

Reliability data and the use of control valves in the process industry in accordance with IEC 61508/61511



Translation of special print from
atp – Automatisierungstechnische Praxis
Volume 47 · Issue 2 · 2005

By:
Thomas Karte, Eugen Nebel (SAMSON AG)
Manfred Dietz, Helge Essig (Infraserv Höchst)

Reliability data and the use of control valves in the process industry in accordance with IEC 61508/61511

Thomas Karte, Eugen Nebel (SAMSON AG) and Manfred Dietz, Helge Essig (Infraserv Höchst)

IEC 61508 and IEC 61511 are the relevant standards for the specification and design of safety-related control loops in the process industry. Control valves used in these loops play a key role when it comes to determining the safety integrity level (SIL) of the safety instrumented function (SIF). A wide variety of sensors and PLCs, the other key components in the safety loop, are available with validated data concerning their probability of

failure. However, this sort of data is only available for a limited number of control valves as statistical proof is difficult to obtain due to the multitude of process conditions that exist in the chemical industry. This paper describes the investigation method used for a series of control valves. The user can determine the SIL achieved using this investigation data, the planned plant structure, and an exact analysis of the process.

Keywords: IEC 61508/IEC 61511/control valve/reliability/proven in use/SIL

1. Demands placed on valve engineering

While IEC 61508 is the standard applicable for safety engineering, IEC 61511 deals with its specific implementation in process engineering. Based on an analysis of possible hazards and risks, action needs to be taken to reduce the remaining risk to an acceptable level. This may include installing safety instrumented functions (SIF) to protect or prevent individual, defined hazardous conditions. These SIFs are part of the entire safety instrumented system (SIS) which is implemented separately from the basic process control system (BPCS). Around 2 % to 4 % of all control valves in a typical chemical plant are part of an SIF. A typical safety loop (Fig. 1) to shutdown a pipeline, for example, comprises a sensor, a safety PLC, and a valve usually fitted with a pneumatic actuator and a solenoid valve, which acts as the interface to the PLC. To size this safety loop and select the appropriate devices, the user must perform and document structural considerations and quantitative calculations concerning reliability. As a result, manufacturers often receive queries concerning their products' probability of failure.

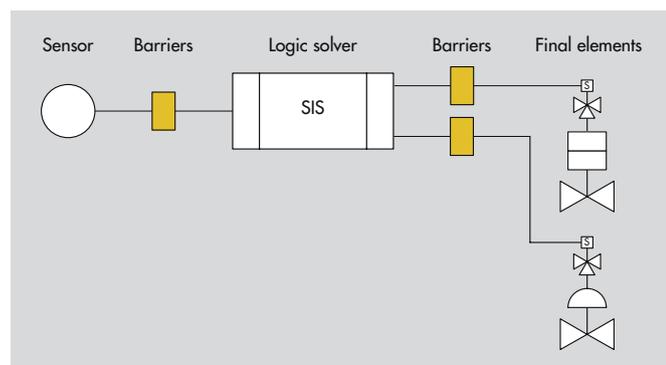


Fig. 1: Safety instrumented function (safety loop)

Based on these considerations, an entire safety loop is rated with a certain SIL. This SIL rating includes the performance of all the components in the loop. Generally, the control valve is regarded to be most important, followed by the sensor. The PLC has the best reliability data concerning probability of failure, even though it has a complex design and is made up of numerous individual components. The reason for this are the precisely defined environmental conditions, i.e. the PLC is operated in the control room and not in the field. Sensors and the control valve, in particular, are field instruments which are exposed to environmental and process conditions. The process conditions are even more complex and difficult to identify when the environmental conditions can be defined by the temperature, humidity, vibration, or even corrosiveness of the atmosphere. Statistical statements are hard to make due to the multitude of conditions.

As a result, data for control valves are generally not available. For example, the safety automation equipment list at www.exida.com includes numerous sensors, barriers, PLCs, and other instruments. However, merely three manufacturers are listed in the valve category (as of October 2004), SAMSON being the only one with valves for general applications in process engineering. A published paper names a further case for applications with burner controls and intended for use with oil and gas [1]. A glance at the corresponding database using the SILver (SIL verification) tool from Exida indicates very low probabilities of failure for these valves.

This article will deal with the background of compiling data and the reliability data achieved. Additionally, the article will

Table 1: Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers.	
SIL	Minimum hardware fault tolerance (see Clause 11.4.3 and Clause 11.4.4)
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

discuss how users can apply these data for their processes and how to determine the SIL of an entire safety loop.

Reliability data can be determined in two ways in accordance with IEC 61508 and IEC 61511.

- Performing an FMEA (Failure Mode Effect and Diagnostic Analysis, [2]). This method is particularly interesting for newly designed constructions. All individual components and operating conditions of an inspected product are investigated, all possible faulty mechanisms are listed, and their probability and possible diagnostics assessed.
- Prior use: This method is described in IEC 61511, based on the general explanation given in IEC 61508 (proven-in-use). No theoretical observations are used to predict a device's characteristics. Instead, past use under similar conditions is analyzed and the required data are derived from the experiences made.

The second method (prior use) is of great importance for applications in the process industry due to the multitude of conditions possible in individual applications. In principle, the basis data of such a method should be provided by the user. This way of thinking is quite similar to the common term 'proven in operation' used in the German chemical industry. Transferring operational experience from the general area of instrumentation and controls to the smaller quantity of safety valves in SIFs is intended by the standard (IEC 61511-1 Clause 11.5.3). The IEC 61511 standard emphasizes the term 'prior use' in particular. In Table 1 of IEC 61511-1, a Hardware Fault Tolerance (HFT) is determined in relation to the required SIL. The hardware fault tolerance defines whether the safety-relevant function is still provided when one or more faults occur. This very far-reaching demand is simplified for prior use equipment. The hardware fault tolerance may be reduced by 1 (IEC 61511 Clause 11.4.4). The process conditions must remain unchanged so that the data can be applied. Difficulties involved on performing such an examination are described in [2]. They include:

- The large number of operating hours required
- A comprehensive recording of failures without any exclusions must be ensured even with the resulting large amount of instruments in the field
- A consistent and repeatable classification of faults is necessary to eliminate human influence.

These requirements make it almost impossible for small or medium-sized companies to compile the data themselves. It's a different story in a large chemical corporation. Specialized knowledge in instrumentation is collected in the centralized engineering department. Design as well as repairs and overhaul work are coordinated in this department and, in the same way, performed in centralized workshops. Installation, maintenance, damage, and repairs performed are documented on life cycle records.

2. Example of the prior use approach

The data listed in the safety automation equipment list for SAMSON AG valves are based on an investigation carried out by the former Hoechst AG. The Höchst Industrial Park (Fig. 2) which emerged from Hoechst AG, is one of the leading research & development sites in Europe for the chemical and pharmaceutical industries. Over 22,000 people work there in around 100 production plants. The production processes range from pharmaceutical products to pigments. Infraserv Höchst provides infrastructure services for over 80 companies on site. The key points of this investigation included:

- Long period of investigation lasting six years (1996 – 2002)
- A large quantity of around 40,000 valves used on site at the former Hoechst AG,
- Complete documentation of all failures was ensured by internal documented procedures. The central Instrumentation & Controls department acted as owner of the valves used in in-



Fig. 2: Höchst Industrial Park (Copyright Infraserv Höchst)

dividual processes and performed the inspection and repair of all cases of damage that occurred on site in all plants.

- Prior to starting the investigation, an extensive record sheet was drafted, allowing failures to be categorized. Workshop staff were specially trained to keep the variations in failure analysis as small as possible using the record sheet. Immediate findings upon detecting damage was given priority without staff attempting to mend the valves on site or doing other types of ad hoc repairs.
- A test area was set up in a decontamination room to allow inspections on valves returned from the field.
- As a result, the findings were not just data recorded in the laboratory as part of a dry run, but instead involved real failure rates gathered under typical operating conditions arising in the process industry in a variety of different production sites.
- The investigation was carried out by Infraser acting as an independent body to record the results as the MTBF (Mean Time Between Failures) for the valve series used under the given process conditions.

The SAMSON Series 240 and Series 250 valves with fail-safe functions were monitored. The resulting MTBF for applications typical of the chemical industry exists for these valve series. Safety-relevant reliability data have been compiled, taking into account internal data from the investigation and an assessment of the whole methodology by Exida. These data are listed in the already mentioned database from Exida, but are also available to customers in general.

The compiled data show surprisingly long MTBFs. Such favorable data unusual for a variety of applications or brands need explaining. The explanation is relatively simple: Both valve series have been improved over many years in close cooperation with the users. The manufacturer, as a rule, discussed critical applications with the user [3, 4]. As a result, these valves feature numerous design properties which are tailored particularly to applications typical of the chemical and pharmaceutical industries. The valve in this case is of prime concern. Key features include low-vibration V-port plugs, omission of pressure balancing while accepting the use of larger sized actuators, and the preferable use of bellows to seal the valve stem. However, the actuators also play a major role: Low-friction diaphragm actuator with optimized diaphragm materials and, in particular, integral positioner attachment, which prevents travel transmission problems arising due to mechanical faults even at high dynamic loads (Fig. 3) [5], are equally important.

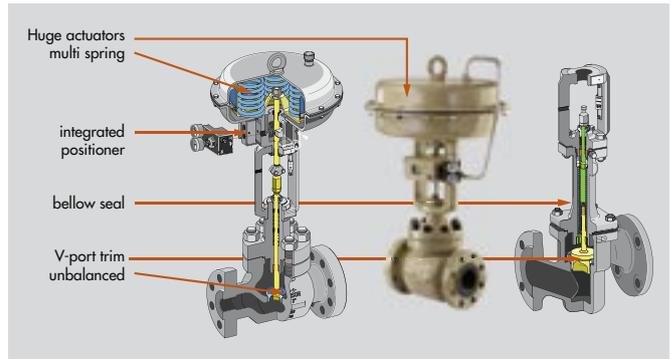


Fig. 3: Key quality-relevant design features [5]

3. The use of control valves in safety loops

The proven reliability of valve data is the basis for users to determine special values for their safety loops in certain processes. The user is, however, responsible for the exact analysis of the process and for deciding which type of valve is suitable, how it is sized and which material is to be used. The wide variations in valves' life cycles are common. For example, valves in some plants operate for over twenty years, while valves in other applications are destroyed within weeks after being installed. The disparity lies in the valves' sizing. Critical operating conditions should be avoided [6, 7]. Fundamentally, the substantial requirements specified in Part 7 of IEC 60534 need to be observed. The user must analyze the process parameters precisely. This analysis must include:

- Pressure drop across the valve, energy loss at the valve, cavitation or flashing occur with the media involved
- The outlet velocity must be limited
- Which material can be used due to the possibly corrosive properties of the process medium
- If viscous or crystallizing media are involved, the effects on the valve body and stem seal need to be taken into account.
- What are the ambient conditions like (temperature, humidity, vibrations, corrosive atmosphere).

On the whole, the valve ought to be sized cautiously, i.e. not operating it at its limits. The accessories play a further key role, for example, yoke, actuator, solenoid valve, or positioner. The interaction of components is particularly significant on sizing mechanical, electrical, and pneumatic connections. A mere statistical approach by adding up fault data of individual components is insufficient in this case. A closer look at the shut-off valve as a whole with all its points of connection should be given priority and assessed with data from proven in operation. The IEC 61508 standard is often regarded as being a number-crunching exercise and criticized for placing too much empha-

sis on quantitative analysis. The basic thought behind the standard though is not the quantitative approach to the safety loop, but concerns the entire safety life cycle, starting with the analysis and listing of possible problems, description of how to solve them, implementation of selected solutions, commissioning, and maintenance. Staff training plays a major role. This type of approach matches to a great extent the comments made above. Based on the valve's general properties backed up by manufacturer's data, the user is responsible for performing an analysis, proper implementation, and appropriate maintenance to achieve the best possible performance provided by the valve design.

Assessment of a safety loop should not end with implementation and commissioning. Assumptions are to be confirmed by observation. Particularly important features include:

- A system to record, assess, and document faults without any exclusions
- Repeated tests at predetermined intervals,
- Meeting certain performance indicators such as closing times, tight shut-off must be recorded during the performed tests in order to recognize possible deviations from acceptable state before a failure occurs.

Seen from this point of view, changed instrumentation gains new meaning. The solenoid valve is normally used to trigger the emergency shutdown valve. Modern diagnostic features in a positioner [8] allow, however, to consider the inclusion of the above mentioned points automatically. The positioner naturally needs to feature the same reliability concerning requirements in cases of emergency (shutdown) as the solenoid valve. The integration of all the components including positioner, solenoid valve, and limit switches required by the valve into one housing is particularly beneficial. Such devices are available (Fig. 4). Extended tests can be used to prolong the plant's running time, in particular, cases when the tests are relevant to requirements specified in IEC 61508. But, even here, a special investigation into the conditions is still required in individual cases to obtain the effectiveness of the diagnostic coverage used. Corresponding suggestions were made, for example, in [9] and will be discussed in detail in another publication.

4. Conclusion

The successful implementation of the standard requires manufacturers and users to work closer together than ever before. The user needs to provide background data about the reliability of their products. Users need to discuss application conditions at least concerning valves in critical plants together with the manufacturer. Using anonymous products such as is the practice with electronic components described in catalogs with

a few reliability data is inconceivable in this case. The user must observe the device in a running plant and the findings should be passed on to the manufacturer even when the device runs properly, not just when faults occur. Based on this cooperation, the full potential of individual devices can be exploited, the best level of safety achieved and cost-cutting capacities recognized.

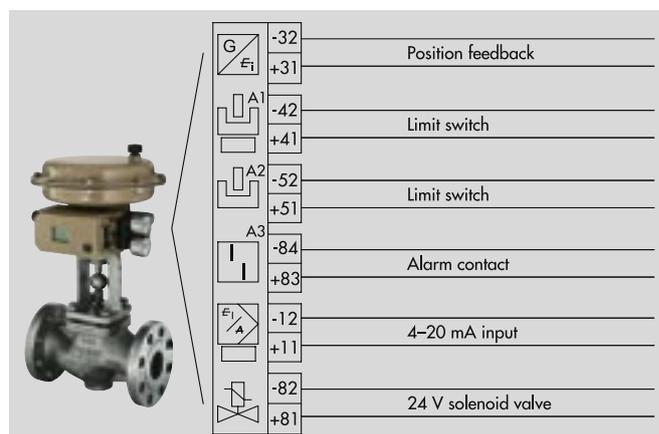


Fig. 4: Positioner with integrated solenoid valve and limit switches

References

- [1]: Muschet, A.: Sicherheitseinstufung von Stellgeräten in Anforderungsklassen auf Grundlage der IEC/EN 61508, Industriearmaturen 1/2004
- [2]: Exida: Selecting Instrumentation Equipment for Safety Applications, Version 2.0, February 2004, www.exida.com
- [3]: Kiesbauer, J.: Control Valves for Critical Applications in Refineries (Stellventile bei kritischen Prozessbedingungen in Raffinerien), Industriearmaturen, 3/2001
- [4]: Diener, R.; Friedel, L.; Kiesbauer, J.: Sizing Control Valves for two-phase flows (Auslegung von Stellgeräten bei Zweiphasenströmung), Automatisierungstechnische Praxis, 3/2000
- [5]: König, G., Kiesbauer, J.: Erst die Hardware, dann die Software, CAV 7/2003
- [6]: Meffle, Kiesbauer, J.: Ein Leitfaden für eine vereinfachte Auslegung eines Stellgerätes auf der Basis von EN 60534, Automatisierungstechnische Praxis, 8, 2001
- [7]: Herbrich, R.: The Enemy in the Valve – Critical Operating Conditions in Control Valves (Der Feind im Ventil – Kritische Betriebszustände bei Stellventilen), Automatisierungstechnische Praxis, 7/2002 IEC 61508, IEC 61511
- [8]: Kiesbauer, J.: New integrated diagnostics strategy for digital positioners (Neues, integriertes Diagnosekonzept bei digitalen Stellungsreglern), Automatisierungstechnische Praxis, 4, 2004
- [9]: Enhanced reliability of final elements, Conference On Functional Safety, Jurata (Gdansk), Poland, 16 September 2004



Dr. rer. nat. Thomas Karte is responsible for application engineering for electropneumatic devices at SAMSON AG in Frankfurt. He is a member of the expert committee of GMA 4.14 concerning valves for flowing media, DKE committee K 963, and Working Group 6 of IEC SC65B.
SAMSON AG · MESS- UND REGELTECHNIK
Weismüllerstr. 3, 60314 Frankfurt am Main, Germany
Phone: +49 69 4009-2086 · E-mail: tkarte@samson.de



Dipl.-Ing. Eugen Nebel is head of the development department for control valves at SAMSON AG. He is a member of the DKE committee K 963.
SAMSON AG · MESS- UND REGELTECHNIK
Weismüllerstr. 3, 60314 Frankfurt am Main, Germany
Phone: +49 69 4009-1595 · E-mail: enebel@samson.de



Manfred Dietz is head of the test laboratory at Infracerv GmbH & Co Höchst AG in Frankfurt.
MSR-Analysentechnik, Prüflabor
Industriepark Höchst – D710
65926 Frankfurt, Germany
Phone: +49 69 305-2663
E-mail: manfred.dietz@infracerv.com



Dipl. Ing. Helge Essig is responsible for the coordination and implementation of typetesting and tests of instrumentation and controls conforming to IEC 61508/IEC 61511 at Infracerv. He is a member of the expert committee of GMA 4.14 concerning valves for flowing media.
MSR-Analysentechnik, Prüflabor
Industriepark Höchst – D710
65926 Frankfurt, Germany
Phone: +49-69-305-15077
E-mail: helge.essig@infracerv.com



SAMSON AG · MESS- UND REGELTECHNIK · Weismüllerstraße 3 · 60314 Frankfurt am Main · Germany
Phone: +49 69 4009-0 · Telefax: +49 69 4009-1507 · E-mail: samson@samson.de · Internet: <http://www.samson.de>