SIL Capable Actuated Valves in a Safety Instrumented System

Background

A Safety Instrumented System (SIS) is designed to safeguard operators, plant equipment and the environment by reducing the frequency or the severity of the hazardous event. An SIS is one of the many layers of protection – to prevent and mitigate - a hazardous event in chemical or oil and gas industries. The layers of prevention include basic process control system (BPCS), operator intervention and SIS while the layers of mitigation include relief valve/rupture disk devices, dikes and emergency response. An SIS is composed of a sensor, logic solver and final control elements and these three components combine to bring a process to a safe state during a hazardous event. The specific control function performed by an SIS is called Safety Instrumented Function (SIF), which has a specified Safety Integrity Level (SIL) in order to achieve or maintain a safe state.

By K.S.Patil, Jaisingh Jadhav and Ram Viswanathan – L&T Valves Limited

Role of Final element (Actuated Valve)

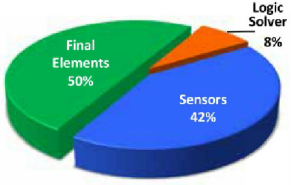
As per IEC 61511, a final element is a part of an SIS which implements the physical action necessary to achieve a safe state. E.g. Valves, switch gear, motors.
The expected functions of an actuated valve functioning as final element are:

1. Perform the intended function reliably
2. Close on trip and/or tight shut off or open on trip
3. Fast acting (< 2 second in some cases)
4. Fail predictably (diagnostics etc.)

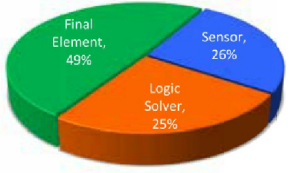
Studies from Oreda indicate that final elements contribute to 50% of all safety loop failures followed by sensors (42%) and logic solver (8%). According to studies by Exida [1], for a SIL 3 safety function, PFDavg is influenced most by the failure rates of final element (49%) followed by failure rates of sensors (26%) and logic solver (25%). Consequently, final element i.e. actuated valve is the most important constituent of a safety instrumented system.

Examples of SIS applications with Actuated valves:

SIL capable final elements are meant for critical safety applications such as emergency shutdown valves (ESDV), remote operated shut-off valves (ROSOV), blow down valves (BDV), and high integrity protection systems



Safety loop failures sources by OREDA



SIL-3 Contribution to PFDavg

(HIPS). An ESDV is employed to isolate the downstream and upstream process lines of the plant while a BDV is open to flare and depressurizes the process lines when there is an upset. Both are connected to ESD and are fail safe. ESDV can also be referred to as Remote Operated Shut-off Valves (ROSOV). ROSOV is defined as a valve designed, installed and maintained for the primary purpose of achieving rapid isolation of plant items containing hazardous substances in the event of a failure of the primary containment system (including, but not limited to, leaks from pipework, flanges, and pump seals).

Closure of the valve can be initiated from a point remote from the valve itself. The valve should be capable of closing and maintaining tight shutoff under foreseeable conditions following such a failure (which may include

Lastly, HIPS is an application-specific safety system such as prevention of over-pressurization of a pipeline and is the last line of defense and should not be confused with an ESD system. HIPS is an independently instrumented system, which has typically higher safety integrity than normal shutdown systems and hence a LOPA (Layer of protection analysis) credit can also be taken if the HIPS system is an independent protection layer. Further, API 521 Annex E lists 5 principal uses for HIPS [3] one of which is eliminating the need for a relief device.

A typical HIPS for over pressure protection comprises the following:

1. 3 sensors (2oo3 voting) to detect over

Table 1 : Factors affecting safety integrity level (SIL)

Factors	Responsibility
Lambda values (Failure rates)	SIS Manufacturer
Beta factor (same cause failure)	SIS Manufacturer
Redundancy	SIS Manufacturer
Partial stroke test (PST) interval	End user
Proof test interval (PTI)	End user
Proof test duration	End user
Mission time (overhaul)	End user
Mean time to restoration (MTTR)	End user

2. A logic solver which receives and processes the input signal from the sensors and transmits the output to the SOV
3. Final elements (Actuated Valves) perform the emergency closure action via a SOV to bring the process to a safe state.

Aspects affecting Safety Integrity Level for the SIF

Though a myriad of parameters affect the SIL value of an SIF, we're going to look at only the important ones that have a significant impact on the final SIL rating.

SIL evaluation methods

The Safety Integrity Level (SIL) of a product is determined by three methods - systematic capability rating, architectural constraints and PFDavg calculation for the product. The final SIL rating achieved shall be the minimum of the SIL achieved in each of the 3 methods.

- Systematic integrity reveals design faults and if statistics are any measure 85% of the failures before start-up are due to systematic (or design) failures and only 15% of the failures happen during operation and maintenance (Source - HSE study on accidents involving industrial control systems). Systematic Capability is established by having the quality management system of the manufacturer audited as per IEC 61508.
- Architectural constraints (AC) as per IEC 61508, Part 2 takes in to account safe failure fraction values and hardware fault tolerance (HFT) to arrive at the SIL value (SFF < 60%, HFT =1, SIL=2 for type A components)
- PFD average approach (IEC 61508 Part 6) uses probabilistic calculations to arrive at the SIL rating (For e.g. in low demand applications, SIL 3 would be achieved if PFD value ≥ 10-4 and < 10-3)

Importance of factors affecting SIL compliance

There are a number of factors that affect SIL rating which are under the purview of the SIS manufacturers and/or end users. It is of paramount importance to consider the factors shown in table 1 in the design stage and neglecting any of these factors could negatively affect the SIL of the SIS while in operation.

Understanding redundancy and Hardware Fault Tolerance (HFT)

SIF architecture is decided by the failure rates and hardware fault tolerance of its components. It is possible to achieve a higher SIL level using redundancy or HFT.

- 1oo1 (1 out of 1): Single channel system and is for low level safety applications. SIL 3 with 1oo1 configuration is difficult to achieve and impracticable on the field as it involves frequent diagnostic tests (PST coverage >70%) and proof test coverage (>90%).
- 1oo2 (1 out of 2): If a failure occurs in one channel, the other is still capable of developing a safety function, e.g. redundancy in 2 Shutdown valves in 1oo2 mode
- 2oo2 (2 out of 2): Non-redundant system which reduces the probability of false trip as both channels have to fail in order for the system to shutdown, e.g. 2 Blowdown valves in a 2oo2 mode
- 2oo3 (2 out of 3): Two of the three channels are required to be functional for the system to comply with the safety function, e.g. pressure sensors in 2oo3 mode.

Difference between Partial stroke tests and Proof tests

In a partial stroke test (PST), the closure element is stroked say 10-15 degrees only. Conducting periodic PST gives the confidence that the closure element or the stem is not stuck while not hindering plant operations by causing a process upset.

However, in a proof test, if the intended safety function is close on trip and tight shut off, the closure element is closed completely from open to close position and a leak test is performed. Not conducting proof tests as per the SRS could reduce the original SIL level as PFD values increase over time without effective proof tests. It's important for SIS manufacturers and end users to understand the need for proof tests, frequency, and the procedures to be followed.

Role of common cause and mode failure

As per IEC 61511-1, common cause failure is failure of two or more components, system, or structures due to a single specific event or cause. IEC 61508-6 also lists a Beta %, which is the fraction of failures of a single component that causes both components of a redundant pair to fail simultaneously or within a short time of each other (Beta: 2% to 20%).

Though IEC 61508-6, Annex D, spells out the methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems, SIS manufacturers can take adequate precautions in the design stage to reduce the Beta factor such as

- diverse sensor technology/manufacturers in the 2oo3 sensors
- redundancy in sealing technology in valves
- diverse valve types in a 1oo2 configuration

References

[1] Final Elements and the IEC 61508 and IEC 61511 Functional Safety Standards, Chris O' Brian & Lindsey D.Bredemeyer, Exida
[2] Health Safety Executive - Remotely operated shutoff valves (ROSOVs) for emergency isolation of hazardous substances: Guidance on good practice
[3] API Standard 521 Pressure-relieving and Depressuring Systems, SIXTH EDITION | JANUARY 2014

About the Authors

K.S.Patil is, Head - Product Design, R&D at L&T Valves Limited. He holds a Bachelor of Technology (B.Tech)-mechanical engineering degree. He has over 30 years of experience in the Valve Industry. He is responsible for Design & Development of Industrial Valves of different types. He holds nine patents related to Valves.

Jaisingh Jadhav is Senior Deputy General Manager – Business Development heading the North American business of L&T Valves Limited. He holds a Bachelor of Engineering degree in Mechanical Engineering and has 24 years of working with L&T.

Ram Viswanathan has 12 years of experience at L&T Valves in different engineering roles in Valves design, R&D & Reliability engineering. He holds a Bachelor of Engineering (B.E.Hons.) degree in Mechanical Engineering, is professionally registered as a CFSP (Exida) and as an Incorporated Engineer (ImechE).