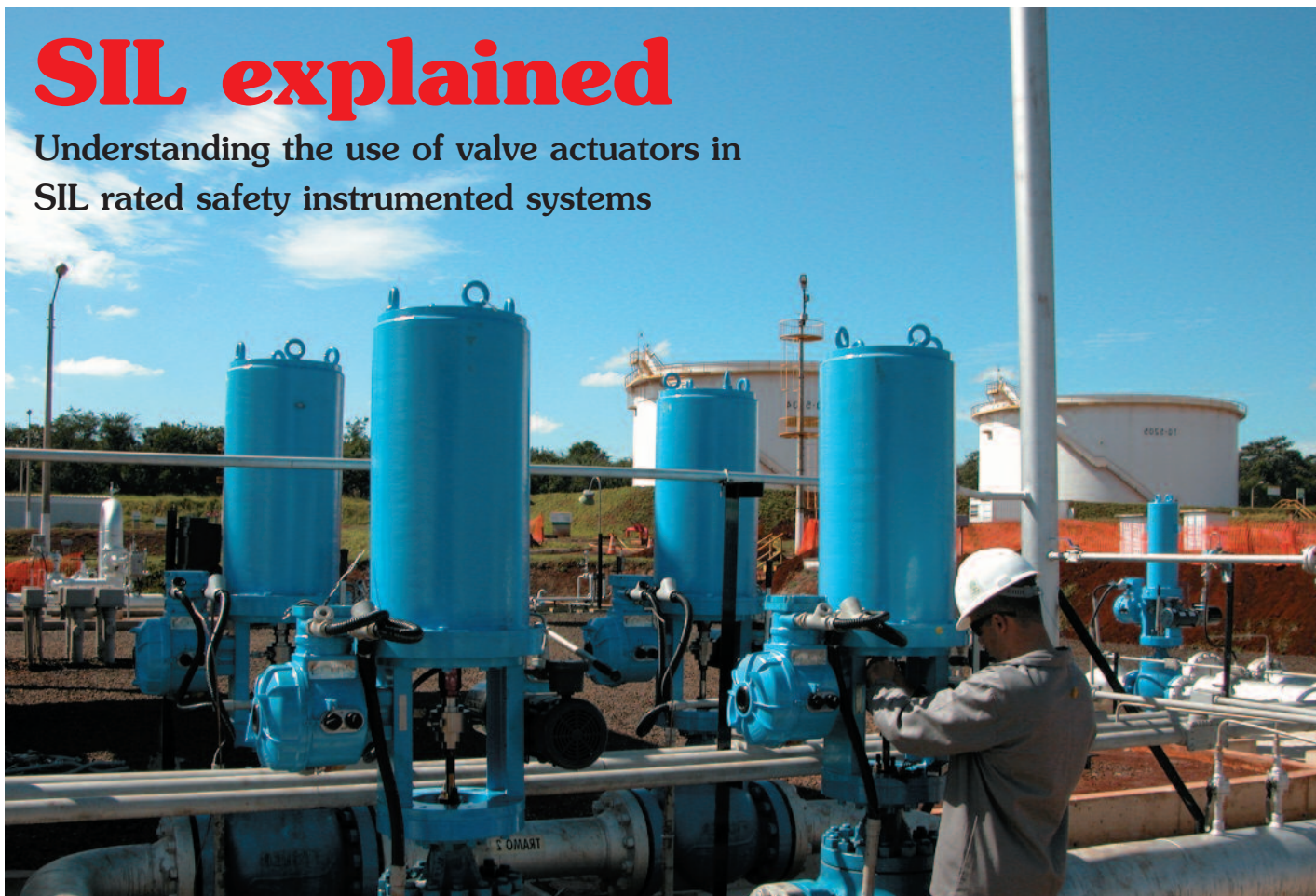


SIL explained

Understanding the use of valve actuators in SIL rated safety instrumented systems



The requirement for Safety Integrity Level (SIL) equipment can be complicated and confusing. In this document, the author sets out to explain SIL and its consequent impact upon the provision of valves and actuators in relation to Safety Instrumented Systems (SIS).

By Richard Harvey, Rotork Fluid Systems

What is SIL?

SIL, an acronym for Safety Integrity Level, is a system used to quantify and qualify the requirements for Safety Instrumented Systems. The International Electrotechnical Commission (IEC) introduced the following industry standards to assist operators with quantifying the safety performance requirements for hazardous operations:

- IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
- IEC 61511 Safety Instrumented Systems for the Process Industry Sector

These standards have been widely adopted in the hydrocarbon and oil and gas industries to define Safety Instrumented Systems and their reliability as a means of improving safety and availability of Safety Instrumented Systems.

What are Safety Integrity Levels?

Safety Integrity Levels are targets applied to the reliability and performance of the safety systems used to protect hazardous activities such as hydrocarbon refining or production. There are 4 SIL levels. The higher the perceived associated risk, the higher the performance required of the safety system and therefore the higher the SIL rating number. The IEC standards define the performance requirements of the safety systems for the required SIL rating.

How are SIL ratings determined?

Once the scope of an activity is determined, the operator can identify the possible hazard(s) and then assess their potential severity. The risk associated with a hazard is identified by assessing the likely frequency of occurrence and the potential consequences if the hazard is realized. The operator must then assign a number for the severity of consequence and frequency.

These numbers are then fed into a matrix to allow the operator to assign the required SIL rating to protect against the hazard. Many tools are available to assist an operator with this process (e.g., HAZOP software — Hazard and Operability). An example of such a matrix is shown in Figure 1.

How are hazards protected against?

Once the SIL ratings have been determined, the operator can then design a risk reduction strategy to protect against these hazards. This is accomplished by applying multiple layers of protection.

Frequency	5	SIL 3	SIL 4	×	×	×
	4	SIL 2	SIL 3	SIL 4	×	×
	3	SIL 1	SIL 2	SIL 3	SIL 4	×
	2		SIL 1	SIL 2	SIL 3	SIL 4
	1			SIL 1	SIL 2	SIL 3
		1	2	3	4	5

Severity of Consequences

Fig. 1: Frequency/consequence matrix.

Risk reduction can be an expensive procedure; therefore, the operator will look to reduce the risk to a level As Low As Reasonably Practicable (ALARP). Figure 2 shows multiple layers of protection are used to develop the required safety strategy. Safety Instrumented System has been highlighted because this is the layer that applies to shutdown systems and valve actuators. The SIS assists in reducing the frequency of the likely manifestation of the hazard and therefore improves the reliability of the system. The consequence of a failure is not addressed by SIS but by other aspects of the risk reduction strategy.

How is SIL used?

Safety Integrity Levels are part of a larger scheme called Functional Safety that deals with techniques, technologies, standards and procedures that help operators protect against hazards. Functional Safety adopts a life cycle approach to industries that deal with hazardous processes that includes plans from concept through to final decommissioning of plants. This process is cyclical and any phase is effected by the requirements of the previous stage(s) so, subsequent stages must be revisited to assess the impact of a change to a previous stage. Figure 3 shows a simplified depiction of the four basic steps of the life cycle.

Pre-design phase

This is the phase where the scope of the project is determined, all hazards are assessed, and a Safety Requirements Specification is formulated. This specification will determine the SIL ratings to be applied to the various activities.

Design phase

Once the pre-design phase is completed, the operator will design the required safety systems and plan how they will be executed. It is this stage where the safety systems are specified. This is also when the testing regimes are allocated to ensure that the SIL ratings can be met.

Realisation phase

Upon the completion of the design phase, the plant is built and commissioned. All safety systems are tested to ensure that they meet the established safety requirements.

Operation phase

The plant is now operational and producing. The safety systems are now regularly tested to ensure that they continue to perform as designed and required.

How does equipment fail?

There are three ways in which safety equipment can fail: systematic, common cause, and random hardware failure. These failures are addressed by the safety life cycle in the following manner:

Systematic failures

These types of failure are not failures of individual components but the system as a whole. These failures are reduced by using proper engineering practice and design during the design phase. These are very rare failures as years of experience and documentation have helped engineers understand how systems interact.

Common cause failures

This type of failure is when identical components within the safety system fail at the same time. Again, experience with products and documentation help engineers design systems that prevent this. Also, these failures can be virtually eliminated by using

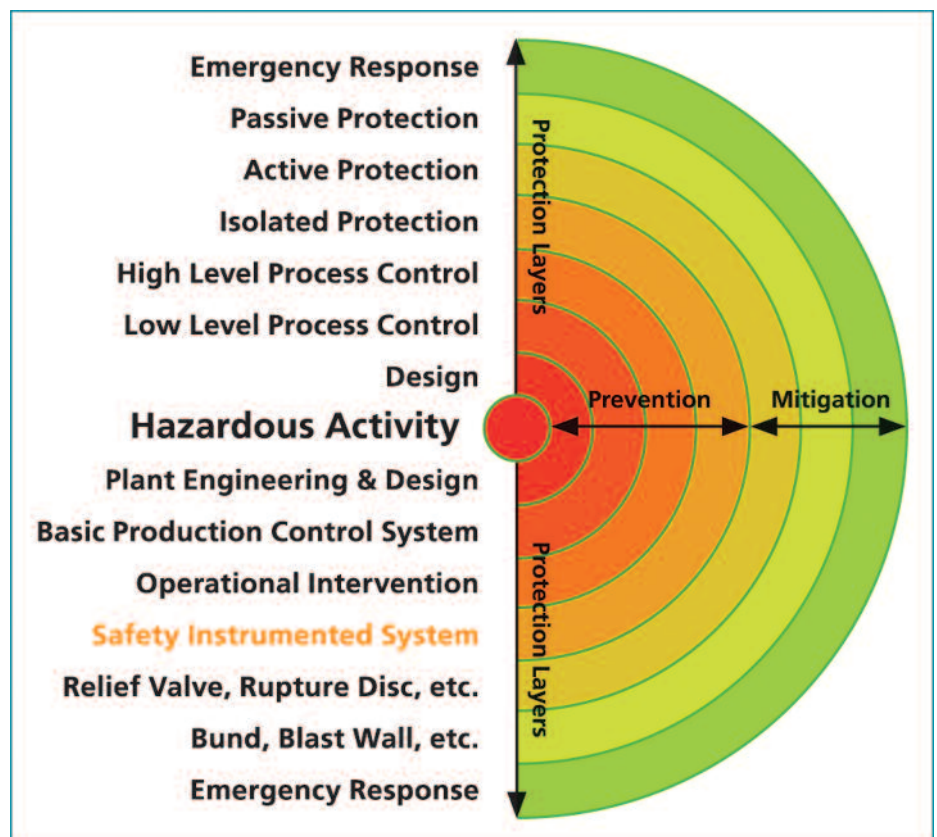


Fig. 2: Layers of hazard protection.

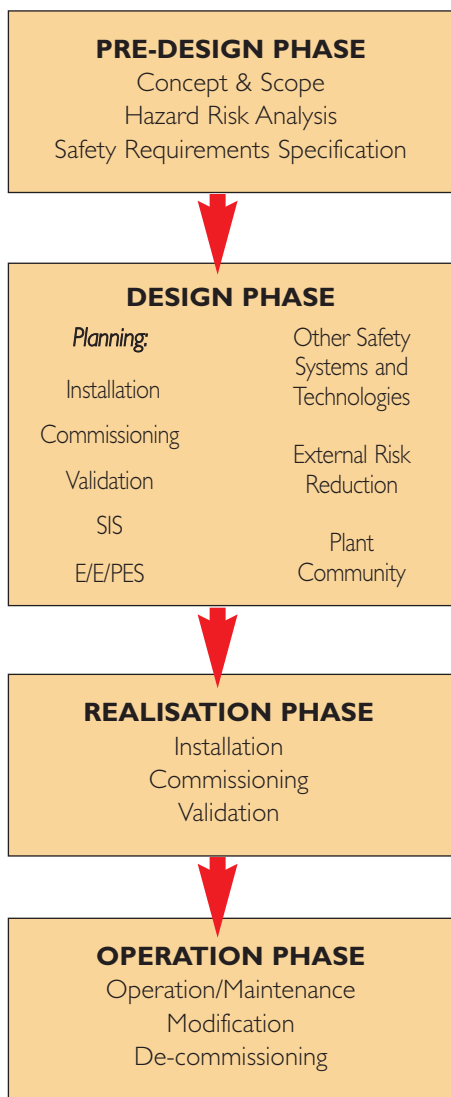


Fig. 3: Functional safety life cycle.

redundant and diverse systems. Common cause failures are generally the result of environmental effects like flooding or excessive temperatures.

Random hardware failure

This is the main type of failure mode — random by their nature. This is the type of failure Safety Instrumented Systems protect against. Engineers try to predict the probability of these failures by assessing the failure rates of the equipment used. This is where SIL specifies the performance and architectural constraints that a safety system requires.

How is the SIS performance quantified?

The Probability of Failure on Demand (PFD) is the measure used to define the level of protection offered by the system. IEC 61508 defines the maximum allowable

SIL Level	Max PFDavg	Chance of failure
1	0.1	<10%
2	0.01	<1%
3	0.001	<0.1%
4	0.0001	<0.01%

Fig. 4: SIL ratings.

PFDavg (the average probability, from 0 to 1, that the safety function will fail to operate on demand) for the Safety Instrumented Function (SIF).

The allowable level is dependant upon whether the system is deemed to be low demand or high demand. Low demand systems are defined as having an expected safety demand interval of greater than one year, and a proof test interval for the equipment that is at least twice that of the expected safety demand interval. The vast majority of fluid power actuated safety valves fall into this low demand type. IEC 61508 defines the required PFDavg as shown in Figure 4.

High Demand safety control systems are defined as those that are operated more frequently than once per year.

What does this mean in terms of performance for the SIF?

The figures quoted in Figure 4 apply to the entire Safety Instrumented Function and not the individual components. Any SIF is

comprised of three discrete areas: “Sensors”, “Logic Solvers” and “Final Elements”. Figure 5 indicates these areas of an SIF for over-pressure isolation. The “Sensors” detect the presence of the potential onset of a hazardous condition (e.g., over-pressure). The “Logic Solver” is the programmable logic controller (PLC) which determines what action to take after the “Sensors” have detected a potentially hazardous event. The “Final Elements” perform the required safety action (e.g., ESD of the valve). The scope of this document only covers the “Final Elements” as this is area where fluid power actuators function.

When assessing the performance of the SIF we must consider the solenoid valve, actuator and valve as a single entity with regard to the PFDavg calculation as the failure of any of these components will cause the SIF to fail.

In order to prove that the SIF is performing to the required SIL rating, it is necessary to know the failure rates of the equipment

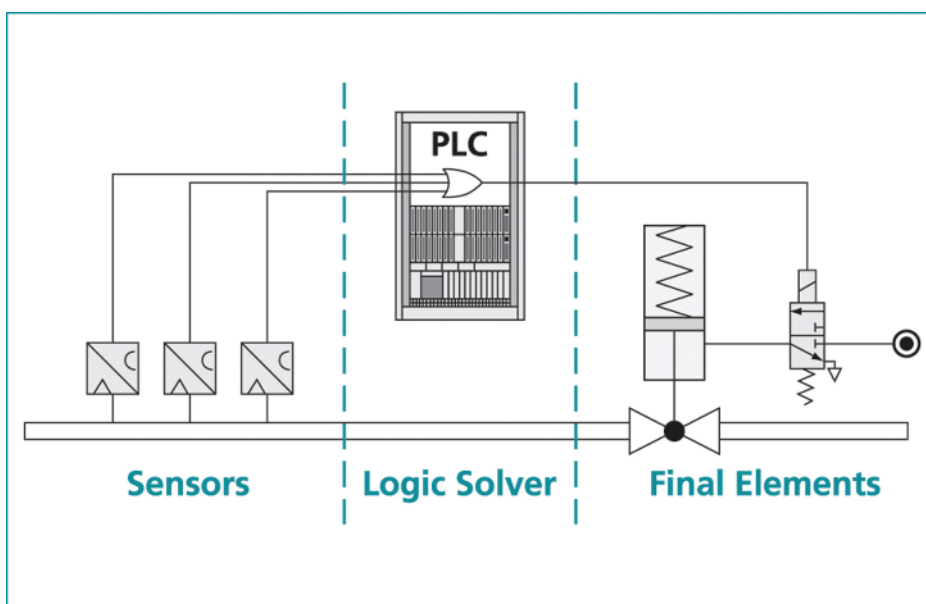


Fig. 5: Example of an over-pressure shutdown.

used so that it can be verified that the maximum allowable PFDavg is not exceeded. Failure rate data gives the operator a measure of when the equipment is likely to fail over a given period of time (i.e., the older the equipment, the more likely it is to fail when required to operate). The PFDavg can be calculated from this data. When it reaches the maximum allowable level, the plant must be shutdown and all safety systems fully tested.

Is it possible to procure an actuator with a SIL rating approval?

The simple answer is no. Only the complete SIF can have a SIL rating, not individual components. However, components (e.g., actuators) can be certified "suitable for use" at a particular SIL rating.

Operators and contractors may look for components certified as "suitable for use" as this will simplify the design process. In addition, if the component has failure rates that are known to be compatible with the required SIL rating, the safety calculations are also made much simpler.

How are actuators certified as "suitable for use" for specific SIL ratings?

There are two aspects to the process of attaining a SIL certificate. The first is assessing the design and failure rates of the equipment. This can be accomplished through either of two techniques: FMEDA (Failure Modes, Effect and Diagnostic Analysis) and "Proven in Use".

The second aspect is the auditing the vendor's manufacturing and quality processes. This audit proves that the vendor is capable of manufacturing the product to the designed performance standard. These assessments must be audited by an approved accreditation body such as Exida or TÜV.

Suitable for Use Method 1 – FMEDA

FMEDA is a technique that assesses the performance of a device by evaluating the effects of the different failure modes of all components in the design. Every component is assessed for the type of failure (dangerous or safe) and the likelihood of failure (failure rate). All of this data is then collated to produce overall dangerous and safe failure rates that can



Safety Integrity Levels are targets applied to the reliability and performance of the safety systems used to protect hazardous activities such as hydrocarbon refining or production.

be used in safety calculations. FMEDA studies can be conducted either by the vendor or a third-party body but, in both circumstances, must be audited by an accredited body to prove that best practices have been used.

Suitable for Use Method 2 – Proven in Use

It may not be possible, practical or cost effective to conduct an FMEDA on a product, particularly if it is of an old or complex design. In these cases, products may be

certified by using "Proven In Use". "Proven In Use" as defined in the IEC 61508 standard is a documented assessment that has shown that there is appropriate evidence, based on previous use history of the component, that it is suitable for use in a safety system. This documented evidence must include the following:

- The manufacturer's quality and management systems.
- The volume of the operating experience with statistical evidence to show that the claimed failure rate is sufficiently low.

About Rotork

Rotork is a global leader in valve actuation technology, providing a range of valve actuators, controls and associated equipment plus services (commissioning, preventative maintenance, retro-fitting, etc).

In addition to having actuators currently operating in both SIL 2 and SIL 3 environments, Rotork Fluid Systems (RFS) also has a Partial Stroke Testing tool (the SVM Smart Valve Monitor) that provides the highest possible diagnostic coverage.

Rotork also provides services related to the safety calculations for the entire final element assembly, including the valve and controlling solenoid valves. By creating a database of known failure rates for various final elements, Rotork is able to provide recommendations for control mechanisms and valves that will provide the end-user with the best possible performing system that yields the best possible long-term financial benefits.

RFS's services assist the end user in extending shutdown intervals to the maximum possible time frame within the required SIL rating and also provide peace of mind against spurious trips.

Failure rate data

Once the studies have been completed, the user is presented with the failure rate data. This data falls into two fundamental categories: dangerous failure rate (λ_D) and safe failure rate (λ_S).

The dangerous failure rate (λ_D) data relates to failures that will result in the SIF being unable to perform the required safety function upon demand. The safe failure rate (λ_S) data relates to those failure modes that will put the safety function in its safe state (e.g., shutdown). SIL is only concerned with the dangerous failure data but the safe failure data is important as this provides the operator a measure of how likely the safety system is to spuriously trip.

Do we need to test the SIF?

As described in earlier sections, SIL prescribes the maximum level that the PFDavg is permitted to reach. There are two types of tests that can be performed to help maintain the PFDavg at a suitably low level: Proof Tests and Diagnostic Tests:

Proof tests

A proof test is a manual test performed during shutdown that tests the entire functionality of the SIF from sensing to actuation. It must be suitably configured to test all aspects of the safety function to prove that the SIF is "as good as new". There may be several negative ramifications — particularly expense related — due to a proof test necessitating a process shutdown.

Diagnostic tests

A diagnostic test is an automatic test performed online that does not necessitate process shutdown. This type of test must be performed at least ten times more frequently than the expected SIF demand rate. A diagnostic test will test only a percentage of the total possible failure modes of the SIF; this percentage is called the Diagnostic Coverage (DC). These tests contribute to reducing the PFDavg of the SIF and thus assist in the extension of the proof test interval. The higher the DC, the greater the benefit gained from the test. For the "final elements" within the scope of this article, this type of test is called a partial stroke test.

SIL for electric actuators

Rotork IQPro intelligent electric valve actuators are available with a Safety Integrity Level option for applications requiring SIL2 and SIL3 levels. Actuators are equipped with the Rotork SIL safety PCB assembly, which monitors the standard IQ/IQT control board and provides diagnostic coverage and redundant control in order to perform the desired safety function if an invalid command signal is generated and/or if the standard actuator control system fails. A safety function status relay provides indication of the actuator availability and redundant safety function operation, with the same status duplicated locally on the actuator display. The two safety functions applicable to IQPro actuators are Stayput (high demand) and Emergency Shutdown (ESD) (low demand).

