrity level (SIL) describes the potential hazard posed by a plant or plant component. It determines the extent to which a risk must be reduced. It does not refer to individual components, but rather to a complete safety circuit. For this, however, it is necessary to use the appropriate components.

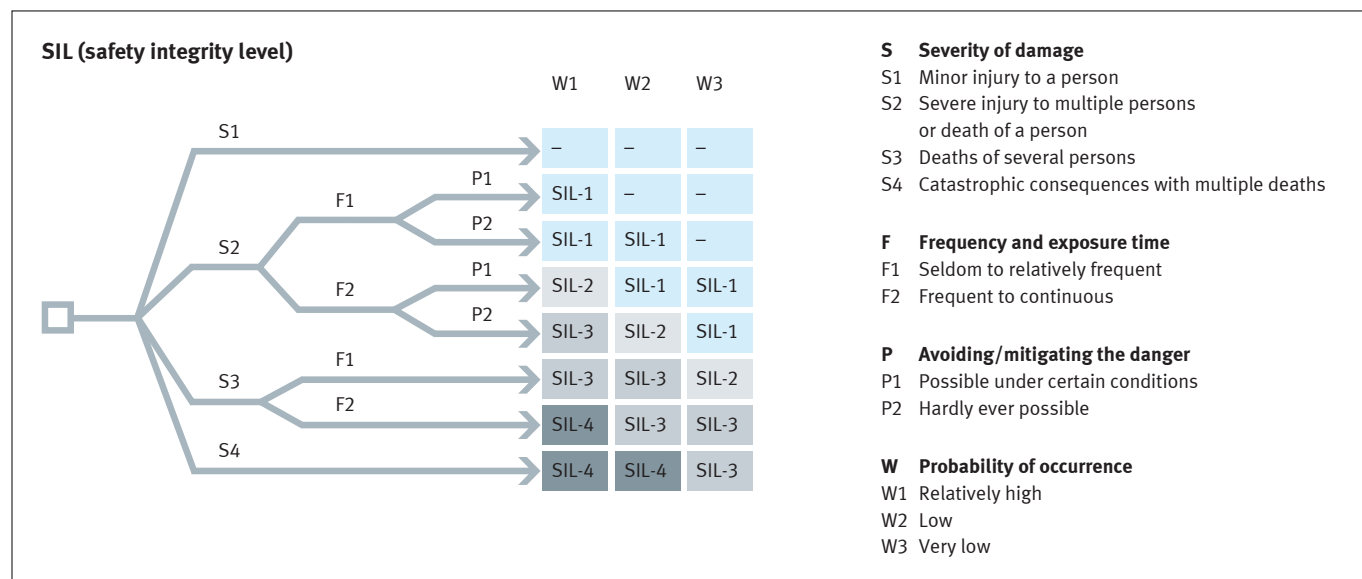


Figure: Risk graph for SIL rating

Standards, regulations and fundamentals

“There will always be a residual risk,” says Reiner Laun, Industrial Segment Manager Chemicals at Festo. Experts agree that there can be no absolute zero risk. It is therefore crucial to bring the risk to a generally accepted level.

Various standards now exist to create an international benchmark and make a clear comparison possible. The plant operators should be able to see as clearly as possible: How do we achieve the required reliability of safety devices?

The IEC 61508 standard specifies both the type of risk assessment and the measure for corresponding safety functions of sensors or internal logic processing. The decisive factors here are that systematic errors are avoided and also that errors that occur by chance remain manageable. This standard is independent of the application. It is therefore also referred to as the basic standard and is regarded worldwide as the basis for specifications, design and operation of safety-related systems.

Industry-specific standards have been derived from this, such as IEC 61511 for plant operators in process automation: This standard defines design criteria for components of the safety functions. This includes, for example, the so-called operational reliability of sensors and actuators. A product is considered “tried and tested” if it has functioned reliably under the special circumstances in the respective operation over a relatively long period of time in accordance with NE 130 ¹, in a verifiable and documented manner.

To understand how exactly these standards regulate risk and safety, it is worth taking a closer look at an example. The first rule here is that malfunctions can occur in a production process. “Electrical, mechanical and electromechanical components can fail because, among other things, they are exposed to wear and atmospheric influences,” says Carsten Schindler, Key Account Manager Chemistry at Festo: “Or the production process can go into a critical state. The decisive factor is that a safe condition is subsequently achieved again by means of protection and countermeasures.

➤ There will always be a residual risk – the decisive factor is to reduce it to an acceptable level. Standards specify both the type of risk assessment and the measures for corresponding safety functions. A common measure to achieve SIL-3 is the use of redundant systems.

¹ NAMUR recommendation 130:
Proven devices for protective devices in process control technology and simplified SIL calculation.

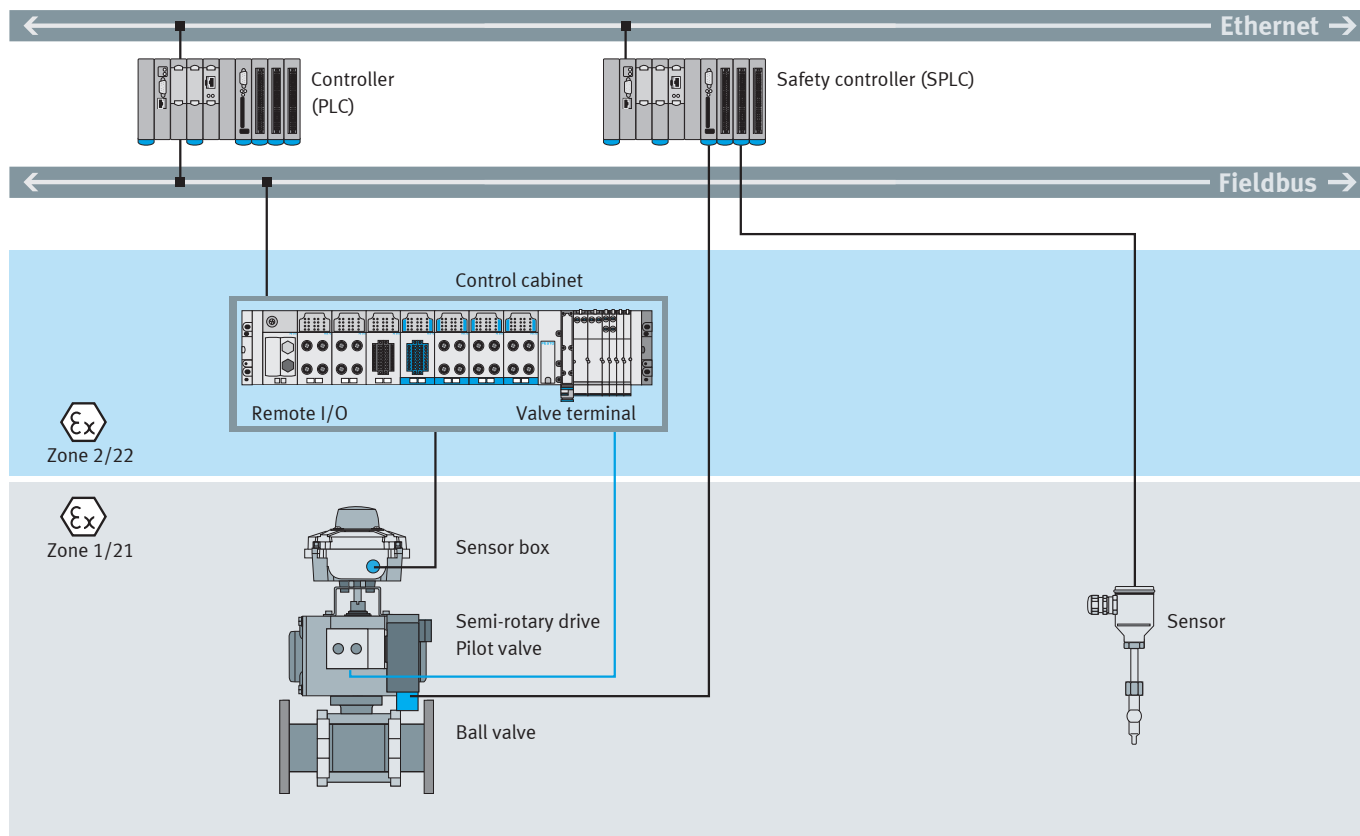


Figure: Sample SIL-2 safety circuit

The illustration shows a standard safety circuit that can be used to automate a mixer, for example. The mixer is filled with media via supply lines. The media flows through a process valve. This usually has no diagnostic function except position sensing and thus reaches a maximum of SIL-2 in this circuit. The programmable logic controller (PLC) determines when the process valve opens or closes. A safety risk arises if the PLC signal does not reach the valve correctly: for example, because the valve terminal does not switch off due to contamination of the compressed air line and thus the process fitting does not close. The liquid then continues to flow unhindered into the mixer.

The corresponding countermeasure: A sensor in the mixer signals that a critical level limit has been reached. It sends its signal to the safety PLC (SPLC), which in turn switches off a pilot valve that functions as a safety valve and is exclusively responsible for this situation. The process is brought into a safe state. However: This example does not provide any further protective measures if the entire actuator or the process valve itself is defective. The only remaining possibilities are an error message and checking by a worker on site.

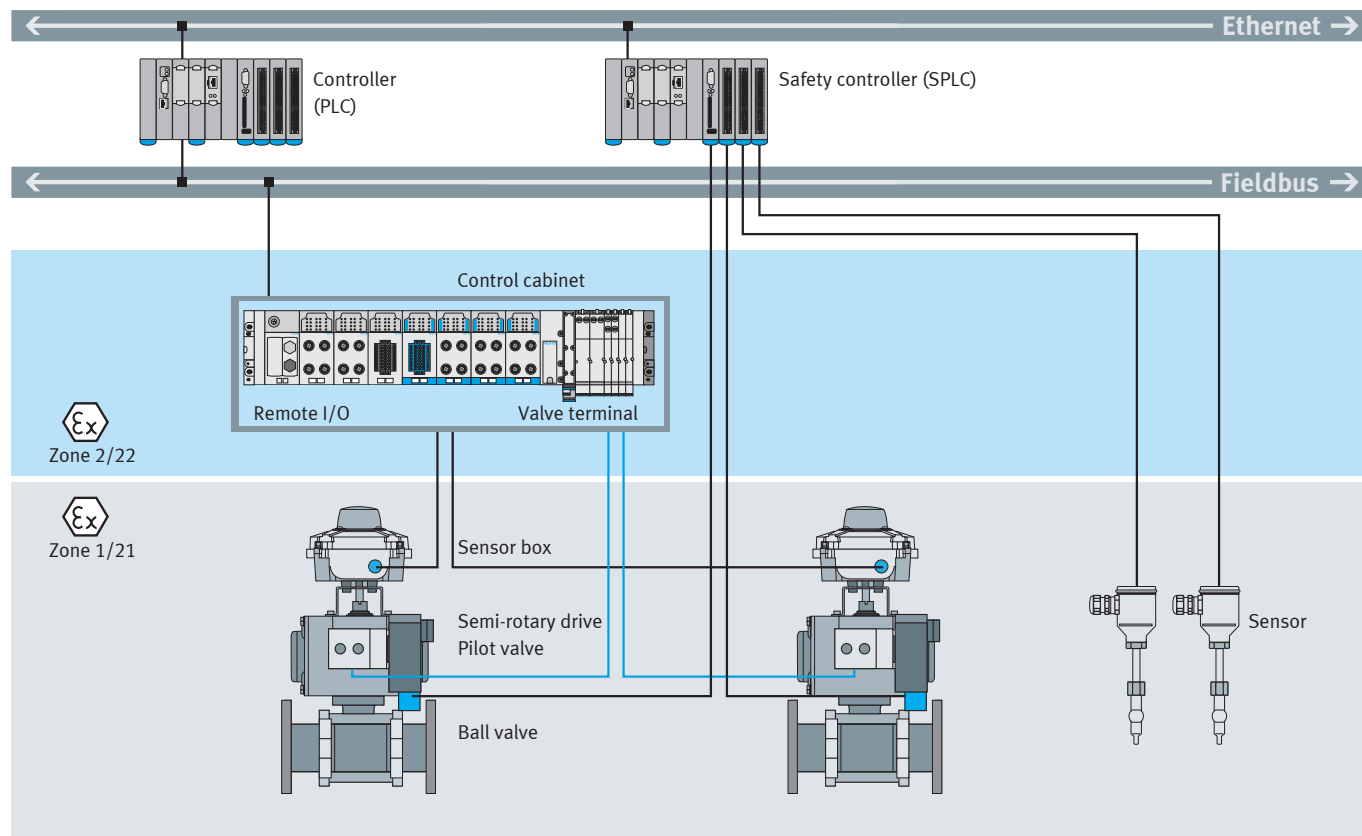


Figure: Sample SIL-3 safety circuit

If the SIL-2 circuit shown above is not sufficient because the reservoir overflowing would have extremely serious consequences, a design is required that further minimizes this risk: redundancy.

Instead of just a single process valve, two process valves are connected in series here. The probability that both valves will fail simultaneously is extremely slight. In addition, the risk can be minimized by installing additional sensors, so that the sensors are also designed redundantly. If required, protective measures can then be initiated by a sensor. In this way, SIL-3 can be achieved even with components that do not have a diagnostic function.

However, here too a systematic error, for example in the sensor technology, could mean that both valves do not switch back. Systematic errors include errors that either already exist at the time of delivery (e.g. software errors) or those that occur due to incorrect materials – possibly also because the product used is unsuitable for the intended task or the prevailing ambient conditions. One possible countermeasure is to use diverse components, i.e. components of different functional or design principles.

Guidance: Reading certificates correctly

Plant operators require proof of the suitability of the components used, preferably a manufacturer's declaration or a certificate from an independent organization such as TÜV² and Exida. However, certificates only show the suitability of the individual component in a safety circuit – the required architecture is often not apparent at first glance.

² Short for German: Technischer Überwachungsverein, English: Technical Inspection Association – a German association that provides inspection and product certification services.

The previous example serves to show that with components that do not have a diagnostic function, SIL-3 is only possible via a redundant circuit. This is the only way to compensate for the failure of a component. This is clearly described in IEC 61511, but can often be misinterpreted by wordings in the manufacturer's declarations and certificates. In addition, there are certificates in circulation that still do not have a standardized text – this can also cause misunderstandings.

1. A SIL-4 certificate is not necessarily the best

When the first SIL certificates for components were issued in the early 1990s, the entire band width of risk graphs was included – up to SIL-4. In reality, due to the excessive risk, building plant components that would require SIL-4 safety circuits are avoided. They would simply be too dangerous for people and the environment and too complex in the instrumentation of the SIL circuits with subsequent maintenance and testing. Therefore, only certificates with SIL-3 are issued now. However, corresponding SIL-4 certificates are still in circulation, which were issued at an earlier date. What this means is that if someone now comes across certificates that document “These components are suitable for systems up to SIL-4”, while another certificate only establishes a suitability of SIL-3, it can actually be the same product. In the second case, only with a more recent certificate that deliberately no longer takes SIL-4 into account. In this context, it should be remembered that SIL refers to the danger potential of a plant – the protective measures to be defined always depend on it.

It is crucial that faults are detected when they occur and that the appropriate countermeasures can be initiated. Standards ensure that there is clear regulation regarding which components and processes are necessary for this. To achieve safety integrity level 3, for example, redundancy of the valves ("double valve") is required.

2. A certificate that imposes many restrictions is not worse

There are currently various variants and wordings of certificates on the market which basically express the same thing. Newer certificates have gone over to formulating the respective suitability for use in detail. “This will probably gradually become the standard,” estimates Schindler. Until then, however, very different variants will be present on the market.

The devices of the aforementioned type series are suitable for use in safety-related systems up to and including SIL-3 to IEC 61508.

Figure: Outdated wording in the certificate

This certificate opens the door to misunderstandings in its declaration “up to SIL-3”: As shown, an individual valve without diagnostic function can only ever be used up to SIL-2, SIL-3 is only possible if a redundant circuit is used. It is indeed true that the certificate refers to this indirectly with the reference “according to IEC 61511”, because the standard clearly defines this connection. Nevertheless, it remains a potential source of incorrect conclusions. Furthermore, a SIL-2 component in redundant arrangement is not automatically suitable for SIL-3 circuits. This suitability is evident from the value of the probability of dangerous failure on demand (PFD value) listed in the certificate.

Newer certificates are more detailed:

The valves are suitable for use in safety-related systems up to SIL-2 in low and high-demand mode. Taking into account the necessary minimum hardware fault tolerance of $HFT = 1$, they can also be used up to SIL-3 with a redundant design.

Figure: New, unmistakable wording in the certificate

The wording “can be used in safety-related systems up to SIL-2” has the effect of downgrading the product with regard to its SIL suitability compared to the previous certificate. In fact, it is exactly the same statement: Both wordings mean the same thing, but the second wording is more transparent and describes the possible uses and the resulting SIL more clearly.

3. The certificate does not say everything – pay attention to the “safety manual”!

The sentence “Refer to the safety manual for advice” can be found as a standard note on all certificates. This is more than an everyday reference to a manual or an accompanying leaflet as in so many products. There is at least one reason why it is particularly worth taking a look at the safety manual: for comparing the specified values and test intervals.

For reasons of uniformity and faster comparability, the certificate always assumes a necessary inspection interval of one year. The probability of dangerous failure on demand is calculated from this. In reality, however, there are components, for example, that need to be checked more frequently. And above all: There are also products for which testing is necessary less often. Especially in the chemical industry, many customers are rightly interested in switching off their plants as rarely as possible for testing purposes. A single day of down-time due to maintenance at a refinery can easily mean a loss of production amounting to one million US dollars. The decisive factor is whether a component is certified in such a way that it will still meet the SIL requirement in the second or fifth year. The probability of dangerous failure on demand (PFD value) changes with the test interval: the longer the test interval, the higher the probability of dangerous failure on demand. “The inspection interval of one year shown in the certificate can therefore contain a hidden value that can have a primarily economic impact. This can be advantageous or disadvantageous and must therefore be considered separately,” says Reiner Laun.

What certificates say – and what they do not

The three examples show: Among other things, a certificate serves to regulate standards, and plant operators can use a certificate to quickly and clearly identify whether a component is suitable in principle for a specific safety function in a safety device for process control technology. However, certified components alone may not be sufficient to achieve the required SIL. Depending on the risk assessment of the plant section, the architecture must also be carefully examined.

Failure to meet this hurdle may result in additional costs: If the audit authority determines that an unacceptable safety risk exists despite the certified components, retrofitting will become necessary. And that costs both time and money.

➤ Certificates provide information on whether a component is basically suitable for a specific SIL. However, this can lead to misunderstandings because some details are not specifically mentioned in a certificate – or because there are different versions in circulation which state the same thing. Understanding the topic saves time and money.

The advantage of durable components

It has already been stated: Test cycles can be expensive. Economic efficiency depends crucially on the reliability of the individual plant elements. Therefore, plant operators want components that, if possible never need to be tested.

After all, modern plants are often largely optimized in terms of process technology. Higher output is only possible if the plant operates highly productively and reliably at the same time, so that inspection times or down-times due to repairs are kept to a minimum. For example, electromagnetic pilot valves: Moisture or dirt cause ageing and wear in the seal of a valve, just as temperature or simply regular use do. “A valve is a finite product because, for example, seals can become porous,” says Carsten Schindler. “Age is the most important factor at work here, followed by environmental conditions. Piston spool valves are often used which have up to six seals. That increases the risk of a stick-slip effect.” But what if a valve could be completely without a seal in the core? One example is Festo's VOFC series: A solenoid valve with piston seat valve technology that does not require a dynamic seal. This means that the ageing caused by wear on the seals is completely eliminated. This significantly reduces the probability of dangerous failure on demand.

But how can the valve be adjusted in such a way that, despite the lack of a soft seal, an equivalent tightness is achieved? What was needed was the engineer's art: The VOFC solenoid valve seat is hard-sealed, polyurethane replacing the usual soft seal.

In accordance with the type test and SIL certification issued by TÜV Rhineland, the VOFC solenoid valves guarantee that, if used correctly, there will be an incorrect circuit at most once in 2,410 switchings. If we assume a requirement case of one year, this means a single incorrect circuit in 2,410 years. In short: Due to the design principle, it is extremely unlikely that the valve will not switch off if required.

Practical example: Multipurpose plant from Bayer CropScience

The valve demonstrates its suitability for use at Bayer's multipurpose plant at the Dormagen site, among other places. It was built in 2002. The company combines various processes under one roof here: from the development of new active ingredients for crop protection and laboratory processing through to piloting and production. Therefore, the plants and equipment must be connected and operated as flexibly as possible in different configurations: Dryers, centrifuges, distillation apparatuses or stirrer vessels are used in different sequences depending on the task: A total of 67 automation systems are responsible for this.

These processes are protected by numerous safety devices in electrical measurement, open and closed-loop technology: In an emergency, for example, dosing valves, exhaust valves or steam valves are switched to fail-safe positions.

To ensure that these process valves close correspondingly quickly in an emergency, there are usually pilot valves between the positioner and the actuator that control the actuator (see also the example in the chapter entitled “Standards, regulations and fundamentals”).

In total, Bayer has installed more than 1,500 of these valves in the multipurpose plant. In the 15 years since the plant opened, there has been no unsafe failure of the solenoid valves. In 2015, 14 of the solenoid valves were removed from the multipurpose plant and subjected to detailed testing at Festo.

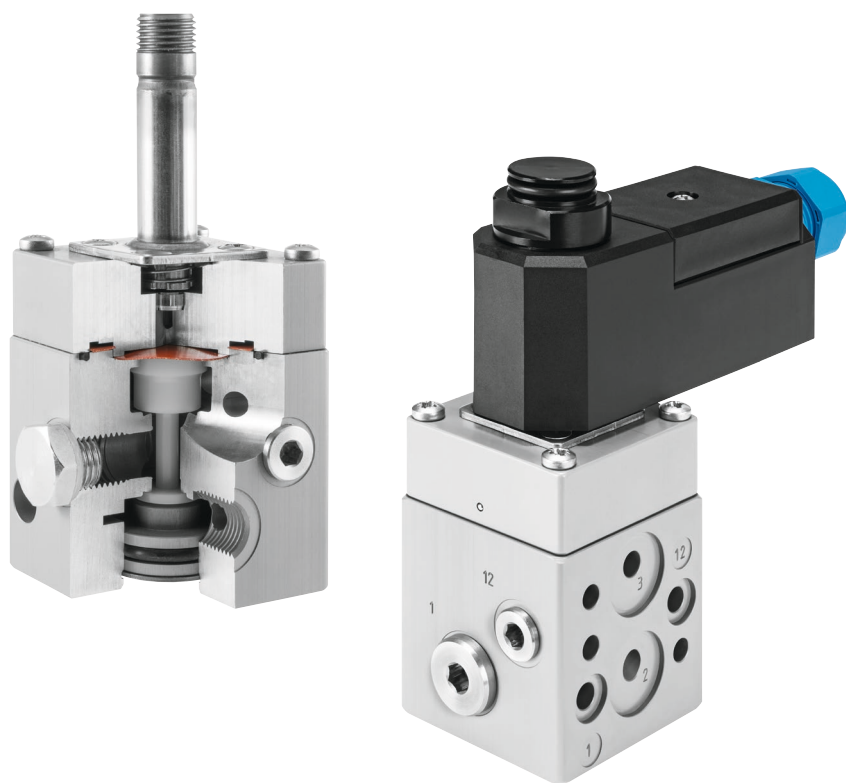


Figure: Solenoid valve series VOFC from Festo

In view of the proven 15-year operational reliability, a laboratory test carried out back in 1998 and the successful follow-up test, TÜV Rhineland issued a certificate: The valve only requires a proof test every seven years. Of course, the operating company is nevertheless responsible for proper and professional installation, operation and maintenance. With the certificate, however, the plant operator can significantly extend the test intervals of the solenoid valves.

Conclusions

SIL is a topic that can become not only safety-relevant but also cost-relevant: Errors in planning and setting up a safety circuit can lead to correspondingly costly retrofitting. Every regular inspection or an actual component failure can also result in significant costs due to production down-time. It is particularly important to pay attention to durable and appropriately certified components. In addition, the entire system should be considered right from the engineering phase and different approaches should be examined.

➤ Plant operators want the shortest possible inspection periods or down-times. However, components such as soft seals are, by nature of their design, finite products. Innovative component development makes it possible to develop valves that do without soft seals and are therefore more durable. Festo's VOFC solenoid valves, for example, have been proven and certified in a Bayer plant for more than 15 years.

Published by:
Festo AG & Co. KG

process@festo.com
→ www.festo.com/process

Your personal contacts:
Reiner Laun
Reiner.Laun@festo.com

Carsten Schindler
Carsten.Schindler@festo.com