

The effects of Partial Valve Stroke Testing on SIL level

The objective of a Safety Instrumented System (SIS) is to reduce the risk associated with a particular process to a level lower than or equal to the tolerable risk level. The SIS does not increase the production output and there is no direct return on investment. It is therefore often said that the SIS should be considered a type of insurance. One will only use the insurance in case something goes wrong. In a perfect world where nothing goes wrong the insurance will never be used. If the process that the SIS is guarding never runs out of control, the Safety Instrumented System will never be used.

In general, a SIS just waits for something to happen. It measures the process variables, performs the configured algorithm on the process variables, and, in a de-energized-to-trip system, if there is no demand from the process, it will keep the output energized. This means that the shutoff valves of such a Safety Instrumented System, which are open during normal operation, will continuously remain in the open position. If the process variables go beyond the normal operating limits, the SIS should take action to de-energize its outputs and consequently close the shutoff valves.

Partial Valve Stroke Testing

The fact that the shutoff valves continuously remain in the open position is the basis for one of the main concerns in de-energized-to-trip type systems. This concern deals with the way one can be sure that the shutoff valves will not be stuck in case a demand from the process occurs. This is especially true since the main failure mode of a shutoff valve is being stuck. It may be obvious that the stuck failure mode is dangerous in de-energized-to-trip systems and that normally such a failure will be unrevealed.

The only way one can be sure a valve is not stuck is to actively test the valve and see if there is any movement from the open position of the valve. This test can be performed as part of the periodical proof test of a Safety Instrumented System. However, proof testing generally only takes place once a year, which means that the valve will be tested only once in a twelve month period.

Reliability analyses usually show that the final element section of the SIS, of which the valve is a part, contributes most to the PFDavg value of the entire SIS and therefore has the most negative impact on the risk reduction achieved by the SIS. Since the proof test interval has a large effect on the achieved risk reduction, it might well be that the only once a year test is just not enough to ensure that the SIS meets the required risk reduction target. Consequently a more frequent periodic proof test is required. On the other hand, as proof tests normally mean that the process is shut down with the accompanying loss of production, the tendency is to minimize the number of proof tests as much as possible.

In order to ensure that the shutoff valves are not stuck and to avoid the frequent periodic proof tests, partial valve stroke testing can be of major assistance.

The concept of partial valve stroke testing is relatively straightforward. As its name already indicates, partial valve stroke testing involves the partial stroking of a valve to check for valve movement without fully stroking, or completely closing, the valve. This verifies that the valve is not stuck and still operational without shutting down the complete process.

By implementing partial valve stroke testing it is possible to detect stuck failures of valves. Therefore a certain diagnostic coverage of these dangerous stuck failures can be accounted for in reliability analyses. The reliability analyses will show that the SIS achieves an increased level of risk reduction.

Benefits of partial valve stroke testing

The results of several Safety Integrity Level (SIL) verifications performed by exida.com showed that the Safety Instrumented Function (SIF) under consideration did not meet the required risk reduction, mainly because of the relatively poor operation of the final element part of the SIF. Only after accounting for the implementation of partial valve stroke testing did the SIF under consideration meet the required SIL level.

An example of a Safety Instrumented Function that did not meet the SIL requirements without the implementation of partial valve stroke testing is shown in figure 1.

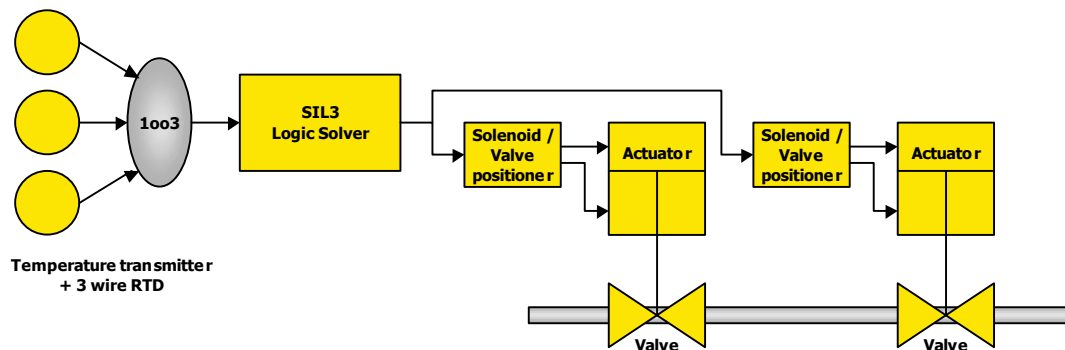


Figure 1 Example SIF

This SIF consists of three generic temperature transmitters with 3-wire RTD's in a 1-out-of-3 voting configuration, a SIL 3 safety PLC, and two 3-way solenoids each operating an actuator with ball valve in a 1-out-of-2 voting arrangement. The valves operate in unclean service. The required SIL level for this Safety Instrumented Function is SIL 3.

The results of the SIL verification, performed with the exida.com online SILver tool, are shown in figure 2. The SILver results indicate that the average Probability of Failure on Demand of the entire safety instrumented function is 2.10E-03, which means that the SIF only meets Safety Integrity Level 2 based on the PFDavg value. This is caused by the high PFDavg value for the final element part. Furthermore the SIL level based on the architectural constraint types according to IEC 61508 / IEC 61511 shows that the safety instrumented function can only be used in SIL 2 applications. This is caused by the fact that the Safe Failure Fraction (SFF) of the actuator - ball valve combination, a type A subsystem, is smaller than 60%. The SFF is so low because a large portion (more than 50%) of the potential failures of the actuator – ball valve combination is dangerous and all these dangerous failures are undetected. See also the Architectural Constraint comment at the end of this article.

Sensor Part Information

Sensor Group(s)	Edit
(1) Temperature group	Details
PFDavg Sensor Part:	2.20E-04
MTTFS Sensor Part (years):	26.36

Logic Solver Part Information

Logic Solver	Edit
(1) Safety PLC	Details
PFDavg Logic Solver Part	4.02E-05
MTTFS Logic Solver Part (years)	81.36

Final Element Part Information

Final Element Group(s)	Edit
(1) Shutoff valves	Details
PFDavg Final Element Part:	1.84E-03
MTTFS Final Element Part (years):	12.39

SIF Performance Metrics

Safety Instrumented Function	Preview
Average Probability of Failure on Demand (PFDavg)	2.10E-03
Safety Integrity Level	2
Safety Integrity Level (Architectural Constraints)	2
Risk Reduction Factor	476
MTTFS (years)	7.64

Figure 2 Results of SIL verification for example SIF without partial valve stroke testing.

In order for this Safety Instrumented Function to meet the SIL 3 requirement, the final element part needs to be improved both with regard to the PFDavg value as with regard to the architectural constraints. When using the same equipment, the only solution is to implement a 1-out-of-3 voting in the final element part. The 1-out-of-3 voting means three 3-way solenoids, each operating an actuator with ball valve, should be used. The 1-out-of-3 voting implies that there are two levels of hardware fault tolerance. The actuator - ball valve combination with a Safe Failure Fraction of less than 60% can then be used in a SIL 3 application (see table 1). Besides the fact that the architectural constraints requirements are met for the final element part, the 1-out-of-3 voting also implies that there is extra safety redundancy in the final element part. The extra safety redundancy will decrease the PFDavg value for the final element part, causing the PFDavg value of the entire Safety Instrumented Function to meet the SIL 3 requirement.

Considering this final element part configuration for the example safety instrumented function, the results of the SIL verification show that the average Probability of Failure on Demand of the entire safety instrumented function is $3.51E-04$. So with the three 3-way solenoids each operating an actuator with ball valve in a 1-out-of-3 voting, the example SIF meets the requirements for SIL 3. However, this solution is very costly and not many companies would want to implement this configuration.

As already indicated earlier the main failure mode of a shutoff valve is being stuck, where for de-energized-to-trip applications this is a dangerous failure mode. Reviewed maintenance records show that at least 60% of valve failures in “severe” service are caused by either a stuck stem or a stuck plug in the valve. Performing partial valve stroke testing will detect these failures. Consequently potential dangerous failures are detected and can be repaired before a hazardous condition occurs. Detecting at least 60% of the valve failures in “severe” service not only means that the average Probability of Failure on Demand of the final element part will decrease, it also implies that the safe failure fraction of the actuator – ball valve combination will increase to above 60%. Previously dangerous undetected failures are converted into detected failures contributing in the numerator of the SFF formula.

Performing a new SIL verification while accounting for the partial valve stroke testing shows that the average Probability of Failure on Demand of the safety instrumented function is now $9.50E-04$. This means that the example SIF meets the SIL 3 requirements based on the average Probability of Failure on Demand. Furthermore, because the safe failure fraction of the actuator – ball valve combination is larger than 60%, the results of the SIL verification show that the SIF also meets the SIL 3 requirements based on the architectural constraints concept. Consequently partial valve stroke testing ensures the required Safety Integrity Level without the need to implement the additional (third) solenoid with actuator and valve combination.

The results of this SIL verification, performed with the exida.com online SILver tool, are shown in figure 3.

Sensor Part Information

Sensor Group(s)	Edit
(1) Temperature group	Details
PFDavg Sensor Part:	2.20E-04
MTTFS Sensor Part (years):	26.36

Logic Solver Part Information

Logic Solver	Edit
(1) Safety PLC	Details
PFDavg Logic Solver Part	4.02E-05
MTTFS Logic Solver Part (years)	81.36

Final Element Part Information

Final Element Group(s)	Edit
(1) Shutoff valves	Details
PFDavg Final Element Part:	6.89E-04
MTTFS Final Element Part (years):	12.21

SIF Performance Metrics

Safety Instrumented Function	Preview
Average Probability of Failure on Demand (PFDavg)	9.50E-04
Safety Integrity Level	3
Safety Integrity Level (Architectural Constraints)	3
Risk Reduction Factor	1053
MTTFS (years)	7.57

[brochures](#) | [newsletter](#) | [free articles](#) | [user survey](#) | [equipment survey](#) | © 2000-2001 exida.com, L.L.C. [See terms of use](#)

Figure 3 Results of SIL verification for example SIF with partial valve stroke testing.

Architectural Constraint Comment

The Safe Failure Fraction (SFF) parameter indicates the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. For each device the SFF can be calculated using the following formula and the device's failure rate data.

$$SFF = \frac{I^{SD} + I^{SU} + I^{DD}}{I^{SD} + I^{SU} + I^{DD} + I^{DU}} \quad \text{Equation 1}$$

A subsystem can be regarded as a type A subsystem if, for the components required to achieve the safety function

- a) the failure modes of all constituent components are well defined; **and**
- b) the behavior of the subsystem under fault conditions can be completely determined; **and**
- c) there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met.

The subsystem is regarded as type B if not all of the criteria listed above are met. Typical examples of type A devices are switches, solenoids, and relays. Type B devices are microprocessor based or devices with complex custom logic.

Table 1 shows the required hardware fault tolerance for a device in combination with the Safe Failure Fraction of that device for usage in a specific SIL level application for type A devices.

Table 1 Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safety Failure Fraction	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
> 99 %	SIL 3	SIL 4	SIL 4

Abbreviations

PFDavg	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault
SIF	Safety Instrumented Function, a set of equipment intended to reduce the risk due to a specific hazard (a safety loop)
SIL	Safety Integrity Level, discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the Safety Instrumented Systems where Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest

SIS Safety Instrumented System, implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s)

References

- [1] ANSI/ISA 84.01, Application of Safety Instrumented Systems for the Process Industries, 1996, Instrument Society of America, Research Triangle Park, NC, USA
- [2] IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems, 2000, International Electrotechnical Commission, Geneva, Switzerland