SAMSON

MANUAL

Competence in Functional Safety

Application notes for safety-instrumented systems

Safety-instrumented system

Instrumentation

Automation

SAMSON

AIR TORQUE · CERA SYSTEM · KT-ELEKTRONIK · LEUSCH
PFEIFFER · RINGO · SAMSOMATIC · STARLINE · VETEC

Founded in 1907, SAMSON has since become a world-wide leader in the manufacture of expertly engineered control valves.

SAMSON has over 50 subsidiaries, amongst them noted manufacturers of special valves.

With our subsidiaries, we are represented in over 80 countries to assist our customers on all continents.

Contents

1 Scope

Safety-instrumented systems serve to protect process engineering plants. One process variable, e.g. pressure or temperature, is monitored by a sensor to ensure it does not exceed a certain limit. If the variable exceeds or falls below the limit, a safety PLC (Programmable Logic Controller) controls a valve, which shuts off or opens the pipeline accordingly.

These control valves are automated by pneumatic actuators controlled by solenoid valves. Some of them are equipped to feed back the end positions. It is state of the art to also use positioners. They perform diagnostic functions on the valve while a process is running, but they can also assume the solenoid valve's shutdown function. IEC 61511 and VDI 2180 stipulate that plants need to be subjected to recurrent tests to detect whether they function safely on demand. In addition, tests can be performed while a process is running. This manual provides information on automating these tests concerning:

- Components and setup
- Performance of tests
- Connection to the process control system or safety PLC
- Interpretation of test results according to IEC 61511 and VDI 2180

2 Validity and intended use of this manual

This manual is intended to assist planners and plant operators to implement state-of-the-art methods of testing control valves.

The examples and proposed equipment setups refer to selected instruments provided by SAMSON AG. Observe the intended use of these instruments as specified in the associated data sheets as well as the mounting and operating instructions. Also refer to the Competence in Functional Safety – Functional safety of globe valves, rotary plug valves, ball valves and butterfly valves manual (WA 236) published by SAMSON AG.

It is the responsibility of plant operators to draw up a risk analysis and specifications for the safety-instrumented systems in their specific plants. Requirements applying to the control valves used in safety-instrumented systems as well as to testing these valves can be derived from them.

3 Structure of this manual

We will start by introducing the requirements stipulated in the VDI 2180 standard. In the following, we will describe a simple example of a safety-instrumented system (SIS). Also, we will deal with possible configurations of the valve and mounted valve accessories used in the safety-instrumented system. Finally, we will discuss state-of-the-art test methods. We will look at the following aspects:

- Possible test procedures
- Integration into the higher-level process control system
- Effects on safety assessment

4 Requirements stipulated in VDI 2180

In Part 5 of VDI 2180, practical recommendations are given for engineering, implementation and operation of safety-instrumented systems.
The main claim is that safety installations must be robust against failures. As a result, measures need to be taken:

- Against systematic failures
- Against random failures
- To improve fault tolerance

In section 3.1 of VDI 2180, Part 5, it is demanded that all three measures always be taken for each safety-instrumented system. It is recommended to use **instruments proven-in-use** (refer to NAMUR Recommendation NE 130), in particular to ensure that the instrument is suitable for the selected industrial process. Recurrent functional tests are to be performed, documenting the test results. Performing and documenting these functional tests can be automated. The proof test to demonstrate that the safety-instrumented system itself is free of faults is performed while the plant is shut down. In addition, tests can be performed while the process is running (**online tests**). Diagnostic coverage (DC) is specific to the selected method and instruments used. Furthermore, the safety-instrumented system can be assessed based on **spurious trips**.

5 Terms, definitions, and abbreviations

Also see SAMSON manual WA 236
The following terms and abbreviations are used in addition:

Term	Abbreviation
Basic process control system	BPCS
Diagnostic coverage	DC
Probability of failure on demand	PFD
Safety integrity level	SIL
Safety programmable logic controller	Safety PLC
Safety-instrumented system	SIS

6 The complete safety-instrumented system

We will use a simple example to explain what a safety-instrumented system refers to (Fig. 1). In our example, the temperature of a reactor is controlled using a heat exchanger. The associated control loop is illustrated by the temperature sensing point T_{10} connected to the control system (BPCS) and by control valve V_1, which regulates the flow rate of the heat exchanger. The safety-instrumented system is completely separated from the control loop with its own sensor (T20), safety PLC, and control valve V_2. This circuit monitors the temperature and closes valve V_2 to shut off the supply to the heat exchanger when the adjusted limit is exceeded. The circuit does not become active, i.e. valve V_2 is not actuated, while the plant operates within the permissible limits. Based on the risk analysis, a clear goal must be set for the safety-instrumented system. This goal could be, for example: when temperature T1 is reached, valve V_2 is to be closed within five seconds with a maximum seat leakage rate of 2 %. Usually, it is necessary to specify the closing time and seat leakage rate required to achieve the safety goal. Further specifications can be added as needed.

The safety-instrumented system is to be assessed concerning its probability of failure on demand (PFD). The PFD goal to be achieved is specified in the risk analysis. In process engineering, circuits and instruments are commonly rated according to SIL 2 (Safety Integrity Level), a minority also according to SIL 3. In accordance with VDI 2180, it is to be proven in three steps that an instrument is suitable for the intended purpose:

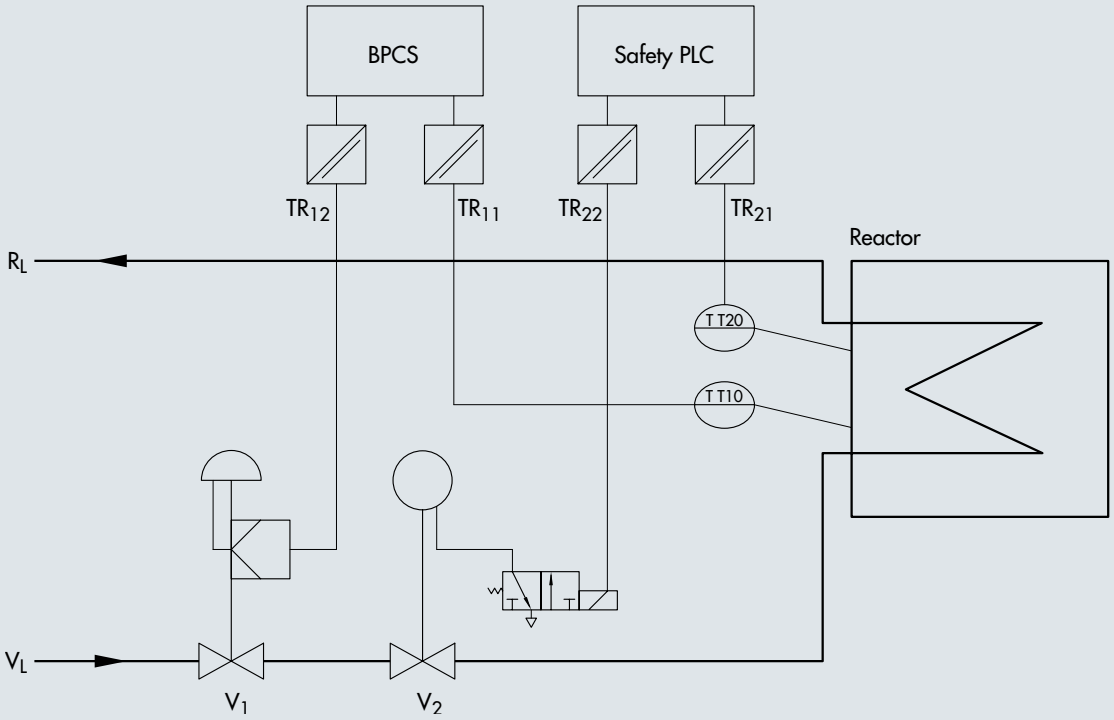

Fig. 1 · Example of a safety-instrumented system

1. Rule out systematic failures by performing a risk analysis according to VDI 2180 as well as the recommendations and notes, e.g. given in WA 236.
2. Determine the rate of random failures. To do so, determine the total dangerous undetected failure rate per hour λ_{du}. After setting a test interval, calculate the PFD_{avg} as shown in formula (1). Compare the calculated PFD_{avg} to the goal set by the plant operator in the risk analysis.

   - Formula (1): $PFD_{avg} = ½ \cdot \lambda_{du} \cdot T_{PR}$

PFD_{avg}	Average probability of failure on demand
λ_{du}	Dangerous undetected failure rate
T_{PR}	Proof test interval

3. Determine the degree of redundancy, which is specified as the hardware fault tolerance (HFT).

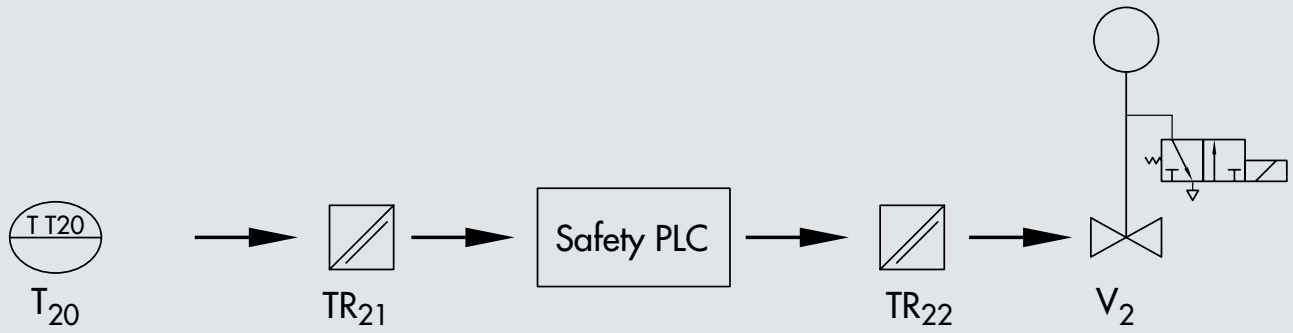

Fig. 2 · Structure of the safety-instrumented system

T_{20}	TR_{21}	Safety PLC	TR_{22}	V_2	Σ
237 FIT	77 FIT	45 FIT	77 FIT	103 FIT	539 FIT

Fig. 2 illustrates how the assessment is done: To calculate the PFD_{avg}, start by determining the failure rate of the entire circuit. In a single-channel setup, this is done by adding up the failure rates of the individual instruments in the circuit, either based on the manufacturer specifications or the values gathered from prior use in the operator's plant. Check the values' applicability to the intended process. In our example, we use the unit FIT (Failure in Time) = $1 \cdot 10^{-9}$/h. The total failure rate in our example is 539 FIT; i.e. λ_{du} equals $5.4 \cdot 10^{-7}$/h. The PFD_{avg} can be calculated according to Formula (1) based on a test interval.

T_{PR}	6 months	12 months	24 months
PFD_{avg}	$1.2 \cdot 10^{-3}$	$2.4 \cdot 10^{-3}$	$4.7 \cdot 10^{-3}$

The results indicate that the PFD_{avg} in our example still complies with the requirements for SIL 2, even with a test interval of two years. Checking the HFT is simple: as single-channel components are used, the hardware fault tolerance is 0. This is still permissible for SIL 2 applications, provided proven-in-use instruments are used.

VDI 2180, Part 4 provides practical examples and approximate formulae for calculations of more complex structures.

7 Instrumented valves

In our example, the control valve with all its accessories as, so far, viewed as a single block. Fully instrumented control valves are often referred to as "final elements". In the next analytical step, we need to look at the individual instruments forming a *final element*.
Four typical configurations will be discussed:

1. **Valve with pneumatic actuator controlled by a solenoid valve:** The valve may be a ball or globe valve, the pneumatic actuator may be a rotary (usually piston) or linear (usually diaphragm) actuator. The actuator is controlled by a solenoid valve. In most cases, the supply air is routed through a supply pressure regulator. Take measures to rule out systematic failures according to VDI 2180 and WA 236. Determine the rate of random failures as described in our example by adding up the corresponding values for the valve, actuator and solenoid valve.

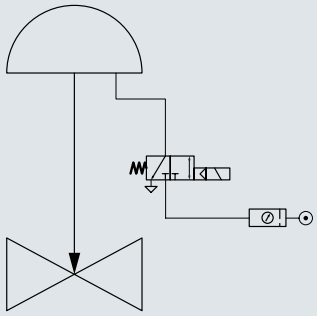

Fig. 3 · Hook-up 1

- Formula (2): $PFD_{Total} = PFD_{Valve} + PFD_{Actuator} + PFD_{Solenoid\ valve}$

As the supply pressure regulator acts in the pneumatic circuit, check whether it may contribute to a failure (unintentionally fill the actuator with air). This could only happen if the solenoid valve could no longer move to the switching position to vent the actuator because the supply air is applied directly. Another dangerous fault could arise, for example because the pressure drop across a micro-flow valve is too high, causing the seat leakage rate to increase. In general, it can be said that failures caused by the supply pressure regulator can be ruled out. Frequently, limit switches are used. However, they only need to be considered in the risk analysis if several control valves need to be moved to their fail-safe positions in series.

2. Valve, actuator, solenoid valve, and positioner:
If positioners are also used for emergency shutdown, the hook-up is as shown in Fig. 4. Alternatively, such a configuration can be used on on/off valves to perform online tests while the process is running. An important online test is the partial stroke test (PST). To determine the safety properties, assess the instruments required for emergency shutdown. In our example, these are the valve, actuator and solenoid valve. The function of the positioner is important for the availability of the configuration in the plant but does not play any role in emergency shutdown. Perform the assessment as described in example 1.

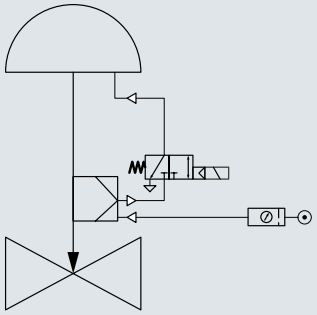

Fig. 4 · Hook-up 2

3. Valve, actuator, solenoid valve, positioner, and booster:
A booster may be needed to achieve certain settling and closing times. Fig. 5 shows a sample configuration. In the example, the booster is mounted between the solenoid valve and actuator. This is necessary if the solenoid valve's air capacity is not sufficient to achieve the required closing time. In this configuration, the booster is part of the safety-instrumented system. As a result, it needs to be assessed concerning systematic and random failures in addition to the instruments mentioned in example 1.

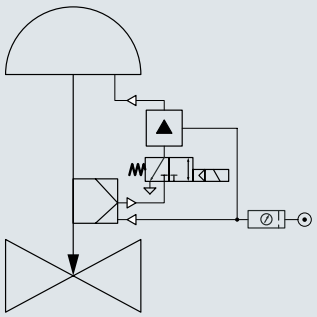

Fig. 5 · Hook-up 3

4. Valve, actuator, and positioner: A simple, yet state-of-the-art configuration is shown in Fig. 6. In the example, a positioner instead of a solenoid valve is used for emergency shutdown. This is possible with positioners, such as SAMSON's TROVIS SAFE 3730-6 or TROVIS SAFE 3731-3, whose emergency shutdown is proven by a manufacturer declaration or certification by an independent expert body. In these positioners, shutdown is performed at a signal of 3.8 mA. In the configuration, the positioner can also be used

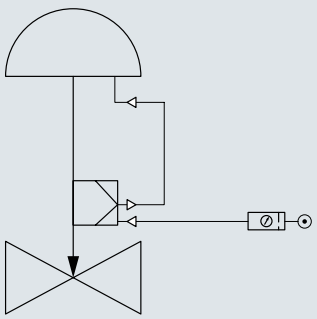

Fig. 6 · Hook-up 4

for diagnostics and testing, such as PST. The shutdown threshold at 3.8 mA and, at the same time, maintaining a current of more than 3.6 mA brings the added benefit that the valve's travel through its full range to the end position can be traced, recorded, and analyzed for diagnostic purposes. As a result, the proof test or spurious trips can be documented and assessed.

8 SAMSON products for safety-instrumented systems

Based on the risk analysis, plant operators determine the requirements placed on safety-instrumented systems. In principle, operators can choose any component from the wide range of valves and accessories available. By establishing prior use and checking the associated documentation, operators can determine whether the selected components are suitable for use in safety-instrumented systems. It is usual, however, to install instruments that come with specifications of safety-related data and a manufacturer declaration stipulating their suitability for use in safety-instrumented systems. Regardless of this, it is the plant operators who are responsible for ensuring component suitability for their specific process according to VDI 2180.

SAMSON devices with manufacturer declaration or certification by an independent expert body are:

Ball valves	SAMSON PFEIFFER	Series 1a, 1b, 20a, 20b, 26d, 26s
Butterfly valves	SAMSON PFEIFFER	Series 4b, 4c
Rotary actuators	SAMSON PFEIFFER	Series 31a
Globe valves	SAMSON	Types 3241, 3251
Linear actuators	SAMSON	Types 3277, 3271
Butterfly valves	SAMSON LEUSCH	Type LTR 43
Control valves	SAMSON VETEC	Types 62, 72, 73, 82, 93
Solenoid valves	SAMSON SAMSOMATIC	Types 3963, 3967
Positioners	SAMSON	Series 3730
Limit switches	SAMSON SAMSON SAMSOMATIC	Types 3738, 4746 Types 3776, 4747
Volume booster	SAMSON	Type 3755

For manufacturer declarations and safety-related data of these instruments as well as notes on using them in safety-instrumented systems refer to the SAMSON documents WA 236 and TV-SK 9838-5.

SAMSON product range (Fig. 7)

9 Automated testing

9.1 Final element

Final elements are valves equipped with various instruments that automate them, such as solenoid valves, boosters, and other valve accessories. We will discuss some possible setups in the following:

1. Fig. 8 shows a classic setup consisting of ball valve, rotary actuator, solenoid valve, and limit switch. For details refer to the schematic drawing.

2. Fig. 9 shows an advanced state-of-the-art setup. The functions of the limit switch and solenoid valve are implemented by a single unit. The schematic drawing shows that the functions provided to the operator are identical to those in the classic setup. Additionally, however, the control valve includes a TROVIS SAFE 3730-6 or TROVIS SAFE 3731-3 Positioner, which can be used for valve diagnostics. The special benefit in this is that all components are integrated into one housing. All moving parts required for attachment to the actuator are enclosed. Apart from diagnostics, this setup with reduced interfaces and mounting parts makes for a particularly rugged and inherently safe assembly. The following signals are used to control it:

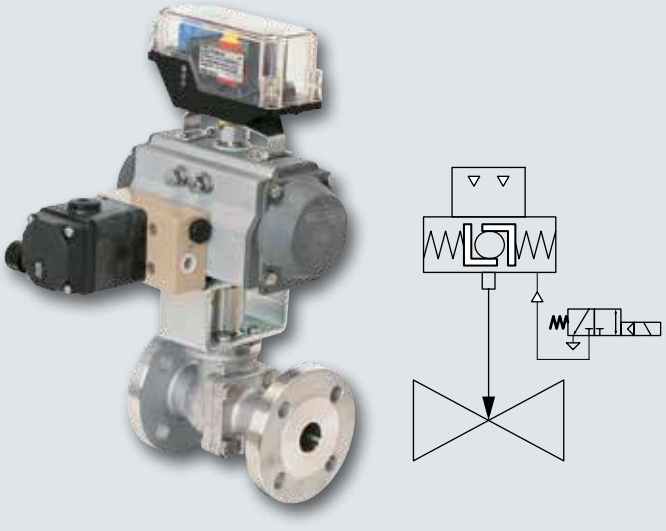

Fig. 8 · Automated ball valve

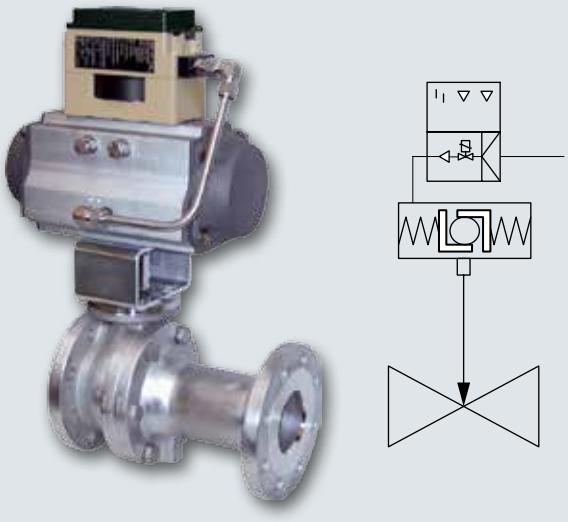

Fig. 9 · Ball valve with positioner

- 24 V for the solenoid valve
- NAMUR signal (EN 60947-5-6) for the limit switches and an alarm signal
- 4 to 20 mA for the control signal of the positioner

3. Fig. 10 also shows an advanced state-of-the-art setup. The rotary actuator is automated using a smart Type 3738-20 Electronic Limit Switch. The following control signals are used:

   - 24 V for the solenoid valve
   - Two NAMUR signals (EN 60947-5-6) for the limit switches
   - One NAMUR signal (EN 60947-5-6) for the partial stroke test (optional)
   - One NAMUR signal (EN 60947-5-6) for an alarm signal (optional)

   With this setup, the classic wiring used in the field can be maintained. By default, the Type 3738-20 Electronic Limit Switch combines all the listed signaling options in one housing, using the additional signal is optional, however. In the setup shown, the limit switch is integrally attached, meaning that the air between the limit switch and the rotary actuator is routed directly. No external piping is required, which makes the attachment particularly rugged and cost effective.

   A version of the electronic limit switch for use with FOUNDATION™ fieldbus communication is available (Type 3738-50).

Fig. 10 · Type 3738-20 Electronic Limit Switch

9.2 Test methods

The setups described above in items 2 and 3 permit automated online tests to be performed according to VDI 2180, Part 5, section 4.6. The following parts can be automated or supported by automated units:

- Test procedure
- Data logging
- Data archiving

The setup ensures reproducible and consistent testing. This method is superior to manual testing and manual data recording merely based on quality. The excellent measuring accuracy of the listed devices improves the scope of testing and the diagnostic coverage as a result.

9.2.1 Online testing: partial stroke test

During partial stroke testing, the valve's closure member is moved while the process is running. A typical test value would be to move the closure member by 10 % of the travel range, but other values are possible depending on the process requirements. When a positioner is used, the test can be performed as a step or ramp test. Fig. 11 shows sample test results achieved with a positioner (TROVIS SAFE 3730-6). The positioner mounted on the valve performs the test and records and saves the test results; an online connection to the process control system is not required. The saved diagnostic data can be read at any time by the higher-level asset management system. The condition of the control valve can be analyzed based on:

Diagnostic data recorded during the partial stroke test, such as:

- End position achieved by the valve
- Travel vs time diagram
- Pressure vs pressure diagram
- Dead time
- Transit time
- Assessment of the valve movement (evenly, abruptly with slip-stick effect). Refer to Fig. 12.
- Breakaway force
- Force required to reach the end position

Constantly recorded process data:

- Number of operating hours
- Operating temperature
- Operating temperature exceeded
- Cycle counter
- Total valve travel counter

For a detailed description of the functions refer to Operating Instructions EB 8389-1S.

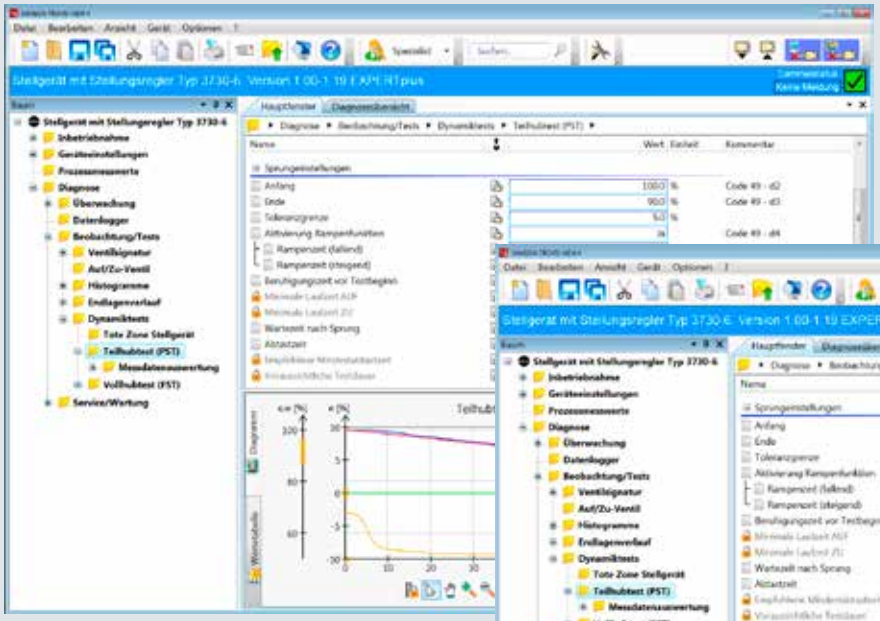

Fig. 11 · Partial stroke test

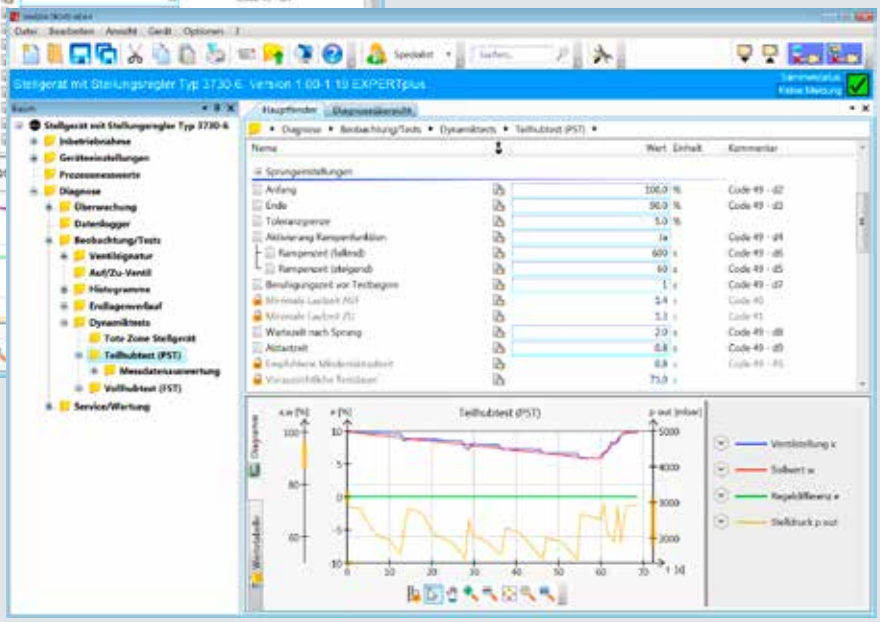

Fig. 12 · Detecting increased friction

As a result, the requirement stipulated in VDI 2180, Part 5 to record the following variables is more than fulfilled:

- Dead time
- Transit time
- Actuating force
- Travel vs. time diagram

Fig. 12 shows impressively how increased friction values, for example, become evident in the diagnostic data recorded during a partial stroke test. The dead time, control performance, and course of the actuator pressure have changed significantly. In the example, the valve still functions and could be shut down on demand. An internal damage about to occur, e.g. due to increased friction, could thus be detected in advance.

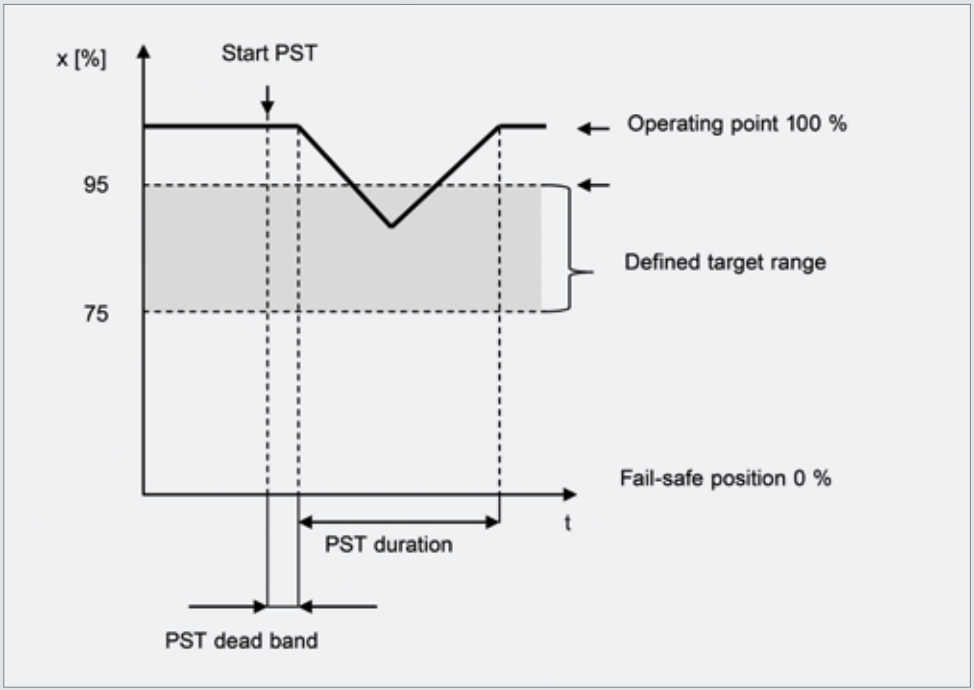

Fig. 13 · Advanced partial stroke test using Type 3738 Electronic Limit Switch

Fig. 13 shows an advanced partial stroke test performed by a Type 3738-20 Electronic Limit Switch. In this case, the solenoid valve is pulsed to achieve a certain target range for valve movement. The necessary pulse length is determined during an automatic configuration routine. The same solenoid valve is used for testing and emergency shutdown on demand, making special pneumatics redundant (EB 8390). This results in high diagnostic coverage, which is a special benefit.

9.2.2 Further test options

According to VDI 2180, Part 5, the diagnostic functions of smart field units can also be used to:

- Automate and document the proof test
- Automate recording of spurious trips

Diagnostics are as described in section 9.2.1. Recording spurious trips is particularly interesting. The Series 3730 and 3731 Positioners, for example, can use their internal data logger and trigger options to record valve movements. The created record is time-tagged and saved in a non-volatile memory. It can be used to retrospectively assess the functioning of the control valve and safety-instrumented system.

9.3 Integration into the process control system

9.3.1 Architecture

To successfully use the described automated tests, their integration into the process, specifically into the safety life cycle, is essential. By connecting the final element to the safety PLC, it must ensure proper functioning on demand. It must be integrated into the asset management system to ensure that testing, data recording and archiving are possible. We will give a short explanation of three proposed architectures:

Fig. 14 shows a possibility of connecting the control valve to the process control system according to Fig. 9 and to the safety PLC. The solenoid valve used to shut down the control valve on demand is energized by a 24 V signal by the safety PLC. The additionally installed positioner provides the described test options. The positioner is controlled by the process control system. For example, the HART® protocol or a fieldbus protocol can be used to configure the positioner, start the tests and read the recorded diagnostic data. This setup implements the state of the art described in VDI 2180, Part 5. However, it has the disadvantage of not including the solenoid valve in the performed tests, which may lead to possible solenoid valve failures not being detected.

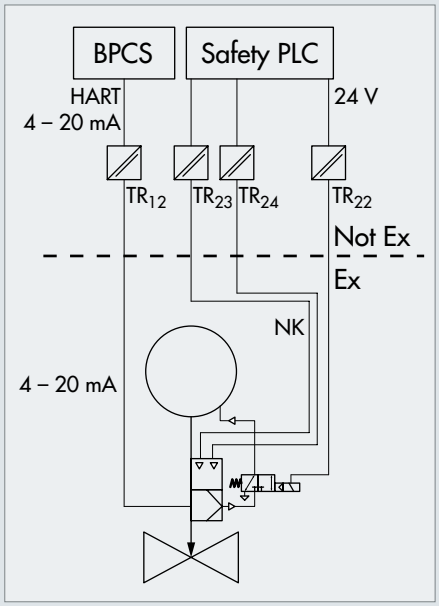

Fig. 14 · ESD configuration 1

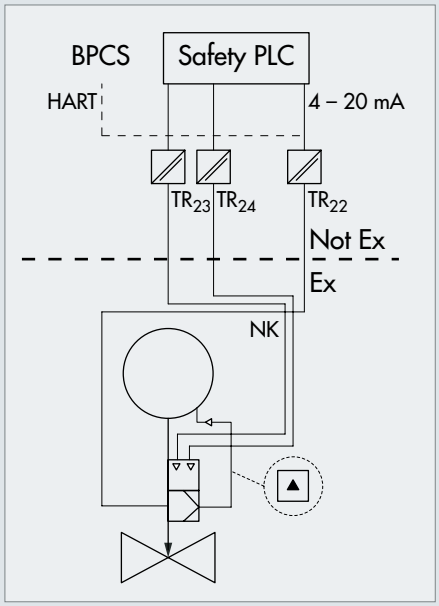

Fig. 15 · ESD configuration 2

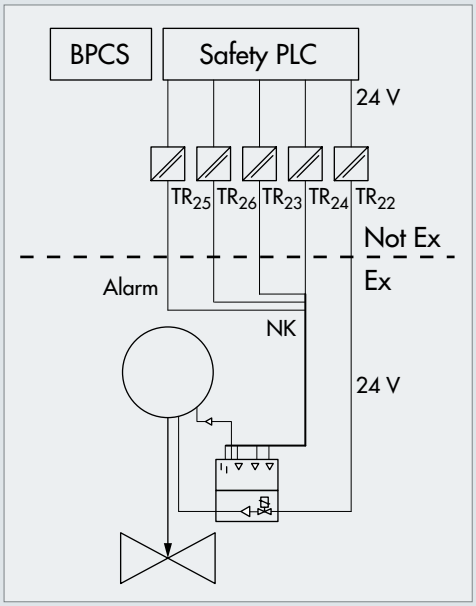

Fig. 16 · ESD, Type 3738-20 Electronic Limit Switch

Fig. 15 shows a different way of connection with far-reaching consequences: the Series 3730 Positioner is not only used for testing, it is also in charge of emergency shutdown. The positioner's pneumatic output is connected directly to the actuator. If the positioner's air output is insufficient for large valves, a Type 3755 Booster can be inserted. The positioner is controlled by a 4 to 20 mA signal. The valve is moved to its end position by a 3.8 mA signal. Concerning the two criteria for emergency shutdown, i.e.

- Safe detection of the 3.8 mA signal and control of the internal pneumatics
- Safe functioning of the internal pneumatics

The positioner is certified by an independent expert body (TÜV Rheinland®). Certified output boards with a 4 to 20 mA signal are available for safety-instrumented systems. The same applies to the required Ex barriers, in this case 4 to 20 mA current-current converters. As a result, the entire circuit can be equipped with instruments available on the market.

The described connection tests the entire pneumatic path, ensuring a high diagnostic coverage. The following criteria are complied with:

- Online test of the mounted valve
- Online test of the pneumatic path
- Digital communication for parameter setting, testing and transmitting diagnostic data
- Detection of spurious trips
- Proof testing
- Control in the end positions

The last item in the above list refers to a particularly progressive way of operating a safety valve. In this case, the valve is not held in the fail-safe end position (e.g. OPEN position) by excessive air or force but it is opened to approx. 98 %, for example. This increases reliability as the valve cannot get stuck in the end position and further diagnostic functions saved in the positioner can be performed.

Fig. 16 shows a connection employing the smart Type 3738-20 Electronic Limit Switch. Connection to the process control system is established using the common wiring, which is a special benefit when upgrading older systems. In this case, alarms are indicated by a NAMUR contact.

9.3.2 Documentation of partial stroke testing

If the test results are to be used, e.g. to achieve a longer test interval, performance of the partial stroke test must be documented. To do so, a setup as shown in Fig. 16 (schematic drawing in Fig. 17) can be used. The limit switch of the Type 3730-x Positioner or the third travel contact of the Type 3738-20 Electronic Limit Switch are set to the desired valve movement target. In the positioner, this can be done using the mechanical travel stop option, which is a certified component. In the limit switch, the function of the NAMUR signal safely indicating the adjusted switching points has been certified by an independent expert body. The limit switch signal is recorded by the safety PLC, time-tagged and archived.

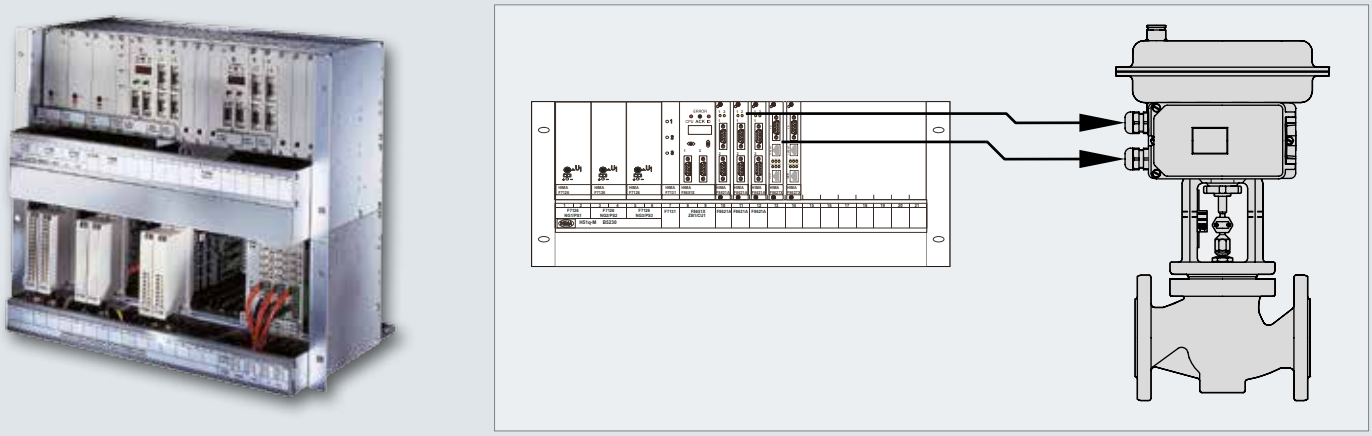

Fig. 17 · PST registration by safety PLC (photo by HIMA)

9.3.3 Continuous workflow

A full test cycle can be divided into the following steps:

- Test is triggered
- Test is performed (valve moved to target position)
- Data are logged
- Data are saved
- Data are assessed
- Alarms are generated
- Data are saved to a tamper-proof archive
- Trends are generated based on several test cycles

Workflow								
Trigger	Perform	Record online	Record online	Store	Evaluate	Alarm	Archive	Trending
Positioner online connection								
Manual/ automatic	Ramp/step response	Parameters, travel/time		Parameter diagram	Positioner information	Generate alarm		
DCS system								
Manual/ automatic		Register event by limit switch	Record transmitted data	Parameter diagram	Instrument conditions	Generate alarm	Store in database	Compare results

Fig. 18 · Workflow of a partial stroke test

The strength of the Series 3730 Positioners is their wide range of diagnostic functions. The listed steps can also be performed individually by the positioner. As part of the entire safety life cycle, an integration into a consistent asset management scheme makes sense. Refer to Fig. 18 for a proposal. A software tool, such as TROVIS SOLUTION, can assist in archiving single data records and in trending over several single measurements. They allow recommended action to be made for predictive maintenance.

At SAMSON's Smart Valve Integration Center (SVIC), integration into different control systems is tested. For details, refer to the SAMSON publication WA 232 Expertise in Device Integration. Fig. 19 shows integration of a positioner into Yokogawa's Centum system. Fig 20 shows integration of the positioner diagnostics (e.g. partial stroke testing) into the Yokogawa PRM system and Fig. 21 into Emerson's AMS system. The PST Scheduler developed by Yokogawa is particularly interesting (Fig. 22). This tool allows online tests to be configured and monitored at the positioner.

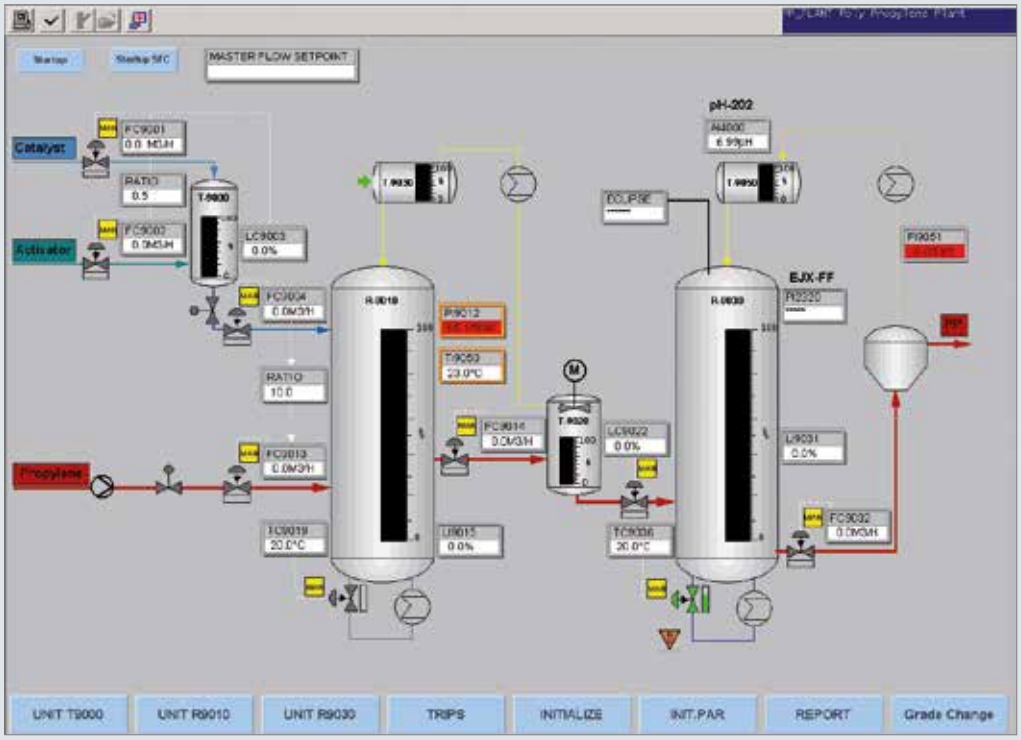

Fig. 19
Yokogawa Centum control system

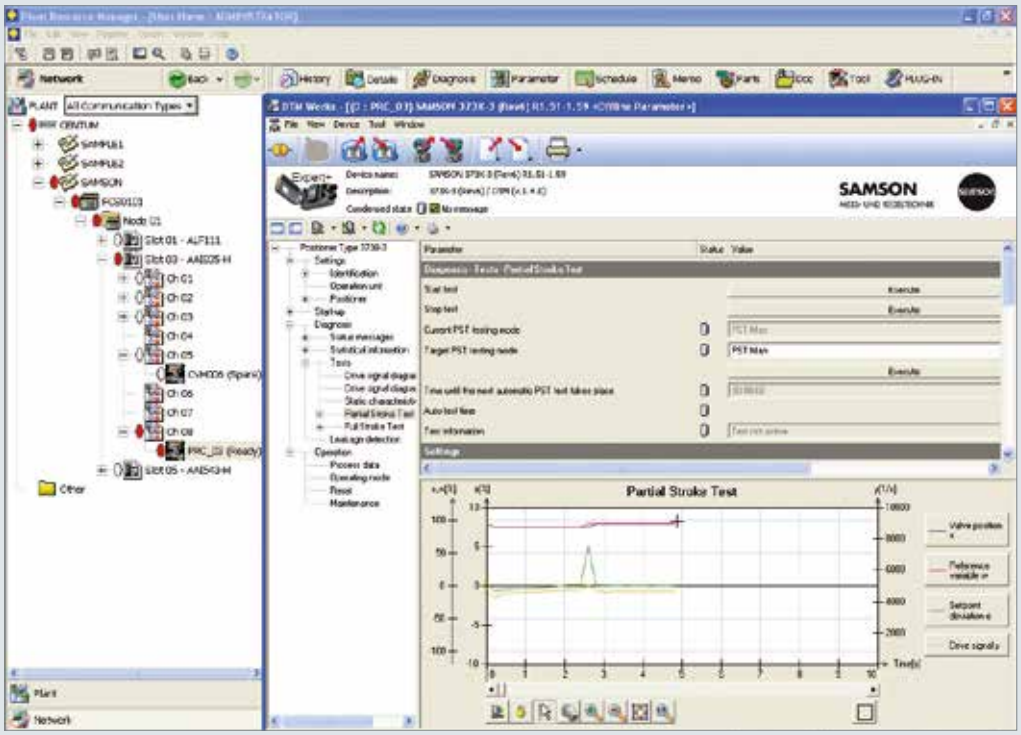

Fig. 20
Integration into Yokogawa PRM

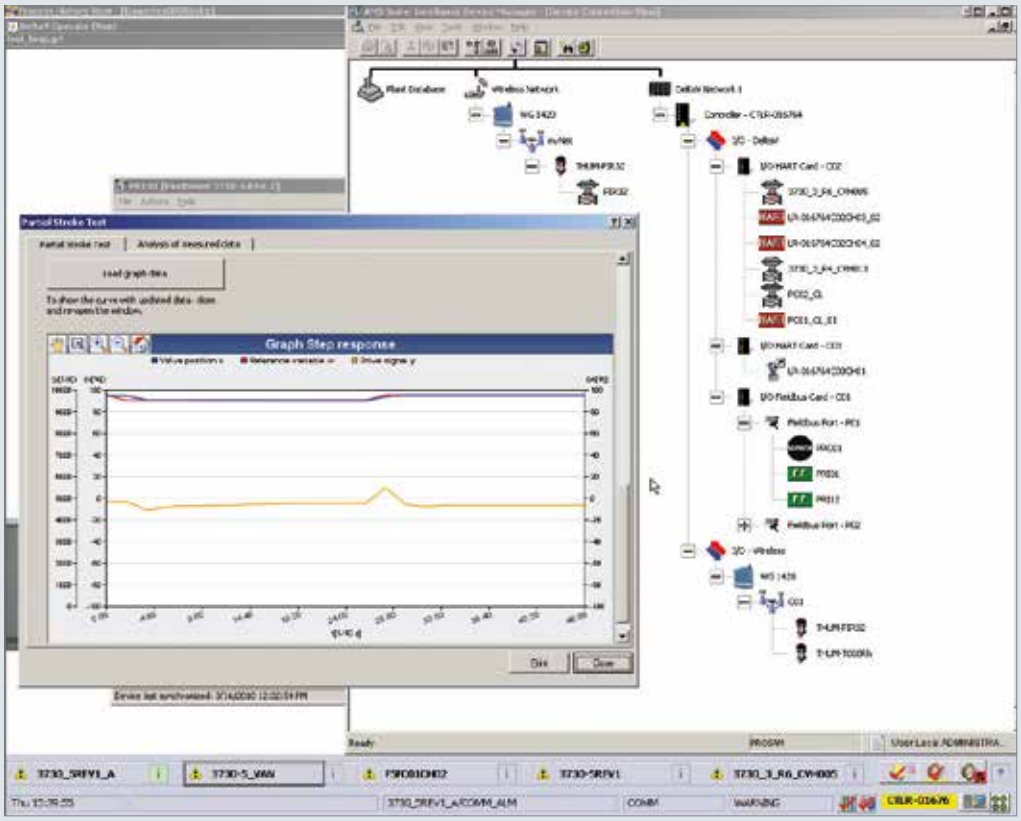

Fig. 21
Integration into Emerson AMS

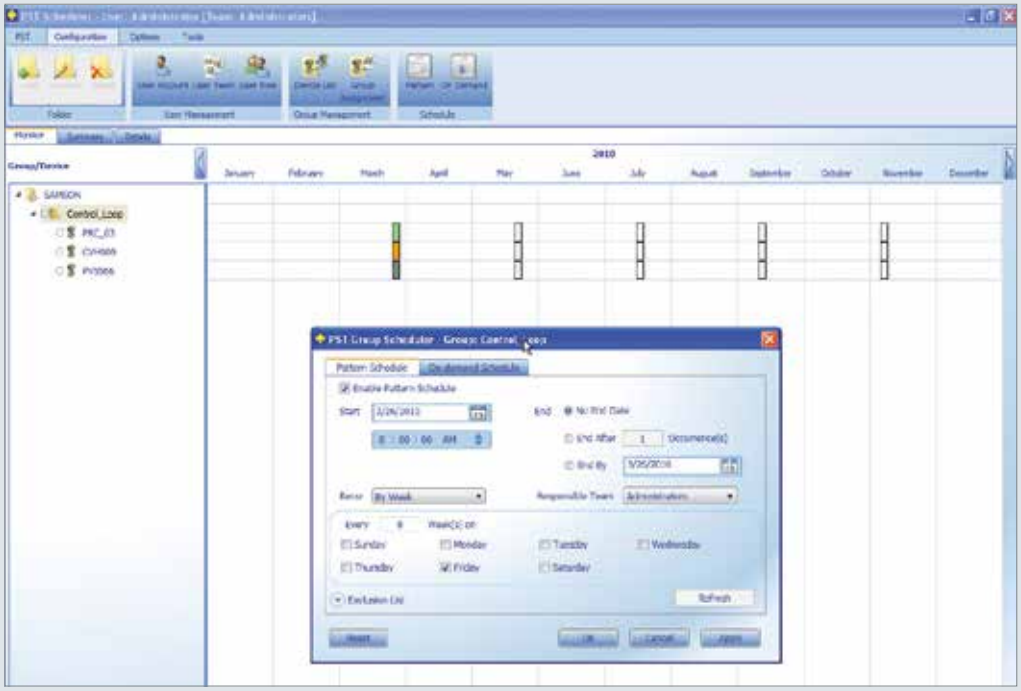

Fig. 22
Yokogawa PST Scheduler

9.4 Effects on safety assessment

9.4.1 Systematic failures

Rule out systematic failures by risk analysis and taking appropriate measures. Particularly in new processes or with test intervals exceeding the standard, it may make sense to take special measures to reveal undetected systematic failures. According to VDI 2180, Part 5, section 4.6, automated online tests can additionally protect the system against undetected systematic faults.

9.4.2 Random failures

Online tests can reveal failures. If operators ensure that detected failures are handled according to a specific scheme by repair or plant shutdown, the number of dangerous undetected failures is reduced. As a result, the PFD_{avg} value improves.

For a quantitative analysis, start by determining the diagnostic coverage. Diagnostic coverage indicates the share of total failures detectable by a test procedure. It is obvious that partial stroke testing can detect the valve being stuck in an end position, yet a fault in the valve's seat cannot be detected. Tests show that a lack of torque reserve is the main cause of failure, e.g. of ball valves, in safety-instrumented systems. As a result, high diagnostic coverage can be assumed. Diagnostic coverage depends on the failures occurring in the specific process and the diagnostics possible. Therefore, it is proposed in VDI 2180, Part 5, Table 2, to determine diagnostic coverage by performing an FMEA (Failure Mode and Effects Analysis), which is based on the diagnostics possible in the specific plant (Table 1). In doing so, a diagnostic coverage value can be determined. Mere manufacturer specifications unrelated to a specific process, sometimes giving up to three significant figures, are not considered trustworthy.

Failure	Possible cause of failure	Failure detectable? Partial stroke test	Failure detectable? Full stroke test	Failure detection
Solenoid valve does not switch	Solenoid valve not energized properly	Detectable	Detectable	Position feedback
Solenoid valve does not switch	Solenoid valve defective	Detectable	Detectable	Position feedback
Control valve reacts too slowly	Reduced cross-section of the air line to the valve	Detectable	Detectable	Monitoring the time until position has been fed back
Control valve reacts too slowly	Control valve response too slow	Detectable	Detectable	Monitoring the time until position has been fed back
Valve does not shut off (completely)	Valve seat and plug worn out	Not detectable	Detectable	PST not possible
Valve does not shut off (completely)	Deposits on the valve seat	Not detectable	Detectable	PST not possible
Valve does not shut off	Plug stem blocked	Detectable	Detectable	Position feedback

Table 1 · Failures and detectability

If diagnostic coverage has been determined, the improved PFD_{avg} value can be calculated according to formula (3):

- Formula (3): $PFD_{avg} = ½ \lambda_{du} \cdot DC \cdot T_{PST} + ½ \lambda_{du} \cdot (1 - DC) \cdot T_{PR}$

PFD_{avg}	Average probability of failure on demand
λ_{du}	Total dangerous undetected failure rate (1/h)
DC	Diagnostic coverage
T_{PST}	PST interval
T_{PR}	Proof test interval

Failures undetected during the partial stroke test need to be taken into account when calculating the PFD_{avg} value, while the effects of detectable failures can be omitted. To do so, the PST interval should be considerably longer than that of the proof test, e.g. ten to twenty times longer. Fig. 23 shows a comparison of the achieved PFD_{avg} values for a specific safety-instrumented system. The figures are selected such that the safety-instrumented system in the example needs to be proof-tested after one year to achieve SIL 2. Diagnostic coverage is assumed to be 0.6 (60 %), a typical value more on the conservative side. With this value, the (proof) test interval can be extended to two years by performing monthly partial stroke tests. This result is plausible as eliminating more than half of the dangerous undetected failures results in roughly doubling the test interval.

The following figures are taken as an example:

- $\lambda_{du} = 1.14 \cdot 10^{-6}/h$
- T_{PR} = 1 year (8760 hours)

Based on formula (1), the calculated PFD_{avg} value equals $5 \cdot 10^{-3}$. This corresponds to half the safety-related availability demanded for SIL 2. As a result, the circuit with its PFD_{avg} can be used as SIL 2; the same value remains for the other components in the circuit. The safety-instrumented system is to be subjected to a partial stroke test. The following values are assumed:

- DC = 0.6
- T_{PST} = 1 month
- T_{PR} = 2 years

Based on these figures, the PFD_{avg} calculated according to formula (3) equals $4.2 \cdot 10^{-3}$. As a result, the system can also be classified as SIL 2 with roughly the same PFD_{avg} value but a proof test interval extended to two years.

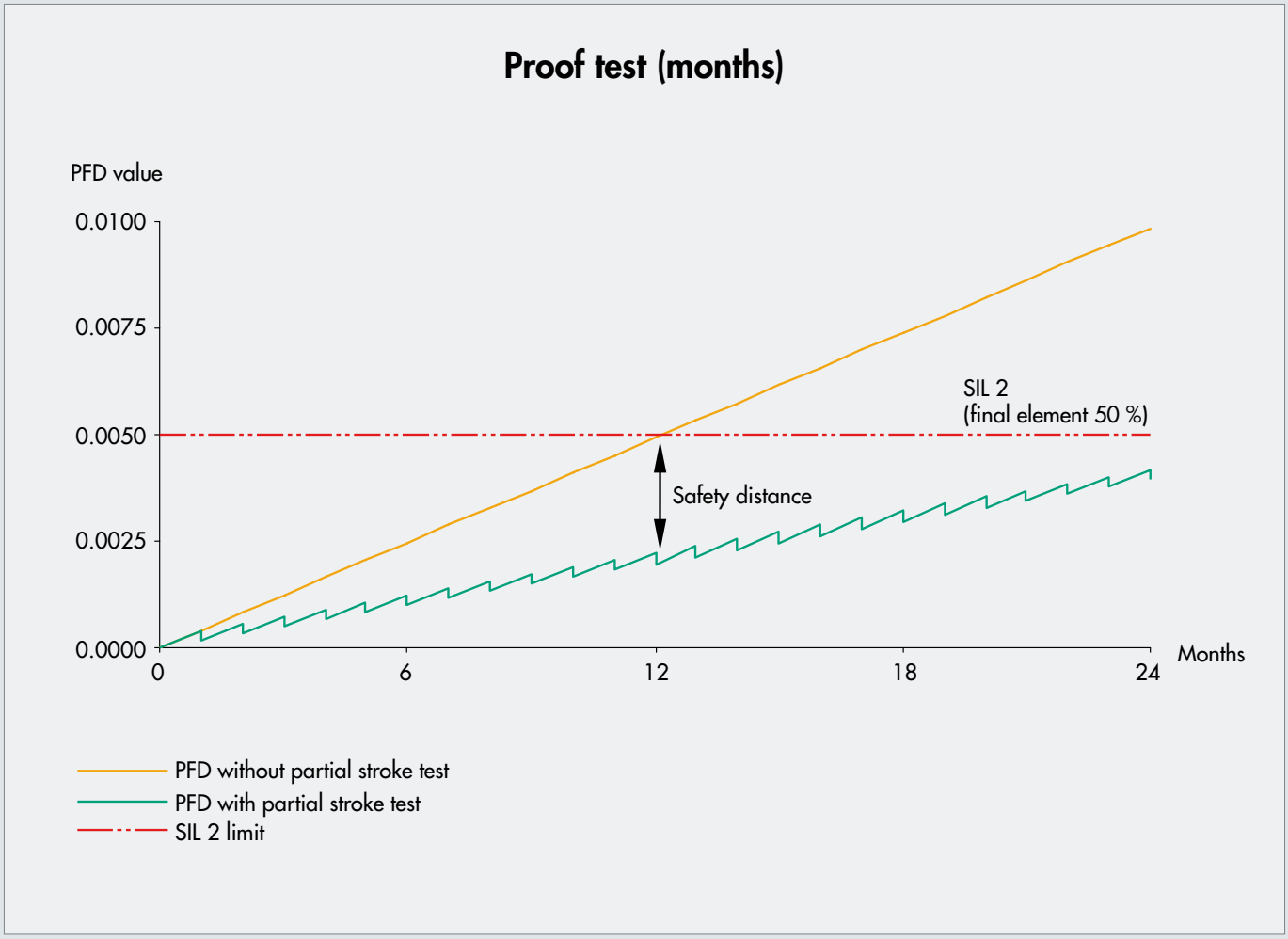

Fig. 23 · PFD_{avg} value with partial stroke test

9.4.3 Measures related to fault tolerance

IEC 61511 and VDI 2180 set a strict limit: single-channel instrumentation is only permissible up to SIL 2 and only if proven-in-use instruments are used. A safety-instrumented system complying with SIL 3 requires redundancy, i.e. two control valves. This requirement is not affected by online testing.

10 Life cycle

In the previous sections, we discussed the automation of control valves used in safety-instrumented systems. We made a conscious decision of keeping the discussion short to provide an overview of the topic. The safety life cycle is the key to cost-efficient operation, high plant availability and a high level of safety. In many phases of this life cycle, state-of-the art instrumentation can provide effective support (Fig. 24).

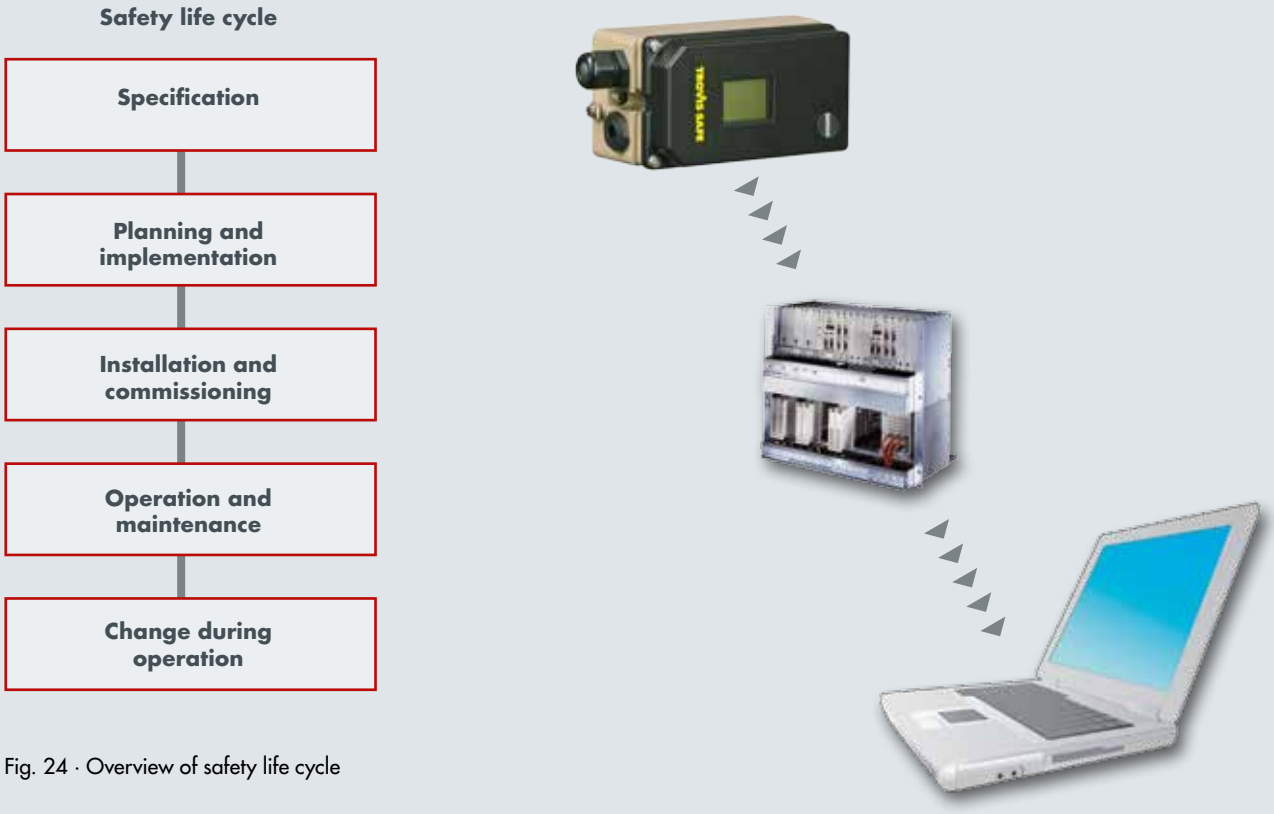

Fig. 24 · Overview of safety life cycle

11 Bibliography

- IEC 61511
- VDI 2180, Part 5
- NAMUR Recommendation NE 130
- Competence in Functional Safety –
  Functional safety of globe valves, rotary plug valves, ball valves and butterfly valves,
  SAMSON AG, WA 236
- Expertise in Device Integration –
  SMART VALVE INTEGRATION CENTER,
  SAMSON AG, WA 232
- Documentation for the Use of Type 373x-x Positioners in Safety-instrumented Systems,
  SAMSON AG, TV-SK 9838-5
- Type 3738-20 Electronic Limit Switch,
  SAMSON AG, EB 8390
- Series 3730 – Type 3730-3 Electropneumatic Positioner, firmware version 1.5x,
  SAMSON AG, EB 8384-3
- Series 3730 and 3731 – Types 3730-2, 3730-3, 3730-4, 3730-5
  and Type 3731-3 Electropneumatic Positioners – EXPERTplus Valve Diagnostics,
  SAMSON AG, T 8389
- Series 3730 and 3731 – Types 3730-2, 3730-3, 3730-4, 3730-5
  and Type 3731-3 Electropneumatic Positioners – EXPERTplus Valve Diagnostics,
  SAMSON AG, EB 8389
- TROVIS SOLUTION,
  SAMSON AG, WA 290
- Götz, Hildebrandt, Karte, Schäfer, Ströbl:
  Implementation of Safety-instrumented Systems in the Process Industry –
  SIL in Practice, special print by SAMSON AG of article
  "Realisierung von Schutzeinrichtungen in der Prozessindustrie – SIL in der Praxis",
  atp 8/2008
- T. Karte, J. Kiesbauer:
  Smart Valve Positioners and Their Use in Safety-instrumented Systems,
  Industrial Valves 2009

SAMSON

MANUAL

Competence in Functional Safety

● Production sites ● Subsidiaries

SAMSON AKTIENGESELLSCHAFT
Weismuellerstrasse 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

2017-06 · WA 239 EN