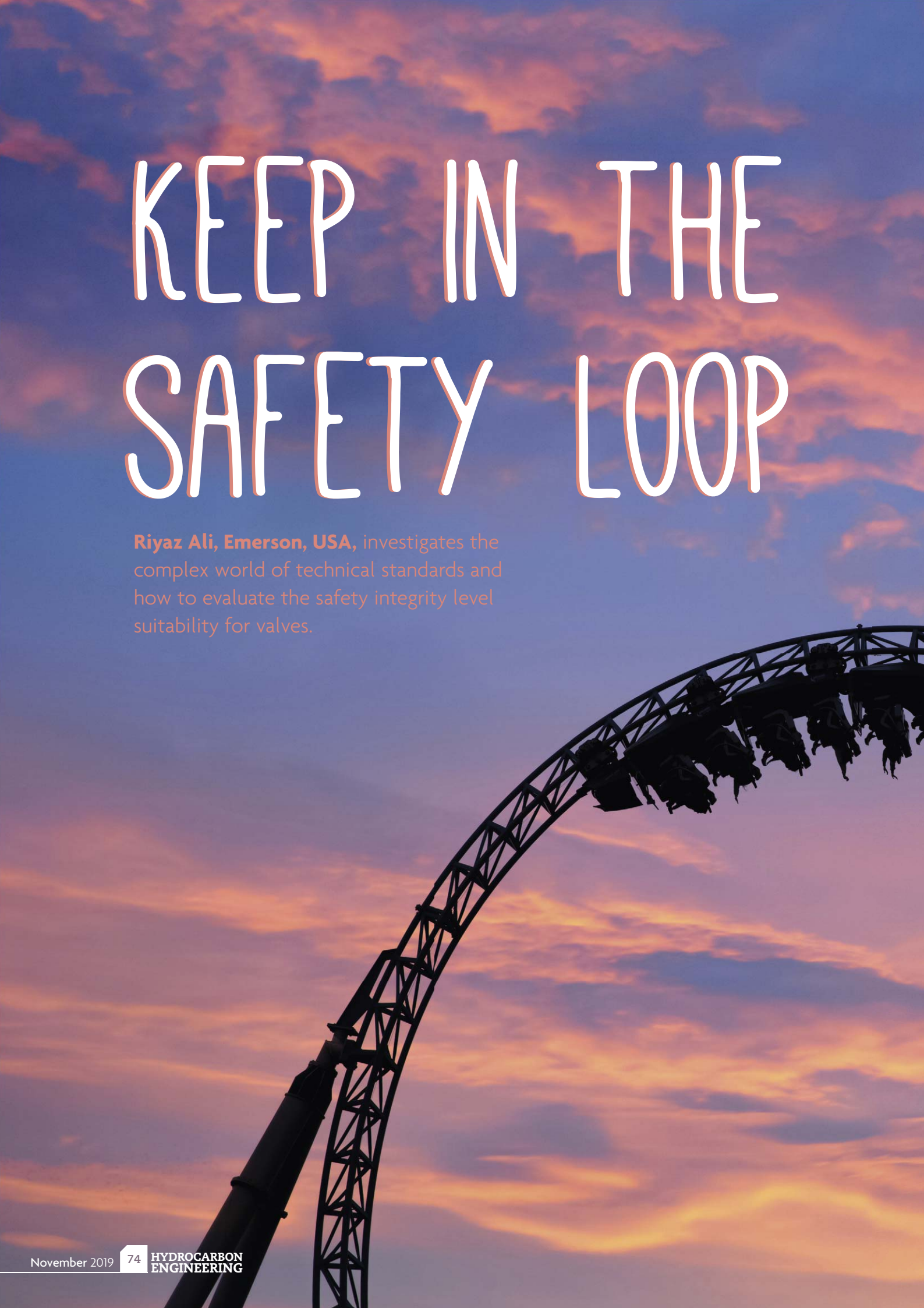
KEEP IN THE SAFETY LOOP

Riyaz Ali, Emerson, USA, investigates the complex world of technical standards and how to evaluate the safety integrity level suitability for valves.



The technical standards IEC 61508 and 61511 are designed to support functional safety in industrial processes, and have been widely taken up by industries around the world.

With the implementation of these standards, many customers are closely looking into their safety instrumented system (SIS) and trying to embrace the requirements effectively.

Final control elements (FCEs), such as control valves, are at the heart of basic process control systems (BPCS). Similarly, final elements (FEs) play an important role as part of a safety instrumented function (SIF) loop (Figure 1).

IEC 61511 sheds light on the basic definitions of BPCS and SIS. Using tools and mechanisms provided in the standard, it is possible to establish when safety integrity level (SIL) suitability of a valve is required.

A BCPS, consisting of a transmitter, controller and control valve, operates under dynamic conditions, with outputs constantly being adjusted for process control. In terms of FCE use, it is a high-demand system.

In contrast, a SIS is typically passive, with low demand, and takes action only when a dangerous condition is detected. It consists of a sensor, logic solver and FE, and is designed to carry out one of three purposes:

- To automatically take the process to a safe state if any specified conditions are violated.
- To permit a process to move forward in a safe manner when specified conditions allow (these are described as permissive functions).
- To take action that mitigates the consequences of an industrial hazard.

Safety availability is crucial for a SIS, so mechanical integrity checks are important and the system is subject to audit by regulatory authorities.

However, end users are often left unsure when SIL suitability is required for the valve.

Defining SIL suitability requirements

IEC 61511 (Part 1, 3.2.3) defines a BPCS 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

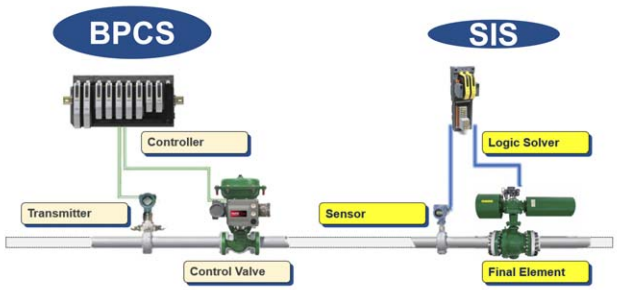


Figure 1. The role of control valves and safety shutdown valves.

manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1."

From this it can be inferred that a BPCS is any system with a SIL ≤ 1. This in turn means that an SIS using SIF with a specified SIL, which is necessary to achieve safety function, needs to have a SIL rating ≥ 1.

The SIL specifies the safety integrity requirements of the SIF and is a quantifiable measurement of risk, used as a way to establish safety performance targets of SIS systems.

A SIL can be expressed in terms of probability of failure on demand (PFD), a value that indicates the probability of a system failing to respond to a demand.

It is also sometimes given in terms of risk reduction factor (RRF), which is simply a reciprocal of PFD (1/PFD).

PFD_{AVG} is a function of test interval time and failure rate of the equipment under control. In short, to establish an SIL suitability rating for a SIF loop, a PFD_{AVG} value needs to be computed for the components of the loop (sensor, logic solver, FE)

To calculate PFD_{AVG}, an equipment failure rate number is required.

Physical and functional failures

Failures are typically categorised as physical (random) failures, and functional (systematic) failures.

Physical failures are caused by the degradation of one or more hardware mechanisms. It is usually permanent and often can be attributed to a specific component or module.

For example, when a control valve is at the end of travel and is 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.

Functional failures, in contrast, are related in a deterministic way to a certain cause, which can be eliminated by the design or manufacturing process, operational procedures or other relevant factors. Functional failures may be permanent or may be transient in nature.

An example of this type of failure is a computer program which has crashed, causing 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.

The key distinguishing feature between physical and functional failures is predictability. Using failure rate data obtained from operating experience, it is relatively easy to predict a physical failure with reasonable accuracy. Functional failures, by their nature, cannot be accurately predicted.

This leads us to the question: does an FCE require a SIL suitability rating?

Determining valve reliability

As established earlier, a BPCS is a high demand application for control valves, and these valves are continuously changing position based on input commends from the distributed control system (DCS).

An SIL rating is not required, but reliability data may be required for a valve. For example, a customer may request the mean time between failure (MTBF) for a particular valve assembly.

The correct term for defining product reliability is mean time to fail (MTTF), usually supplied in units of hours. This is more commonly applied to electronic components, but trends are available even for mechanical items.

FCE manufacturers can help industry end users by providing MTTF data for devices and equipment. The MTTF provides useful data for the process industry, and the components of MTTF can be divided into four categories:

- Safe detected.
- Safe undetected.
- Dangerous detected.
- Dangerous undetected.

This leads to the establishment of useful information including the mean time to fail safe (MTTFs), mean time to fail dangerous (MTTFd), and safe failure fraction (SFF).

MTTFs calculations provide plant availability, which is a very important measurement of process plant uptime capability and may impact upon production and quality at the plant.

Similarly, PFD_{AVG} can be calculated using computational methods. This data, along with field experience obtained while talking to various process sector industries, can clarify basic queries on the reliability of valves.

Control valves and SIL

Individual devices do not have a SIL rating. However, these components can be assessed as suitable for use in a SIF loop at a particular SIL.

Generally, industry practices and routines define which valve designs should be used for safety vs control applications.

However, the reliability of control valves make them suited to many safety applications, and from both financial and maintenance standpoints there are benefits in using the same valve designs for both purposes.

Control valves used in safety scenarios can be categorised into three different usages:

- An on/off FE (Figure 2).
- A dual-purpose control and safety use (Figure 3).
- A dual-purpose use in addition to an on/off valve (Figure 4).

If a control valve is designated to carry out a safety function, then it should meet the SIL of the SIF loop.

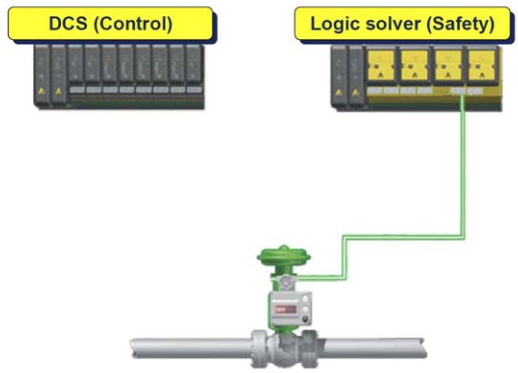


Figure 2. An on/off FE control valve.

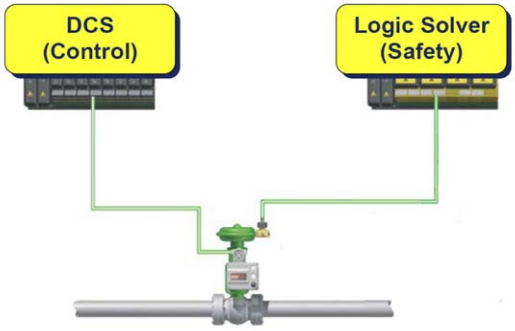


Figure 3. A dual-purpose control and safety valve.

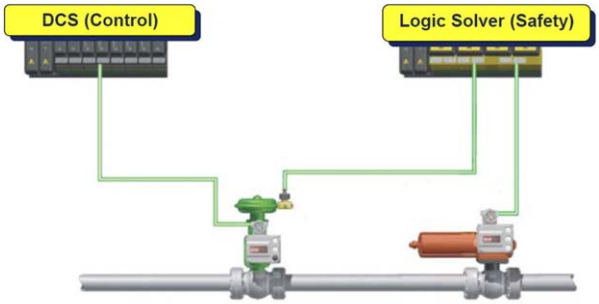


Figure 4. A dual-purpose control and safety valve with an on/off valve.

In this case, failure rate numbers will be required to compute the total PFD_{AVG} 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 it is not required to have SIL suitability.

Proof-testing to reduce PFD_{AVG}

The FCE used in BPCS is nearly always dynamic, so there are no concerns such as hidden failures.

However, the FE in SIS is regarded as dormant (passive), remaining in a static position, without any mechanical movement, for long periods of time. It only moves when predetermined conditions are met or exceeded.

Without any mechanical movement, unreliability inherently increases, and SIS valves are prone to sticking due to long static dormant status.

The IEC 61511 safety life cycle insists upon validation and verification, so these valves are proof-tested at regular intervals. A partial stroke test (PST) is performed, decreasing the pressure to move the valve from 1 to 30%.

PST could be initiated remotely, using companion software (such as Emerson AMS ValveLink or snap-on), or locally, depending upon customer plant philosophy and maintenance team approval – ensuring plant production is not impacted and testing is conducted safely and reliably, without an unnecessary trip.

This testing improves the PFD_{AVG} of the valve by helping diagnose possible valve failures before they occur, moving the SIS valve into the realm of predictive maintenance.

Additional diagnostics can identify friction build-up, valve shaft shear, air supply pressure deviations, pneumatic path leakage, and stick slip phenomena.

Correctly identifying the SIL requirements for FCEs provides a number of key benefits to the end user, including:

- Safer systems with lower failure rates.
- Lower costs for engineering, operation and maintenance by correctly allocating SIL for SIF loops.
- Proper testing interval allocation.
- Reduced risk.
- Consistent valve design across the plant.
- Compliance to industry standards IEC 61511.
- Reduced cost of ownership.
- Lower manpower requirements.

Conclusion

Mechanical equipment, such as valve bodies and actuators, do not have any diagnostics capabilities, so they can only be used in SIL 1 applications. A digital valve controller mounted on an FE improves the diagnostic coverage factor, which in turn improves the safe failure fraction (SFF) number, allowing the possible use in higher SIL-rated SIF applications.

Clear understanding of failure mechanisms for electronic components and mechanical parts will help end users to design their BPCS and SIS related field devices more optimally and accurately.

This will eliminate initial premature failures and unnecessary plant trips during normal operation. It will also help end users determine what systems are fit for purpose, which will result in optimum engineering with capital cost savings.

If the FE is designated to carry out a safety function, then it should meet the SIL level of the SIS function loop. In this case, failure rate numbers will be required to compute the total PFD_{AVG} 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 an FCE is designated for normal process control then, as per the IEC 61511-3 (Part 1, 3.2.3, BPCS) definition, the control valves do not have SIL suitability requirements.