An Overview of Functional Safety in the Process Industry

This white paper explores the various standards, definitions and products that can help you achieve greater functional safety in process applications.

FESTO

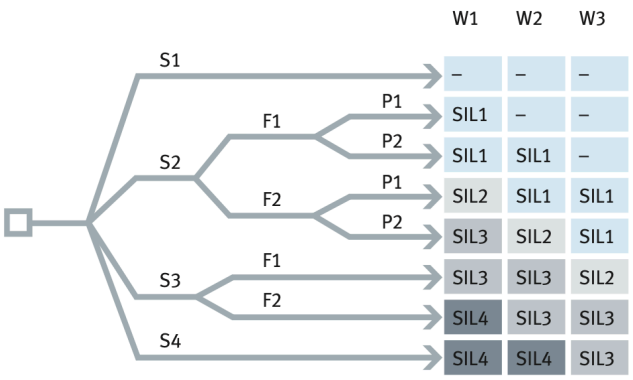
Implementing functional safety is critical in the process industries, which include dangerous chemical, petroleum and petrochemical applications. The systems in these industries, down to the lowest practical level, must be designed to reduce hazards against people, property and the environment—especially in the event of a malfunction or failure. To explore this topic further, this paper provides you with a helpful overview of the following:

- Safety Integrity Levels (SIL), including how to assign a level to your system.
- The standards, definitions and characteristic values for calculating SIL.
- The various products, including fail-safe valves and redundant architectures, that can help you implement functional safety easily and cost effectively.

How to Determine and Assign SIL

An important metric for the process industry, SIL measures the safety level or risk expected for a system in terms of PFD, or the probability of failure on demand. There are four distinct levels, with SIL1 representing the lowest risk and SIL4 representing the highest acceptable risk. In general, as the levels increase, the associated safety level also increases. At the same time, the probability that the system will fail to perform properly is lower. Typically, the system's complexity and installation and maintenance costs increase with the levels as well. Once a level has been assigned to a system, specific installation principles, such as redundant circuit design, must be observed to minimize safety risks in the event of a malfunction.

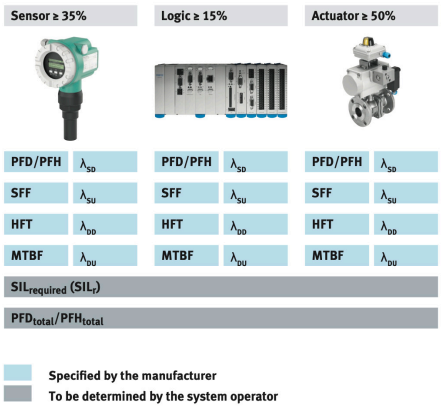
SIL (Safety Integrity Level)



S	Severity of the harm	
	S1	Slight injury to a person
	S2	Serious 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/reduction of harm	
	P1	Possible under certain conditions
	P2	Hardly possible
W	Probability of occurrence	
	W1	Relatively high
	W2	Low
	W3	Very low

In addition to the PFD, calculating SIL depends on several characteristic values such as the probability of failure per hour (PFH), or the probability that a safety function will fail during continuous use. Other important values include:

- **Safe failure fraction (SFF):** The proportion of safe failures to total failures.
- **Mean time between failures (MTBF):** The average time between two successive failures.
- **Hardware failure tolerance (HFT):** The ability of a system to continue to execute the required function in the event of faults or deviations. For HFT0, a single failure can eliminate the safety function. For HFT1, at least two failures must occur simultaneously to eliminate the safety function. And for HFT2, at least three failures must occur simultaneously to eliminate the safety function.
- **Device types A and B:** Type A means we can adequately determine the failure behavior and characteristics of all system components. Type B means we cannot determine the failure behavior of at least one component in the system.
- **Failure rate (λ):** Failure rate is the variable that determines the reliability of a component. There are many types, including:
    - Safe failures, or λ_S
    - Safe identifiable failures, or λ_{SD}
    - Safe unidentifiable failures, or λ_{SU}
    - Dangerous failures, or λ_D
    - Dangerous identifiable failures, or λ_{DD}
    - Dangerous unidentifiable failures, or λ_{DU}



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

Functional Safety Standards for Process Applications

The basic standard for functional safety is IEC 61508, which encompasses electrical, electronic and programmable electronic safety-related systems. It also outlines the methods for assessing safety risks using a risk graph, as well as designing suitable safety functions for sensors, logic circuits, actuators and other devices. Bear in mind, IEC 61508 requirements only pertain to complete safety instrumented systems (SIS) and not to individual components. A SIS typically consists of the following:

- Sensors—e.g., pressure and temperature sensors, as well as filling level gauges.
- Evaluation and output units like safety programmable logic controllers (PLC).
- Automated process valves, which comprise the solenoid valve, actuator and process valve.

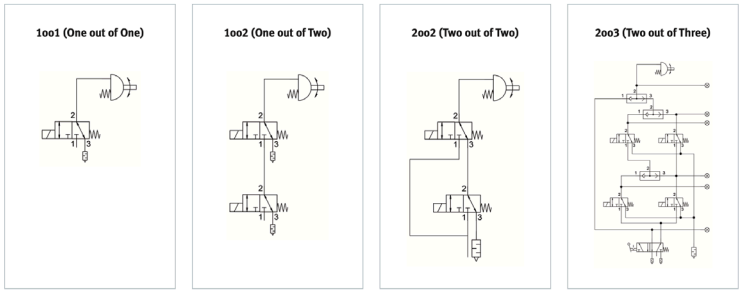
The standard IEC 61511 describes how to implement IEC 61508 for the process industry with a focus on applications with a low demand mode. Unlike high demand safety functions, which are expected to occur more than once a year, low demand functions have an expected demand rate of less than once a year. Any company that implements or operates a system that represents a potential hazard for employees, local residents or the environment must minimize the process risks under fault conditions. To do so, IEC 61508 and IEC 61511 outline the following steps:

- Define and assess any risks according to detailed failure probabilities for sensors, controllers, actuators and other components.
- Define and implement measures to minimize residual risks.
- Use only evaluated or certified devices.
- Conduct recurring tests to ensure compliance with safety functions.

A Deep Dive Into Redundant SIS Architectures

IEC 61508 and IEC 61511 recommend diverse redundancy to increase the safety integrity of programmable electronic systems. These architectures, which place process safety and reliability at the forefront of hardware design, play a critical role in applications that process crude oil, natural gases, chemicals and other hazardous substances. They include:

- **1oo1 (One out of One):** This architecture features only one element. If the contact fails to open in the event of an emergency, then the system could suffer a dangerous failure.
- **1oo2 (One out of Two):** This design improves system safety by adding redundancy. Because only one contact is required to initiate a safe shutdown, the PFD is lower.
- **2oo2 (Two out of Two):** This configuration adds redundancy for better process reliability. Because the outputs are wired in parallel, both contacts must operate to initiate a process shutdown, reducing the spurious trip rate but increasing the PFD.
- **2oo3 (Two out of Three):** This design, in which two out of three channels must agree on the output, adds advanced redundancy for better safety and process reliability. It involves more components, increases input/output (I/O) requirements and power consumption, and is commonly seen in applications like gas turbines, compressors and heaters. This architecture reduces both the spurious trip rate and average PFD.

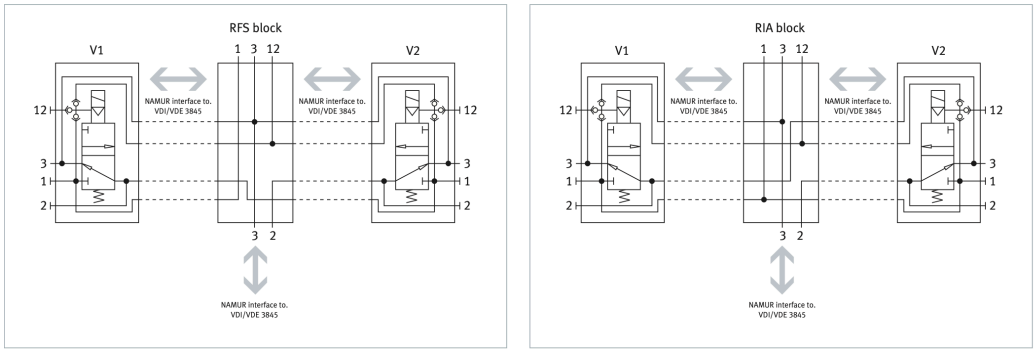


Basic and advanced SIS architectures.

The most common redundant systems at the field level are 1oo2, which increases safety, and 2oo2, which increases uptime. In a 1oo2 configuration, two valves are connected in a series and energized during operation. Should a valve or solenoid fail, the entire system is exhausted to protect the system from damage. Media conveyor lines frequently require 1oo2 for the higher safety level it achieves. In a 2oo2 configuration, two valves are connected in parallel and energized during operation. Should a valve or solenoid fail during operation, the entire system remains active and continues to work. Cooling circuits, which require this constant uptime, typically utilize the 2oo2 architecture.

Redundancy at the Field Level

To visualize how several redundant SIS architectures play out in the field, let's explore a few examples. This first scenario involves a redundant NAMUR block, which enables users to install two Festo VOFC or VOFD Series solenoid valves. These valves are interconnected, providing redundancy for automated process valves. In addition, the NAMUR interface makes redundancy easy to implement, lowers warehousing costs and makes valve replacement quick and easy. Blocks are available with a fail-safe function (1oo2) or with higher uptime (2oo2), and users can mount the block directly on quarter-turn actuators using the standardized interface. With a 1oo2 configuration and using an additional auxiliary power terminal, the NAMUR block can also be used with piloted solenoid valves on actuators that have a positioner for fail-safe functionality. This solution offers users high levels of flexibility, thanks to the many ignition protection options, global certifications and connections.

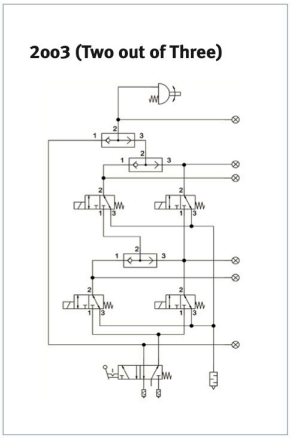


NAMUR block configurations for fail-safe redundancy (1oo2) and higher uptime (2oo2).

Our next example involves redundant in-line valves for 1oo2 and 2oo2 architectures. With these compact systems, two VOFD Series valves are combined into one housing. Thanks to their special coating, these valves meet the highest safety standards in process engineering and can withstand tough ambient conditions. In addition, their redundant circuits ensure fail-safe functionality (1oo2) or achieve higher uptime (2oo2) for automated process valves. Like the NAMUR block option, this solution offers users high levels of flexibility, thanks to the many ignition protection options, global certifications and connections.

Our last example combines the NAMUR block and in-line valves, creating a 2oo3 system that provides maximum safety and process availability at the same time. The block itself is an in-line variant that users can easily integrate into their system, with standard valves mounted directly on the block via the NAMUR interface. This 2oo3 design offers several benefits:

- Users can easily replace individual valves or bypass their functions. This bypass can be unlocked with a key, enabling personnel to conduct maintenance during operation.
- Users can mount mechanical pressure indicators or pressure gauges directly on the valve block, providing reliable indication if a valve is pressurized.
- Users can replace the mechanical displays with electronic pressure sensors to reflect control system status.



NAMUR in-line redundancy option (2oo3).

Learn More About Functional Safety

Safety engineering is one of the most important requirements in the process industry. At Festo, we offer products and solutions that are the perfect prerequisite for implementing safety engineering as easily and cost effectively as possible. To learn more, please download our Guideline for Functional Safety.

Other Products For Safety-Related Applications

The following products from Festo can help you improve safety integrity throughout your process application:

- **Actuators.** We provide single- and double-acting actuators that are tested and ready-to-install in safety systems. Our automated process valves use only certified components, and we can perform SIL or ATEX assessments of actuators according to the manufacturer's declaration.
- **PROFIBUS redundancy.** Our redundant PROFIBUS solution increases safety between the distributed control system and remote I/O. If a PROFIBUS cable is removed or the node is faulty, then a second PROFIBUS cable and node take over, reliably sending and receiving all control system protocols.
- **Control cabinets.** Customizable control cabinets protect components from environmental factors, fluids and foreign matter. Choose from tubing or piped connections. And whether you're using pneumatic, electric or electro-pneumatic components, you'll receive a control cabinet that meets your application's unique requirements. On request, we can conduct an SIL assessment of the cabinet, and for explosion protection, we can manufacture cabinets in a 2GD or 3GD design that meets international and National Electrical Code (NEC) standards.

Modified by:
Festo Corp.
1377 Motor Parkway
Islandia, NY 11749

Publisher:
Festo SE & Co. KG.
Ruiter Strasse 82
D-73734 Esslingen
www.festo.com