When SIL suitability is required for final control elements

by Riyaz Ali, Emerson Process Management, United Arab Emirates

Final control elements (control valves or safety shut down valves) are the key components of any closed loop control system, whether used for a basic process control system (BPCS) or for a safety instrumented system (SIS).

Financial constraints derive different constructions of valves suitable for throttling vs. on-off applications.

However, due to past accidents, reliability has become a key criterion for valve selection process. Many of process industries based on their plant specific experience are tempted to use control valves for safety shut down applications, specifically smaller size valves, which may not be cost-prohibitive. This article will provide clarity on when to assign the SIL suitability for valves used in different scenarios (process control vs. safety shut down) and establish criterion to assign safety integrity level (SIL) applicability for "final element".

With wider adoption of IEC 61508 and 61511 standards, many of the process industries are looking closely into their safety instrumented system and trying to embrace standards. Final control element (FCE) as part of safety instrumented function (SIF) loop and basic process control system (BPCS), plays an important role. However, confusion remains when SIL suitability is required for valve.

EC61511 sheds light on basic definitions of BPCS and SIS, which allows clarifying the exact need. Using prospective guidelines provided in the standard, it can be established when SIL suitability of valve is required.

Safety integrity level (SIL) is the discrete level for specifying the safety integrity requirements of the safety instrumented functions. It is a quantifiable measurement of risk used as a way to establish safety performance targets of SIS systems. A SIL level can be expressed in terms of probability of failure on demand (PFD) or risk reduction factor (RRF). Risk reduction factor is simply a reciprocal of PFD (1/PFD). SIL levels are designated in terms of PFD or RRF as a range of numbers.

PFD is a value that indicates the probability of a system failing to respond to a demand. PFD is a function of test interval time and failure rate of the equipment under control.

In short, to establish a SIL suitability rating for a safety instrumented function (SIF) loop, a PFD value needs to be computed for components of the loop (SIF loop consists of sensor, logic solver, final element) To calculate PFD, an equipment failure rate number is required.

Failure mechanism

Failures are categorised so that failure data can be organised in a consistent way. ISA technical report ISA-TR84.00.02-2002 – Part 1 talks about two failure modes – physical (random) failures and functional (systematic) failures.

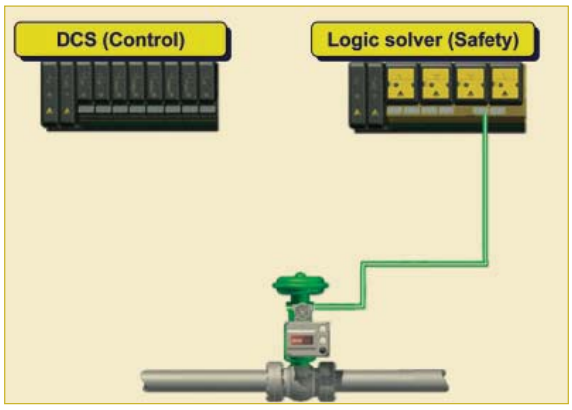

Fig. 1: Case 1.

Physical or random failures result from the degradation of one or more hardware mechanisms. It is often permanent and attributable to some component or module. For example, when a control valve is at the end of travel and not moving with the change in the control signal due to a broken shaft, the failure has occurred because of a physical failure of the component in the valve.

On the other hand, functional or systematic failures are failures related in a deterministic way to a certain cause, which can be eliminated by a modification of the design or manufacturing process, operational procedures, or other relevant factors. For example, a computer program has crashed and there is no physical damage, but the system has failed. The end result is that the program is not working and a failure has occurred due to a systematic error in programming code.

A major distinguishing feature between a random failure and a systematic failure is that failures arising from a random failure can be predicted with reasonable accuracy, while systematic failures, by their very nature, can not be accurately predicted.

With a basic understanding of failure mechanisms, it is clear that with mechanical items like control valves, failures can be classified under the physical or random failure category, which is simpler by nature.

Systematic failures are typical characteristics of programmable electronic systems or microprocessor-based devices. The reliability concept has been around the industry for a long time but due to advancements in electronics and control systems, this concept is more crucial than ever before. Because a final control element is part of the control loop, its reliability data is also being questioned by end-users. This leads to a basic question:

Does a "final control element" require a SIL suitabilty rating?

To understand the exact need, let us discuss control systems used in process sector industries. Control systems are frequently separated into two categories: systems that protect the equipment, classified as "safety instrumented system" and systems that control the equipment, known as a "basic process control system." Final control elements are part of both systems.

According to IEC 61511 part 1, 3.2.3, a basic process control system (BPCS) has been defined as:

A system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1.

This definition leads us to conclude that a BPCS is any system that has a SIL<1. Therefore, SIS systems employing safety instrumented functions with a specified safety integrity level, which is necessary to achieve safety function, need to have a SIL rating equal to or above 1.

This above conclusion raises some interesting questions:

i) Why are control valves SIL certified?

Industry practices and routines generally define which valve design needs to be used for a safety versus control applications.

However, due to reliability attributes of control valves, especially on smaller sizes, make them suitable for safety applications.

Financial considerations and maintenance aspects (using same valve design for both control and safety) are making control valves attractive for safety applications. We can categorise three different scenarios as below, where control valves can be used as safety shut down valves.

- *Case 1:* Control valves which are used only as an on/off single final element
- *Case 2:* Control valves which are used in a dual purpose context (both for control and safety)
- *Case 3:* Control valves which are used in a dual purpose context in addition (redundancy) to an on/off valve

Case 1

A control valve is used for safety applications. In this case control valve is the "final element" of the SIF loop and needs to have SIL rating equal to or above 1.

Case 2

Is it possible to use a single control valve common for both safety and control?

According to IEC61511 part 1 clause 11.2.10, it states that a device used to perform part of a safety instrumented function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function, unless an analysis has been carried out to confirm that overall risk is acceptable.

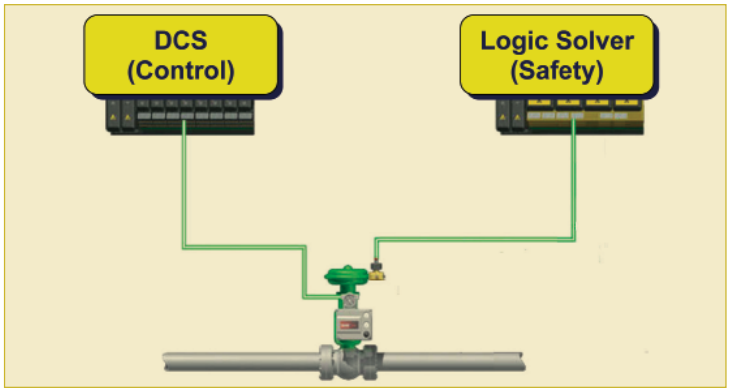

Fig. 2: Case 2.

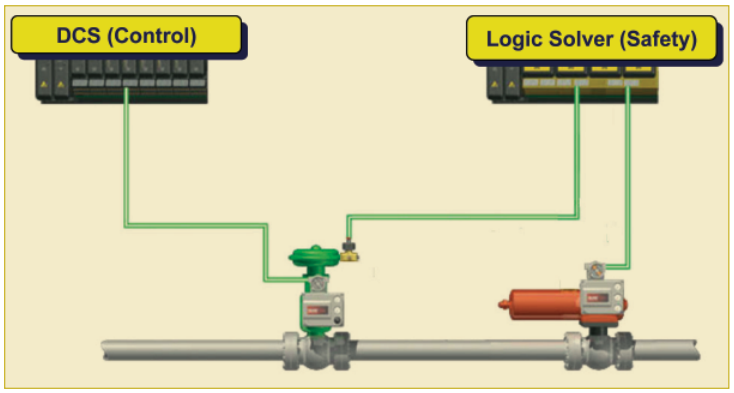

Fig. 3: Case 3.

This may possibly lead to following interpretation:

- *Yes*: If all possible failures of the control valve do not place a demand on any SIF then a control valve may be used with no further analysis. In this case, the control valve is the final element of the safety instrumented function (SIF) loop, and needs to have SIL rating equal to or above 1.
- *No*: If failure of the control valve will place a demand on a SIF then it may not be used as the only final element in that SIF.
- If failure of the control valve will not place a demand on SIF, for which it is intended but may place demand on any other associated SIF, then the control valve may be used in a SIF only after detailed analysis. An additional step to further analysis will be necessary in these cases to ensure that the dangerous failure rate of the shared equipment is sufficiently low. In this case, the control valve is the "final element" of the safety instrumented function (SIF) loop, and needs to have SIL rating equal to or above 1.

Case 3

In this scenario a control valve is used to provide additional hardware fault tolerance for higher SIL application, which is similar to using a control valve for safety but with the added burden of justifying and verifying the SIF design and its final SIL value.

ii) Why are control valves that are used in a BPCS required to be SIL certified?

As per IEC definition, a SIL rating is not required but it is possible that reliability data for a valve may be required. Industry or end users may require failure rate data of equipment or in loose term MTBF (mean time between failure).

Essentially *MTTF* (mean time to fail) is the right term to define product reliability. It is usually furnished in units of hours. This is more common for electronic components, but trends are seen even for mechanical items.

iii) How can MTTF provide useful data for the calculation of PFDavg (probability of failure upon demand)?

MTTF can be simplified to:

1/(sum of all failure rates) or equal to $1/\lambda$.

In general, components of MTTF can be categorised in the following categories:

- Safe detected (λ^{SD})
- Safe undetected (λ^{Su})
- Dangerous detected (λ^{SD})
- Dangerous undetected (λ^{Su})

This data leads to useful information:

- $MTTF_s$ (mean time to fail safe) and
- $MTTF_{cf}$ (mean time to fail dangerous)
- *SFF* (safe failure fraction)

$MTTF_s$ can be computed by adding $(\lambda^{SD} + \lambda^{SU})$ and reversing the number

$MTTF_{cf}$ can be computed by taking λ^{DU} and reversing the number.

SFF can be computed using the equation:

$SFF = 1 - (\lambda^{DU}) / (\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU})$, or

$= (\lambda^{SD} + \lambda^{SU} + \lambda^{DD}) / (\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU})$.

PFD_{avg} can be calculated using simplified equation of failure rate of equipment under control (EUC) times test interval divided by two.

$MTTF_s$ calculations provide plant availability, which is a very important measurement of process plant up-time capability. A spurious trip that is considered a safe but unplanned trip may be too strenuous for piping and other equipment. Not only are production and quality affected, profits may be as well. Also, it is important to consider the higher risk associated with plant start up. IEC 61 508 stresses more on "safety event", in case of demands, which relates to dangerous undetected failures and are used to compute PFD_{avg}.

As such, mechanical equipment like valve bodies and actuators do not have any diagnostics capabilities. According to IEC 61508 part 2, Table 2, with a hardware fault tolerance (HFT) of zero, they can only be used in SIL 1 applications. A digital valve controller mounted on a "final control element" improves the diagnostic coverage factor, which in turn improves the SFF number, allowing the possible use of higher SIL rated applications (per IEC 61508 part 2, Table 3) by use of the partial stroke test.

Conclusion

If a control valve is designated to carry out a safety function then it should meet the SIL level of the safety instrumented system function loop. In this case, failure rate numbers will be required to compute the total PFDavg of the loop. The end user may possibly ask for third party certification to comply with IEC 61508 requirements to meet certain SIL suitability. However, if a control valve is designated for normal process control then as per IEC61511-3 part 1, section 3.2.3, basic process control system, the definition does not designate control valves to have SIL suitability.

References

[1] International Electrotechnical Commission, "Functional Safety - Safety instrumented systems for the process industry sector" – IEC61511

[2] International Electrotechnical Commission, "Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems" – IEC61508

[3] Control Systems Safety Evaluation & Reliability – William M Goble

[4] ISA Technical report ISA-TR84.00.02-2002 – Part 1

Contact Mark Tapson,
Emerson Process Management,
Tel 011 974-3336,
mark.tapson@emerson.com

This article was published by EE Publishers, in June 2011 - EngineerIT and is published with permission.