Innovative Control Technology

SPECIAL PRINT

Safety in the Process Industry

SAMSON AG
Manuel Hinkelmann
Marcel Richter
Monika Schneider

SAMSOMATIC
Marc Belzer

Translation of special print from:
cav 6-2014, cav 8-2014, cav 10-2014, cav 12-2014

Table of contents

Safety in the Process Industry

Functional Safety: Different Roles in the Process Industry

Seveso, Bhopal, Piper Alpha: places where some of the worst accidents in the chemical and petrochemical industry occurred. The catastrophes, which resulted in numerous deaths, were caused by human error and technical failures: Not only the applicable rules and regulations governing industrial accidents force plant operators to reduce the residual risk created by their plants to a tolerable level.

In 1976, an uncontrolled exothermic reaction in a reactor in Seveso, Italy caused a safety relief valve to burst open. As a result, an unknown amount of a highly toxic dioxin was released into the atmosphere. In Bhopal, India, several tons of toxins were released into the atmosphere in 1984 due to a failure of the safety systems. In 1988, a fire destroyed the Piper Alpha offshore oil platform moored in the North Sea. This catastrophe was caused by a temporarily missing high-pressure valve and other sources of error, such as a negligently secured pipeline, insufficient explosion protection and external platforms continuing to pump oil towards Piper Alpha during the fire.

Deaths and severe injuries among staff and residents as well as environmental damage are merely the visible consequences of such accidents.

The risk produced by a plant increases with the severity of consequences created in the event of failure and the probability that a failure occurs. To reduce the residual risk to a tolerable level, plant-specific emergency plans, passive and active mechanical safety measures as well as electronic safety-instrumented systems (SISs) are implemented; such safety-instrumented systems are independent of the basic process control system and comprise sensors, a safety control system and a final element. There is a clear assignment of tasks in the SIS: The sensors measure the controlled variable (e.g. temperature, pressure, filling level) and transmit the measured data to the safety-related control system. The safety-related control system processes the received data independently of the basic process control system (BPCS) and causes the final element to perform the safety-instrumented function in the event of failure. The final element performs the safety-instrumented function, i.e. it opens or closes the valve as required. The term "final element" refers to the entire control valve including all mounted accessories, such as solenoid valve, positioner and booster.

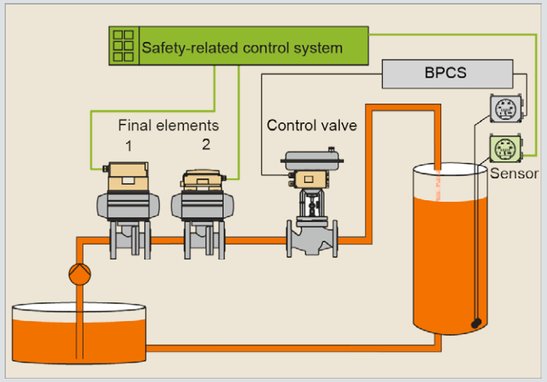


Fig. 1 · Architecture of a safety-instrumented system comprising a sensor, two final elements and a safety-related control system (example taken from SAMSON training system)

These units are expected to interact in the event of failure and maintain the plant in a safe state. The performance required of a safety-instrumented function is quantified in four discrete safety integrity levels (SIL 1 to 4). The safety-instrumented system is categorized based on IEC 61508 and IEC 61511. While IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems) is directed at manufacturers of individual units for use in a safety-instrumented system, IEC 61511 (Functional safety - Safety instrumented systems for the process industry sector) is relevant to planners, constructors and operators of safety-instrumented systems.

Role of manufacturers

As part of a holistic safety life cycle, manufacturers of safety units develop the required hardware and software in compliance with IEC 61508. As a result, they are also responsible for assessing the safety of their products. Some of the important factors in this area include the materials used or the technical design a unit is based on. Alternatively, the suitability of a product for use in a safety-instrumented system can be determined based on prior use, which comes with the benefit that real ambient and process-related influences are taken into account.

The manufacturer determines the characteristic values relating to safety based on the mathematical models and calculation methods of the FMEDA (Failure Modes, Effects and Diagnostic Analysis) and possibly based on existing data from prior use. The characteristic values are documented and confirmed in a product-specific manufacturer's declaration that the manufacturer bears responsibility for. It is possible to have an independent body supervise and certify the development process. The manufacturer is also responsible for providing instructions on a product's proper use, which are given in the safety manual. The characteristic values provided by the manufacturer only describe the safety integrity that an individual unit can achieve.

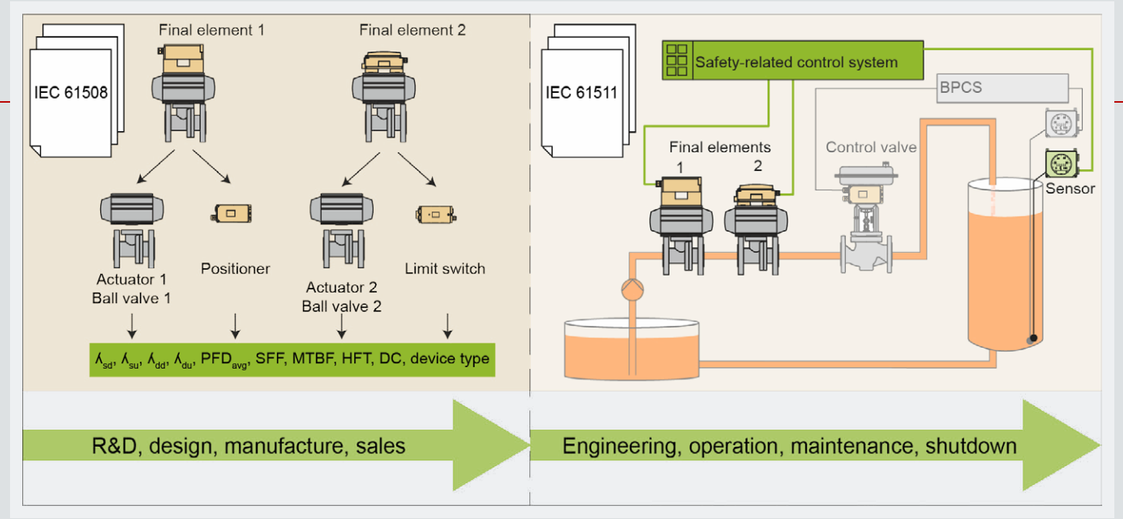


Fig. 2 · Different roles in the process industry exemplified by the safety life cycle of a final element (left: manufacturers, right: planners, constructors and operators)

Role of planners and constructors

Plant operators analyze the requirements placed on the safety-instrumented system (SIL rating) using a suitable method, such as risk graph, risk matrix or LOPA (Layer of Protection Analysis). Planners and constructors are responsible for designing the entire safety-instrumented system to match the SIL rating and selecting the individual safety units (sensors, final elements and safety control system) depending on the latest developments in safety engineering. According to the standard, the suitability of a selected unit must be certified for the ambient conditions and the specific process. For the use of control valves, this means that valves must be sized properly and that the sizing process is to be documented accordingly.

The achieved performance of the safety-instrumented function, or SIL rating, depends on the device type used (degree of complexity according to the standard), the selected architecture and the probability of failure. Ideally, operators should rely on probability of failure values gathered from their own experience, i.e. prior use. Additionally, the data provided by NAMUR can be used. The organization also publishes a series of practical recommendations for plant planners and constructors including NAMUR Recommendation NE 130, which deals with proven-in-use devices, or NAMUR Recommendation NE 106 on test intervals for safety-instrumented systems.

λ_{sd}	Safe detected failure rate
λ_{su}	Safe undetected failure rate
λ_{dd}	Dangerous detected failure rate
λ_{du}	Dangerous undetected failure rate
PFD_{avg}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction
MTBF	Mean Time Between Failures
HFT	Hardware Fault Tolerance
DC	Diagnostic Coverage
Device type	Type A non-complex devices (e.g. positioners) Type B complex devices (e.g. electronic limit switches)

Table 1 · Characteristic, safety-related values documented and confirmed by product-specific manufacturer's declarations or certificates

Authors:
Marcel Richter, Product Management and Marketing for Positioners and Valve Accessories, SAMSON
Monika Schneider, Technical Documentation, SAMSON

Functional Safety: Protecting Control Valves Against Failure

Plant planners, constructors and operators benefit from the expertise of manufacturers in selecting individual safety-related components. The companies associated in the SAMSON GROUP, for example, develop and manufacture the entire range of final elements from valves and actuators to valve accessories, such as positioners, solenoid valves or limit switches. As a result, users can rely on the proper functioning of all components.

A safety-instrumented system (SIS) in the process industry consists of sensors, a safety-related control system (logic solver) and a final control element. Considering the safety life cycle of the final element, a clear distribution of roles becomes evident (Fig. 2): Manufacturers of safety components develop and manufacture according to IEC 61508. Planners, constructors and operators of safety-instrumented systems follow IEC 61511. German users find a regulation with practical advice on planning, constructing and operating safety-instrumented systems in VDI/VDE 2180, which is based on the international IEC 61508 and IEC 61511 standards. The German standard stipulates that measures be implemented against systematic and random failures as well as measures related to fault tolerance.

Systematic failures often undetected

Systematic failures have a fundamental effect on the reliability of mechanical components. For the proper selection and sizing of a component, it does not suffice to achieve the required calculated safety integrity level. The component must also be selected so that its principle of operation and sizing match the process it is to be used in. Moreover, conditions must be established to ensure that the component functions reliably. For example, it is obvious that a safety valve can only function reliably on demand if it can fulfil its fail-safe function (i.e. move to the required end position) at any time. This can only be ensured if the manufacturer's instructions on assembly, installation and operation of the valve are observed. Additionally, no external mechanical influences or temporary events must impair the proper functioning of the safety valve. Systematic failures cannot be expressed statistically. They need to be mastered or excluded by suitable measures as part of a comprehensive functional safety management (FSM) system focused on failure prevention. Nevertheless, undetected systematic failures may occur. A classical example of an undetected systematic failure is a ball valve that has been assembled, installed and started up correctly, but does not perform its fail-safe action on demand as the ball is jammed in its operating position. This can happen if the valve has remained in its operating position for a longer period of time. Suitable counteraction to be taken by plant operators includes testing the proper functioning of a valve at regular intervals during plant shutdowns or performing automatic tests while the process is running, e.g. partial stroke tests (PST). Such measures represent the latest developments in safety engineering and are a reasonable addition to functional safety management.

Fig. 1 · Demonstration model of a safety-instrumented system at SAMSON

Statistically expressing random failures

Contrary to systematic failures, random failures can be expressed statistically. Such failures cannot be avoided in electronic components; in some cases, they cause the safety function to fail. Random failures of mechanical components are hard to imagine if the stipulations of the applicable standards are followed by the manufacturers (IEC 61508) and operators (IEC 61511) under a comprehensive safety life cycle approach. Even though random failures hardly ever occur in mechanical components, the standards mandate that they be taken into account. This is mainly done by the dangerous undetected failure rate λ_{DU}. This rate is given in the manufacturer's specifications. Typical values based on a worst-case estimate for proven-in-use equipment are also found in NAMUR Recommendation NE 130. Using the dangerous undetected failure rate, the average probability of failure on demand (PFD_{avg}) can be calculated. The PFD_{avg} value is directly related to the safety integrity level (SIL) stipulated in IEC 61511. The fault tolerance expresses the capacity of a safety-instrumented system to still perform its fail-safe function when hardware or software faults occur. A common method of increasing the fault tolerance is to use redundant systems. In redundant safety-instrumented systems, the failure of a single component does not affect the safety function of the entire system as a second component takes over the safety function of the faulty component.

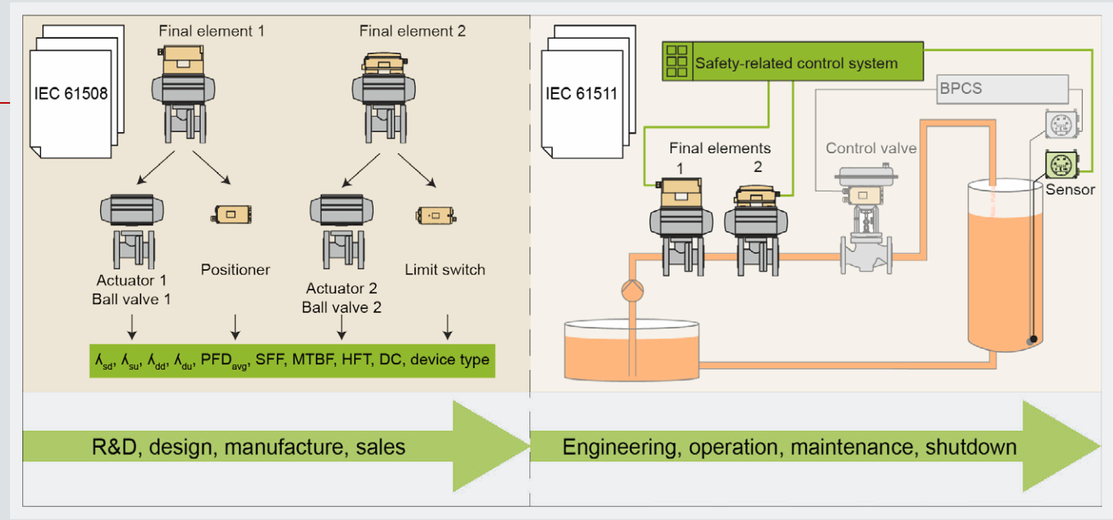


Fig. 2 · Different roles in the process industry exemplified by the safety life cycle of a final element
(left: manufacturers, right: planners, constructors and operators)

Selecting safety components

Plant planners, constructors and operators benefit from the expertise of manufacturers in selecting individual safety-related components. The companies associated in the SAMSON GROUP for example develop and manufacture the entire range of final elements from valves and actuators to valve accessories, such as positioners, solenoid valves or limit switches. Back in 1995, SAMSOMATIC already applied for certification of solenoid valves manufactured in compliance with the then-preliminary DIN V 19251 standard. Since then, the solenoid valves have been proven in use and are now being employed in smart SAMSON valve accessories as well. In 2006, a version of the Series 3730 Positioners with ESD (Emergency Shut Down) function was introduced. Since then, SAMSON equipment has been capable of emergency venting: the Series 3730 and 3731 Positioners as well as the smart Type 3738 Electronic Limit Switch with integrated solenoid valve and limit contact function. As one of the first valve manufacturers, SAMSON had its complete R&D, design, production and sales process for valves audited by TÜV SÜD according to IEC 61508-1 in December 2011. For plant planners and operators, such a manufacturer certification brings benefits in attesting prior use according to NAMUR Recommendation NE 130 as the prior use period is shortened by six months.

Despite the different roles assigned by IEC 61508 and IEC 61511, SAMSON considers itself responsible for supporting operators and providing them with information on functional safety. To do so, SAMSON holds hands-on trainings and participates in events, such as the SIL road show that tours Germany. In connection with this article, the authors want to highlight the SAMSON seminar dealing with control valves and valve accessories used in safety-instrumented systems (SSA). The seminar includes a demonstration of a comprehensive safety-instrumented system and allows all participants and trainers from R&D, product management and after-sales service to discuss topics first hand.

Authors:
Marcel Richter, Product Management and Marketing for Positioners and Valve Accessories, SAMSON
Monika Schneider, Technical Documentation, SAMSON

Check Valves in Safety-instrumented Systems: Functional Safety in Practice

Check valves increase plant safety. When mixing liquids for example, they prevent the liquid mixture from flowing back into the lines carrying the pure liquids, which would contaminate the pipelines and connected tanks.

Backflow prevention assemblies by SAMSOMATIC are mainly composed of a differential pressure transmitter, inlet and outlet valves as well as a control unit. The differential pressure transmitter senses the pressure drop between the measuring points located immediately upstream of the inlet valve and immediately downstream of the outlet valve. Under normal conditions, the pressure upstream of the inlet valve is always greater than the pressure downstream of the outlet valve. The differential pressure transmitter sends a standardized signal corresponding to the differential pressure to the control unit, where the signal is compared to an adjusted minimum limit. If the measured differential pressure is below the adjusted limit, the control unit simultaneously closes the inlet and outlet valves. Any medium backflow is thus prevented. The SAMSOMATIC backflow prevention assembly is suitable for use in safety-instrumented systems (SISs). As a general rule, the required safety integrity level (SIL) is higher the higher the requirements placed on the safety-instrumented system are. According to IEC 61511 "Functional safety - Safety instrumented systems for the process industry sector", it is described in three discrete levels (SIL 1 to SIL 3) and defines the objectives to be achieved by the components used in an SIS. Based on calculations and depending on the version, the backflow prevention assembly can be used in SIL 2 or SIL 3 applications.

Architecture for SIL 2 rating

A pneumatic ball valve with external solenoid valve is used as the inlet valve. At the outlet, a pneumatic control valve is used; it is also fitted with an external solenoid valve and additionally equipped with a positioner for normal control operation. Alternatively, the external solenoid valve is not needed if the positioner comes with an integrated solenoid valve or if the positioner includes a forced venting function even when it is controlled using a two-wire connection. The logic solver supplies the solenoid valves of the inlet and outlet valves with a control voltage (e.g. 24 V DC) as long as the differential pressure between the inlet and outlet valves is greater than the adjusted limit. In the event of emergency, i.e. when the differential pressure falls below the limit, the control unit interrupts the electric binary signal supplied to the solenoid valves. The solenoid valves cause the pneumatic actuators with fail-close action to vent. The inlet and outlet valves are closed.

Architecture for SIL 3 rating

The assembly for such applications also includes a pneumatic ball valve as the inlet valve and a pneumatic control valve as the outlet valve. Contrary to SIL 2 applications, each of the two valves is fitted with two solenoid valves connected in series. Additionally, the differential pressure measurement as well as control are performed by redundant units. As a result, the ball valve as well as the control valve are moved to their fail-safe positions by de-energizing the associated solenoid valves when the limit is not reached in one of the redundant measurement and control channels. Moreover, the outlet valve is equipped with a smart positioner. A positioner with partial stroke testing (PST) function reduces the probability of failure on demand. During a partial stroke test, the valve is briefly moved to a predefined position before returning to its operating position. If they are performed at regular intervals, such partial stroke tests can indicate that the valve is jammed in its operating position and will not be able to move to its fail-safe position on demand.

To optimize the assembly, it is possible to mount an additional electronic limit switch (e.g. Type 3738 by SAMSON) on the on/off valve at the inlet, which can perform an automated stroke test similar to the positioner on the control valve.

According to IEC 61511, the safety-instrumented functions should be separated from the non-safety-instrumented functions wherever practicable. In case a failure of the non-safety-instrumented function does not impair the safety-instrumented function, it is also possible to integrate a unit into the safety-instrumented system as well as the control loop. This possibility is available for the outlet valve used in the SAMSOMATIC backflow prevention assembly. The smart positioner allows the control valve to be used for control tasks. At the same time, the valve's fail-safe action is maintained as the solenoid valves' wiring has priority over the positioner's control function. This ensures that the actuator is vented on demand regardless of normal control operation, which forces the control valve to move to its fail-safe position.

Simultaneously using the control valve in the control loop and the safety-instrumented system provides an added benefit in terms of safety monitoring: the control function allows plausibility checks to be performed easily, for example by monitoring the set point deviation. Constant monitoring of the availability is also possible because the valve needs to move to different positions depending on the process requirements.

The SAMSOMATIC backflow prevention assembly is designed for universal use. The inlet and outlet valves are taken from the wide SAMSON GROUP product range, which allows them to be tailored to the specific conditions. For example, valve bodies in different styles and made of different materials can be selected to match the process medium and ambient conditions.

Fig. 3 · Rotary actuator with Type 3738 Electronic Limit Switch and redundant wiring of two Type 3967 Solenoid Valves

Authors:
Marc Belzer, Product Manager for solenoid valves, SAMSOMATIC
Monika Schneider, Technical Documentation, SAMSON

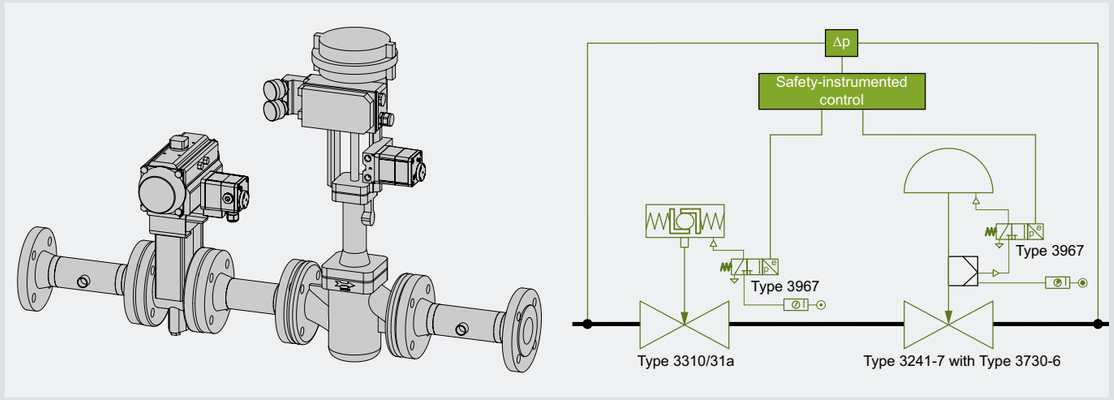


Fig. 1 · Possible backflow prevention assembly for SIL 2 rating

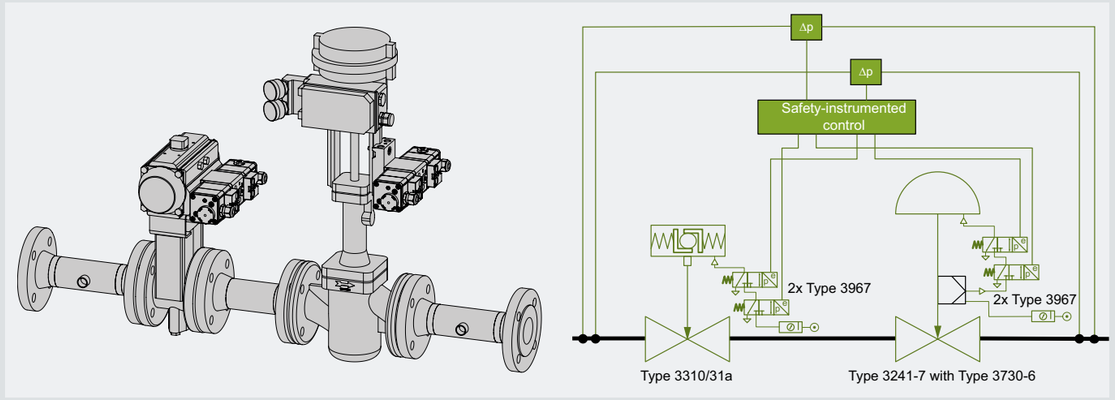


Fig. 2 · Possible backflow prevention assembly for SIL 3 rating

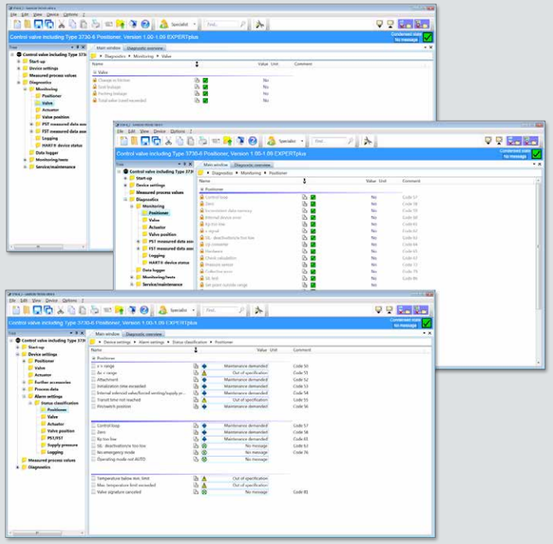
Benefits Through Integrated Valve Diagnostics: Early Detection of Weaknesses

There are obvious benefits provided by state-of-the-art valve diagnostics, particularly by diagnostic functions integrated directly into the positioner: round-the-clock monitoring of the control valve pinpoints the causes of possible malfunctions. In an ideal case, the event (i.e. a failure) can be prevented because the valve diagnostics identified weaknesses in a control valve ahead of time. This allows plant operators to bring forward necessary maintenance work and prevent plant shutdowns.

Valve diagnostics are based on the continuous collection of important data on control operation and the control valve itself in the positioner. This includes, for example recording the targeted valve position and the actual valve position reached (set point and actual value), adding up the travel cycles performed, and repeatedly saving the zero point. But it is not possible to draw any sound conclusions on the control valve's state based merely on these collected statistical data. This requires the data to be analyzed. Many of the diagnostic systems available on the market only offer their full functionality when used together with an external software tool. This solution has one major weakness: the collected data, their assessment and consequently the information on the control valve state depend on a software and require a connection to external systems. On site, the control valve state can only be read off the positioner with restrictions in most cases. This is different in positioner designs with integrated, on-board diagnostics. There, the control valve data are not only collected but also analyzed in the positioner, which makes important diagnostic data and functions available in the field independent of software and communication connections. SAMSON has over a decade of experience in integrated valve diagnostics. Right from the start, the instrumentation and controls specialist focused on decentralized methods for analyzing measured data. The EXPERTplus valve diagnostics integrated into the Series 3730 and 3731 Positioners monitor the control valve throughout its entire service life – 24 hours a day, seven days a week – without impairing the valve's control response throughout the positioner's full life cycle. The diagnostics check the start-up, control loop behavior and limit violations. By applying the monitoring functions, EXPERTplus can expose any changes in friction forces, steady-state errors and zero errors as well as assess the state of the valve trim.

Diagnostic information based on the top-down principle

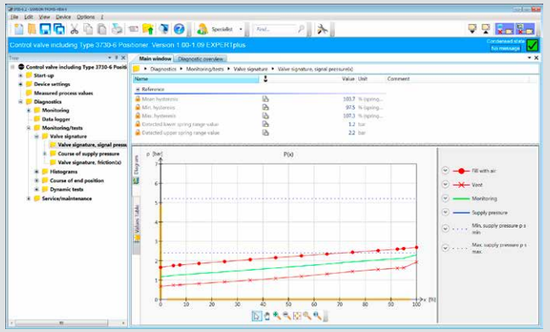
In SAMSON positioners with diagnostic functions, every fault condition that may occur in a control valve is assigned one of up to four states. The device status is shown as a condensed state. The flexible status classification allows individual messages to be assigned depending on customer requirements and complies with NAMUR Recommendation NE 107. For users, it becomes easy to detect what caused an error message, from getting a rough idea to finding the details. For example, if the positioner indicates an "Out of Specification" error message, all fault conditions classified under a different state can be excluded in a first step. As a result, the number of possible causes is reduced. Further information is provided by the error codes, which are also shown directly on the positioner display. If this on-site analysis does not suffice, plain-text messages issued over the DTM or EDDL offer further details on the type and location of the change of state that triggered the error message. In addition, diagrams help illustrate the causes. Test functions provide valuable insights into the condition and reliability of control valves during plant shutdowns or, if permissible, through in-process testing. For example, a control signal test helps assess the positioner's supply pressure and indicates possible leakages in the control valve. The step response test is particularly important as it provides information on the dynamic response of the valve. In shut-off valves that remain in one position for a long time, the test additionally prevents the plug stem from getting jammed. Cancelation criteria can be defined for the test to prevent the closure member from moving excessively or to avoid unwanted overshooting. All test results are saved in the positioner regardless of whether the tests can be triggered on site. In this case, NAMUR Recommendation NE 107 is taken into account as well.



Diagnostic messages: indication and classification on the SAMSON user interface TROVIS-VIEW

Optional accessories increase safety

Solenoid valve, position transmitter and inductive limit contacts increase safety in processes where special requirements apply. The mentioned components can optionally be integrated into the positioner, which minimizes the number of mechanical interfaces and makes the control valve more rugged. The main philosophy behind SAMSON positioners is to prevent faults.



To get the valve signature for control valve assessment, the signal pressure is plotted versus the valve position.

State-of-the-art valve diagnostics enable round-the-clock monitoring of the control valve and pinpoint the causes of possible malfunctions.

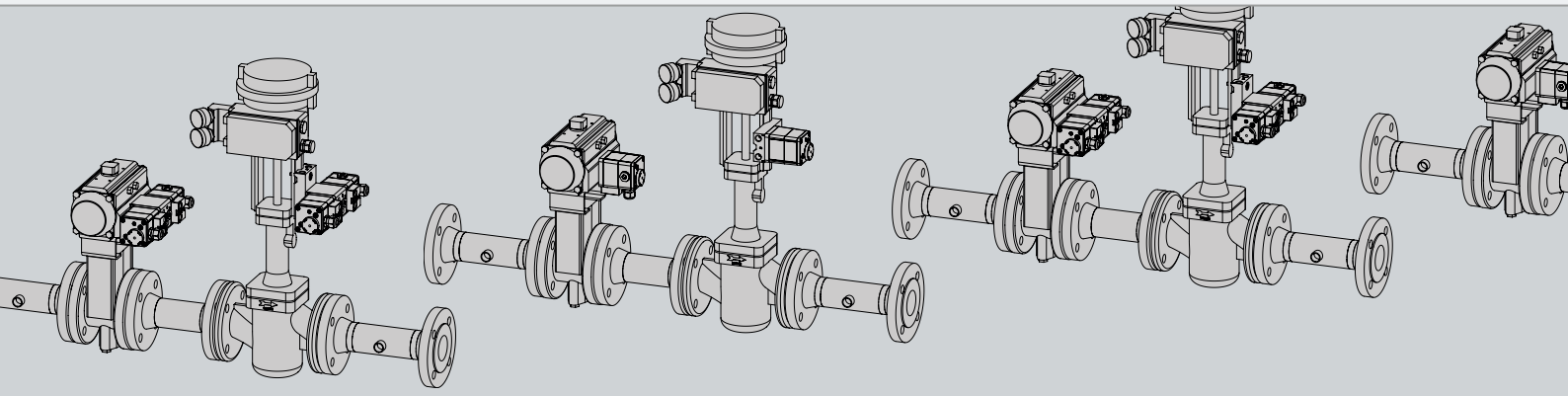
Background image: Eric Middelkoop - fotolia.com

Seamless integration into process control systems

With the Series 3730 and 3731 Positioners with diagnostic functions, the SAMSON R&D set a high standard for on-site operability early on. Nevertheless, positioner integration into an existing asset management system is equally important. Depending on the positioner version, integration is implemented using HART®, PROFIBUS PA or FOUNDATION™ fieldbus. Based on these communication protocols, SAMSON offers all standard integration options, such as EDDL and DTM. This is where the valve diagnostics integrated into the positioner come in handy since the external diagnostic software does not need to be tuned to the process control or asset management software. Extensive tests are performed at a dedicated SAMSON laboratory to ensure that each positioner type and each firmware version are compatible with the integration systems commonly available on the market.

Authors:
Manuel Hinkelmann, Product Management and Marketing for Positioners and Valve Diagnostics, SAMSON
Monika Schneider, Technical Documentation, SAMSON

Where Innovation is Tradition



SAMSON AG · MESS- UND REGELTECHNIK · Weismüllerstraße 3 · 60314 Frankfurt am Main, Germany
Phone: +49 69 4009-0 · Fax: +49 69 4009-1507 · E-mail: samson@samson.de · Internet: www.samson.de
SAMSON GROUP · www.samsongroup.net

2015-04 HD · WA 333 EN