Innovative Control Technology

SAMSON

SPECIAL PRINT

Implementation of Safety-instrumented Systems in the Process Industry – SIL in Practice

By:
Arno Götz,
Endress+Hauser
GmbH + Co. KG

Andreas Hildebrandt,
Pepperl+Fuchs GmbH

Thomas Karte,
SAMSON AG

Bernd Schäfer,
HIMA Paul Hildebrandt,
GmbH + Co. KG

Johann Ströbl,
TÜV SÜD Industrie
Service GmbH

English translation of article published in
atp – Automatisierungstechnische Praxis
8/2008 · Edition 50
www.atp-online.de

SAMSON GROUP

Implementation of Safety-instrumented Systems in the Process Industry – SIL in Practice

Arno Götz (Endress+Hauser GmbH + Co. KG), Andreas Hildebrandt (Pepperl+Fuchs GmbH),
Thomas Karte (SAMSON AG), Bernd Schäfer (HIMA Paul Hildebrandt GmbH + Co. KG),
Johann Ströbl (TÜV SÜD Industrie Service GmbH)

The IEC 61508 and IEC 61511 standards have become widely accepted as the basis for handling safety-instrumented systems. In German-speaking countries, the VDI/VDE 2180 standard supplements these international standards. Users have become familiar with the basic terms, such as SIL, failure rate, safe failure fraction etc. However, many users are often uncertain when it comes to implementing these concepts in everyday operation.
The decisive point is to combine the required degree of operational plant safety with legally compliant documentation and practical solutions, while taking into account the economic aspects as well. It is assumed in this article that the demands placed on a SIF (safety-instrumented function) are based on a hazard and risk analysis. This article explains which points need to be observed when implementing safety equipment and includes tips on how to use the instruments in practice. Besides the technical aspects, integration into a higher level safety management system is dealt with.

Safety in the process industry/safety-instrumented systems/IEC 61511

1. Introduction

The scope, theoretical background and, not least, the terminology and phrasing of IEC 61511 continue to raise numerous questions whether they concern the understanding of correlations or rather relate to the cook book approach to simple implementation. Numerous publications go into depth on special issues. By way of contrast, this article describes a safety-instrumented system containing components from various manufacturers in unified terms. The objective is to highlight the central ideas of IEC 61511 and their practical implementation. In keeping with the nature of the matter, the findings cannot result in simple instructions. However, the classical engineering approach proves to be the crucial point of safety instrumentation.

2. Normative basis for risk reduction in process plants

The applicability of the standards already prompts many questions:

- Do the requirements have to be met on all accounts?
- Are the standards intended just as recommendations?
- What happens if the recommendations are not observed?

These are just a few examples taken from everyday practice.

In this case, the standards pyramid (Fig. 1) brings clarity. This pyramid illustrates a growing degree of freedom available for making decisions and the potential to move away from rigid legal regulations towards individual approaches to solutions, whereby the focus must always be on the safety objective to be achieved. However, it must be evident that the individual responsibility and liability grows as the chosen solution becomes

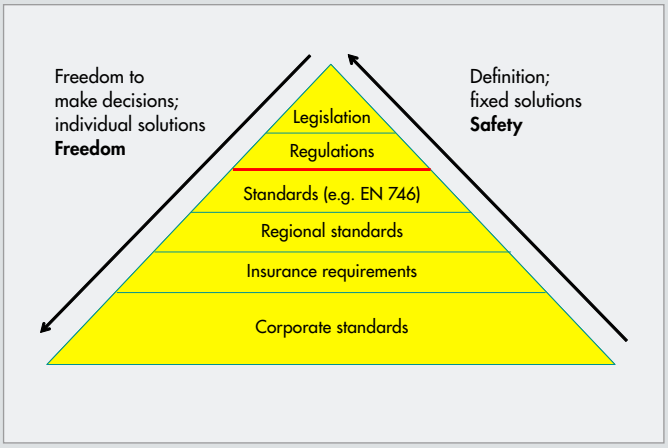

Fig. 1: Normative framework

more unique. In the event of failure and the question of accountability, the user must provide evidence concerning the observance of the recognized codes of practice. In the event of damage, the person responsible is personally liable. By implication, the approach towards clear guidelines provided by regulations and laws, and away from uncertainties regarding recognized codes of practice and their interpretation naturally offers safety and less personal responsibility for the operator. This, however, means the loss of flexible solutions.

Initially, it must first be clarified whether the plant concerned must comply with the standard, a relevant law or a regulation. Many chemical or petrochemical plants and process furnaces in Germany are subject to the German Hazardous Incident Ordinance.

In the Hazardous Incident Ordinance (12th BImSchV 2000), the following is mentioned concerning standards and regulations in Article 3 "General obligations of the operator":

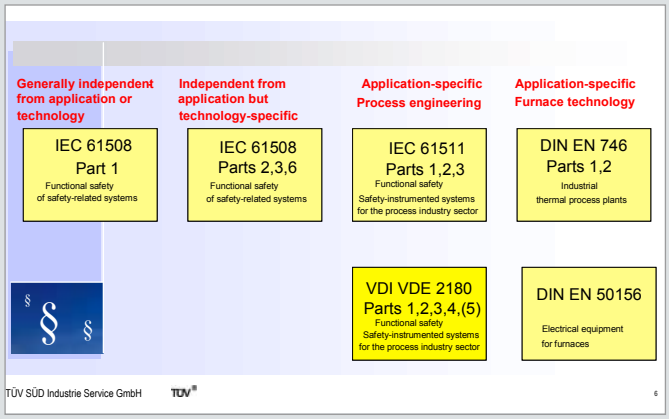

Fig. 2: Normative structure

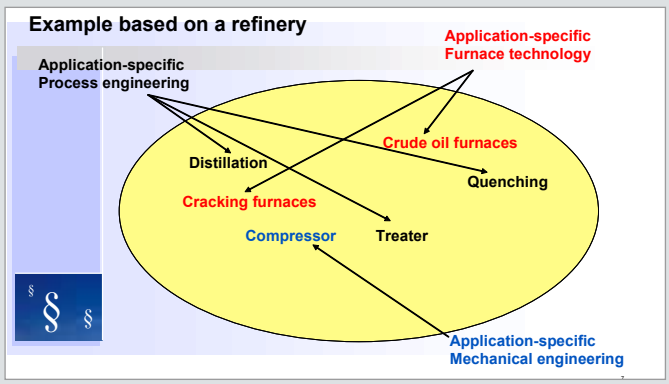

Fig. 3: Relation between application-specific standards

"(1)...
(2)...
(3)...
(4) The nature and operation of the installations in the establishment must be in keeping with the state of the art of safety technology."

That means the operator is obliged to keep the plant to the state of the art of safety technology. According to the Hazardous Incident Ordinance, the state of the art of safety technology means "the level of development of modern procedures, equipment and operational methods that can reliably indicate the practical suitability of measures for preventing major accidents or for limiting their effects. In particular, determination of the state of the art of safety technology shall employ procedures, equipment and operational methods that are comparable to those which have been successfully tested in operation."

The recognized codes of practice are the basis for the safety analysis. Since the state of the art of safety technology runs ahead of the recognized codes of practice, variations in individual cases are to be discussed.

Standards only lead the way. Other ways to achieve the safety objective are also admissible. In the event of damage, however, their equivalence must be verified. In cases where different non-standard approaches to solutions are used, the planner or planning team is personally liable for any damage.

If standards are applied, application-specific standards have priority over generic standards. For example, the EN 746-2 standard must be followed in conjunction with DIN EN 50156 (Electrical Equipment for Furnaces and Ancillary Equipment) for the assessment of safety equipment in process furnaces in the petrochemical industry. This is illustrated in Fig. 2 (normative structure). In addition, Fig. 3 shows how application-specific standards are associated with individual process units based on an example at a refinery.

Industrial plant safety is basically divided into three sections:

- Safety management
- Technical requirements
- Staff qualification.

In the following sections, the technical requirements of safety-instrumented systems are dealt with.

3. General principles

By dividing a safety-instrumented system into the units "sensor", "control unit" and "final element", the following general relationships apply in addition to the device-specific features. A very good practical description is made in [1]:

According to a much-cited study by the Health and Safety Executive (HSE) in the UK, the most frequent cause for safety equipment failure can be found in the organization. For example, planning errors, incorrect maintenance or errors made after revisions at a key point are named. For this reason, IEC 61511 focuses on the safety life cycle (Fig. 4).

To implement a safety-instrumented system, the first step involves drawing up clear specifications to describe the demanded function and its quality (SIL). Example: At a pressure over ... bar in tank ..., valve ... isolates pipe ... within ... seconds with a maximum permissible residual leakage rate of ..., risk coverage SIL 2. In addition to this safety objective, comprehensive instructions for the safety equipment are created by measures concerning proper planning and sizing, implementation, commissioning, behavior during operation, maintenance requirements and revision procedures.

The standard imposes three basic requirements:

- Avoid systematic faults
- Determine the rate of random faults
- Fulfill architecture requirements

To understand the requirements derived from these three points placed on the SIS subsystems, the process conditions must be considered. By definition electrical, electronic and programmable electronic systems are assessed in IEC 61511. If these systems are housed in a defined environment (in relation to temperature, humidity, vibration, corrosive or dirty atmosphere), a very systematic and detailed procedure takes effect to bring random and systematic faults under control. However, the weight of individual measures shifts considerably if:

- Components are assessed that are exposed to the process media and/or corrosive ambient conditions.
- It applies to a mechanical system since its failure mechanism and diagnostic capability vary fundamentally from those of electronic systems.

The user is responsible for ensuring devices are used as intended. It is important to not only rely on a general fault analysis or a database alone, but to additionally determine the specific suitability for the process concerned. Therefore, great importance must be attached to proven-in-use in this case. [1] mentions that it is unadvisable to use new devices blindly even if they are certified without proven-in-use evidence!

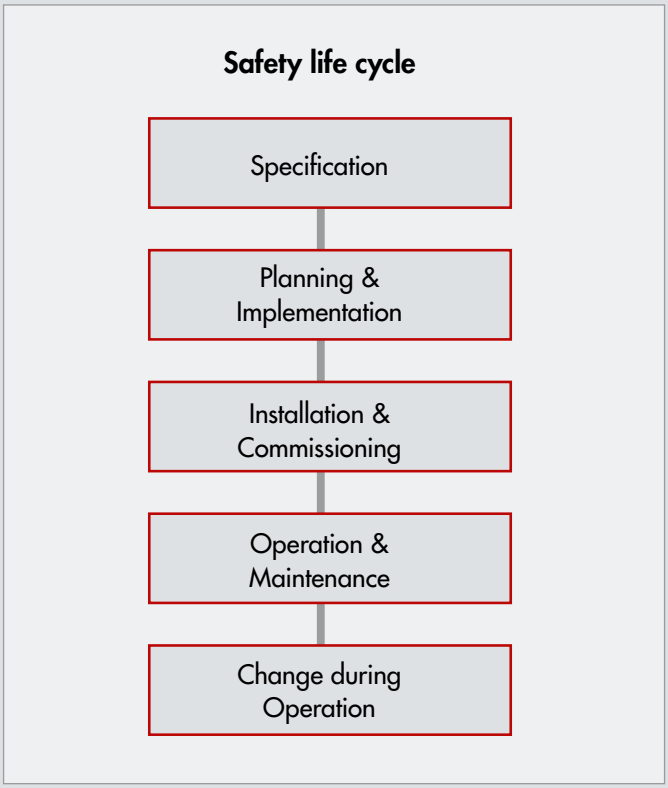

Fig. 4: Simplified safety life cycle

Key elements of a compliant implementation of a safety-instr mented system include:

- Precise specification of the necessary functions: For example, the description that a valve must close still leaves the leakage rate unspecified. A few percent seat leakage are absolutely no problem for the shutdown of a heat exchanger and plant safety would be achieved. Yet, if the discharge of a toxic gas to the atmosphere is to be prevented, a leakage rate within ppm range must be specified.
- Proof tests: To discover dangerous, undetected faults, proof tests are a vital element of the overall safety concept. The proof-test interval and procedure must be fixed. The proof test coverage must be determined by a corresponding analysis. A high degree of automation is preferable.

- Diagnostics: In addition to the proof test, a high degree of diagnostics is desirable. Diagnostics means the automated detection of faults while the process is running. In contrast to this, proof tests are usually performed after plant shutdown. They also mostly require much more complex architectural measures, such as installing a bypass to a valve. A good example of diagnostics is the discrepancy monitoring used for pressure transmitters.
- Proven-in-use: To rule out systematic faults, IEC 61511 proposes two options: The device concerned is developed in compliance with the requirements of IEC 61508 or there is evidence based on user's experience (proven-in-use). The requirements for proven-in-use are, however, not phrased in detail. In this case, a NAMUR Recommendation planned for mid-2008 will provide clear guidelines. In any case, proven-in-use involves the use of devices in the process, i.e. all process and environmental influences are accounted for. It is also explicitly allowed to take into account operational experience in non safety-instrumented systems, provided the operating conditions are the same. The HFT (hardware fault tolerance) in Table 6 of IEC 61511-1 of devices proven in use are upgraded by one. As a result, a SIL 2 system with proven-in-use devices can be designed with a single channel. Alternatively, certification in accordance with IEC 61508 is required.

Fig. 5: Examples of sensor connections affected by the process

- Documentation: All stages of the safety life cycle must be documented. This applies in particular to the proof test. The documentation of this stage must also describe the state of the system prior to the proof test. These data can be used by every operator to build fault statistics that apply to the individual process. When using external databases, it is important to ensure that the operating conditions are comparable.
- Error analysis: IEC 61511-1 (section 11.4.1, NOTE 2) justifies the demand for additional fulfillment of a certain HFT due to the restricted precision of safety data. The propagation of errors is an important mathematical tool used in scientific or technical observations. This method has not yet been applied though for the calculation of random faults according to IEC 61511. References indicating that the used numbers can show inaccuracy of more than one decimal power [2], seem to be feasible to experts in the field of instrumentation. Unfortunately, none of the SIL calculation tools on the market to date feature an option for the propagation of errors.
- Availability and sources of safety data: It is advisable, already when selecting devices, to check the availability of safety data. Some manufacturers publish these data on the Internet.

4. Final elements/sensors

4.1. Differences between field devices and control cabinet equipment

At many points IEC 61511 differentiates between logic systems (control cabinet equipment) and sensors or final elements (field devices). The latter are installed in the field and, as a result, are exposed to environmental conditions as well as the process media. This results in chemical and physical loads caused by, for example pressure, temperature, vibration and humidity. Process media affect field devices, e.g. due to corrosion, crystallization, polymerization, abrasion, formation of deposits and other effects (Fig. 5). When final elements are used, flow velocities and the occurrence of cavitation and flashing also play a key role [3]. Since the aforementioned mechanisms are systematic influences, they must be taken into account already when planning a plant. Where new processes are concerned, the assessment of these effects may be more difficult. This can be counteracted by applying special measures, such as shortened test intervals.

4.2. Differences between mechanics and electronics

Mechanical components are a key part of the function chain for sensors and for final elements even more so. The scope and theoretical background of IEC 61511 are strongly characterized by electronic systems. The table in Fig. 6 lists the differences between mechanical and electronic systems. Macroscopic dimensions, as are predominant in final elements, are easier to test. This fact and the fewer number of parts suggest that statistical errors are less relevant or not at all relevant within the required precision. Correspondingly, an elimination of errors is permissible in many cases, but must be justified. By contrast, systematic faults are of vital importance and must be ruled out by systematic engineering methods. Besides a proper design and a controlled production to meet specifications, the consideration of process conditions plays a decisive role.

4.3. Responsibilities of manufacturer and user

Accordingly, the safety analysis cannot be based merely on the safety data provided by the manufacturer. Despite the manufacturer's diligence during the safety assessment of sensors and final elements by the manufacturer, it remains ultimately restricted to the device technology. An assessment of a pressure transmitter for example, starts with the process diaphragm and ends with the terminal block (electronics and mechanics). The results of this analysis are provided by the device manufacturer. This is not sufficient by far, especially for critical processes.

A safety-instrumented system can only work as intended when the manufacturer instructions concerning installation, commissioning, operation, maintenance etc. are followed and, in particular, the influences of the specific process and the respective environment are taken into account. It can only be said again that plant safety can only be achieved by applying founded engineering practices and when the user cooperates with the device manufacturer.

4.4. Exclusion of systematic faults

It is advisable to draw up a loop data sheet for every sensor or final element to verify the exclusion of systematic faults. Besides the individual components, the interfaces (mechanical attachment, force transmission, electrical connection including cables and terminals, pneumatic connection including pipes and fittings) need to be assessed as well, even if these elements are not described or only briefly in IEC 61511. All in all, a complete analysis of all possible operating states requires extensive examination. At this point, reference is made to the publication of Part 5 of VDI 2180 planned for 2008.

4.5. Safety manual

The manufacturer presents all safety-relevant information in a safety manual. The user must consider these instructions entirely. This manual contains information for the safe application of the device, for example:

- Applicability in safety-instrumented systems
- Permissible device constructions and versions (hardware, software/firmware)
- Restrictions for safe operation
- Safety data
- Parameterization and configuration instructions
- Device behavior in operation and in the event of failure
- Procedure for proof testing

Electronic system	Mechanical system
• **Large number of components**	• **Restricted number of components**
• **Functionality of semi-conductors in microscopic dimensions**	• **Macroscopic dimensions**
• **Aging by diffusion processes (Arrhenius equation)**	• **No statistical failures but wear**
• **Limited level of testing of components in enclosure**	• **High level of testing in production and in service**
	• **The valve must be sized for the specific application**

Fig. 6: Differences between mechanical and electronic systems

4.6. Redundancy

In practice, it may be better to use redundant sensors or final elements in safety-instrumented systems for reasons of availability.
Possible architectures for redundant subsystems of safety-instrumented functions include:

- Identical redundant architecture (identical sensors): Its advantage is a higher availability of the safety-instrumented system (for example, for voting 1oo2), simplified stock-keeping and simplified commissioning and maintenance. Limits arise from possible restrictions when controlling systematic faults while the process is running.
- Diverse redundant architecture (various measuring procedures or the same measuring procedure using various devices): Besides the higher availability of the safety-instrumented system (for example, for voting 1oo2), the control of systematic faults is better implemented. It reduces the probability of simultaneous failures of several channels.

Examples of diverse redundant subsystems:

- Two pressure transmitters of various series or by various manufacturers
- Two different devices with varying measuring principles for the same physical unit, for example differential pressure transmitter and radar level gauge for non-contact continuous level measurement
- Two different devices for various physical units, for example pressure transmitter and temperature transmitter (provided that pressure and temperature are process-relevant variables)
- Redundant isolation of a pipeline by a globe valve and a ball valve

4.7. Safe parameterization

If parameters of devices in a safety loop are set incorrectly, the safety-instrumented system may not be able to fulfill its task. This is where the safe parameterization of the device comes into effect. Sensors with this function prevent operational or input errors. By validation of the data entered in the device, safe parameterization is independent from the tools used to set device parameters. The concept is based on the selection of appropriate basic settings and range checks for determined device parameters. The number of freely editable parameters is reduced to a minimum. After validation of the parameter readings, these inputs are verified again. Safe parameterization is activated by a password in a menu-driven process. At the final stage, the device is locked. This ensures that the configuration and parameterization cannot be changed unintentionally.

4.8. Proof test

Safety-instrumented systems must be tested at regular intervals. The proof-test interval is based upon the SIL verification (mathematical proof). The test is intended to reveal dangerous undetected faults. It produces proof that the components still meet the requirements.
The exact specification of requirements is the basis for the proof test. Based upon this, the parameters to be recorded must be quantified by defining set points and error ranges in the test instructions. Furthermore, the rate of detectable faults must be determined (proof test coverage); if the value of the proof test coverage is too low, this may jeopardize keeping the claimed SIL. For example in the field of final elements, it may be better to precisely measure the closing time, end position, leakage etc. of a valve in addition to the visual inspection of the closing procedure usually performed to date. These measurements and the necessary documentation can be implemented by modern instrumentation and possibly automated as well [4, 5]. The results of the proof test (especially the encountered state) must be documented. Supplementary inspections while the process is running are recommended. This helps recognize for example, corrosion, vibrations, noise, detectable leakages to the atmosphere, at an early stage.
The partial stroke testing method currently applied to final elements while the process is running can be interpreted according to the aforementioned versions as a part of an overall concept for proof tests and diagnostic methods. A detailed description can be found in [4, 5]. This method can be regarded as best practice. It reduces the rate of dangerous undetected faults in the final element. The safety margin gain may lead to the extension of the proof-test interval; an interval twice as long is realistic for favorable parameters. As always, each application must be checked individually. As for all diagnostic methods, this method primarily improves the PFD value. A change in the redundancy degree requirements (HFT) is not possible according to IEC 61511. Fig. 7 shows an example of a modern positioner with diagnostic functions and the logging of a partial stroke test.

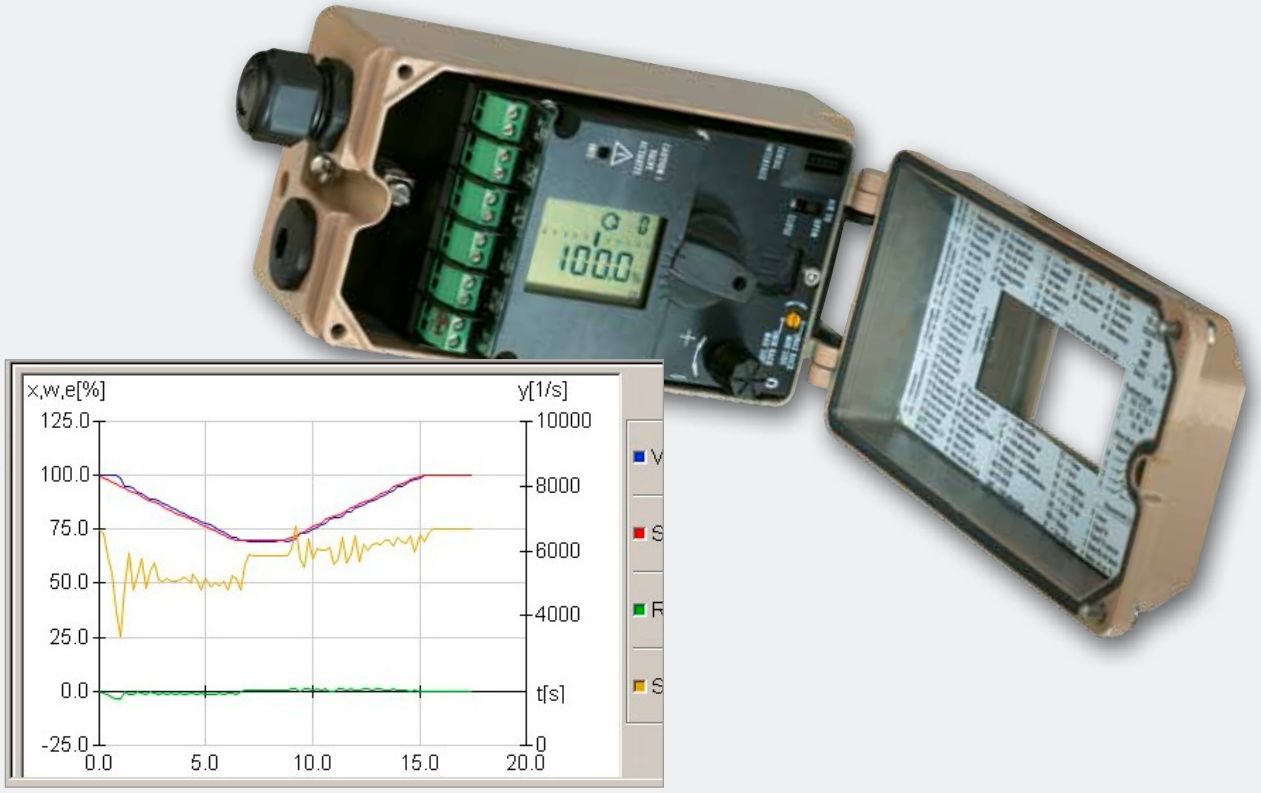

Fig. 7: Positioner with diagnostics, partial stroke test logging

5. Control equipment

Normally, logic systems with certification according to IEC 61508 are used in safety-instrumented systems.
The following points need to be taken into account on selecting a system:

- Required I/O types (e.g. initiator inputs, line monitoring, explosion protection requirements)
- Online extendibility (software, hardware)
- SIL-compliant communication between distributed systems
- Required safety/response times (is the system able to bring the process to the fail-safe state quickly enough?)

When comparing safety data, it is important to know whether the figures were determined in accordance with IEC 61508 or ANSI/ISA TR84.0.02 since they produce different results.
Minimum programming tool requirements include:

1. Precise, unique and non-manipulable identification of the program version and modules used
2. Revision management by a certified comparing system.

Minimum application software requirements include:
1. Programming guidelines
2. Consistent use of previously validated and/or certified standard software components.

Following these points leads to clearly structured programming and makes plant commissioning and maintenance easier, especially when several suppliers are involved. The programming guidelines of the application software must take the following into account:
a) Project structure (e.g. libraries, control units)
b) Naming conventions for both variables and components

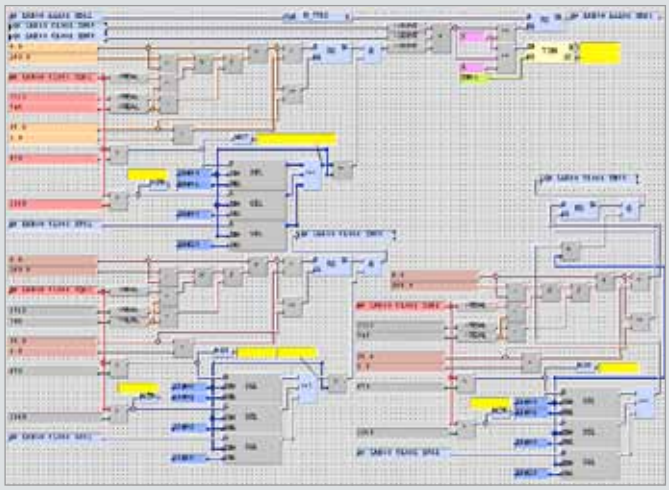

Fig. 8a: Programming example: Conventional coding

Fig. 8b: Programming example: Using standard modules

c) Complete definition of program/safety parameters that are to be set
d) Logic typicals (standardization and definition of the same logic processes)
e) Documentation (how is the project to be documented?)

The application software must have a modular structure with repeatedly used functions and function modules ([7], sheet 3). This helps minimize the extent of maintenance and testing. Fig. 8 compares a discretely structured logic and the same logic with interconnected standard modules.

Standard modules are usually used for the following functions:
- I/O conditioning, e.g. voting for 1oo2, 2oo3, 2oo2 architectures, analog input monitoring, scaling/correction modules
- Diagnostic functions, e.g. online drift diagnosis, discrepancy and range monitoring
- Maintenance switch for final element/sensor tests
- Partial stroke test

When programming standard modules, the use of at least one simplified V-model in accordance with IEC 61511 is recommended. It describes the entire software development process, from specification to final validation. Fig. 9 shows the individual process phases. Validation can be performed by the programming company or by an external organization.

The following must be observed throughout:
1. Total documentation of all phases mentioned in the V-model (requirements and test specifications, test reports, module documentation etc.)
2. Four-eye principle as organizational requirement, e.g. different persons specify and perform the test

6. Safety loop assessments

IEC 61511 states that the following measures must be implemented depending on the targeted SIL:
- Fault avoidance
- Fault control
- Fault detection

An analysis concerning the architecture (HFT) and PFD (probability of failure on demand) is to be performed for each safety function.

7. Architecture requirements

In accordance with IEC 61511-1, Table 6 (see Fig. 10), field devices can be instrumented up to SIL 2 with a single channel. SIL 3 requires a redundant architecture.

7.1. PFD (probability of failure on demand)

The PFD must be calculated and meet the required SIL in accordance with IEC 61511-1, Table 3. The PFD can be calculated using formulas that can be found in IEC 61508-6 and VDI 2180-4

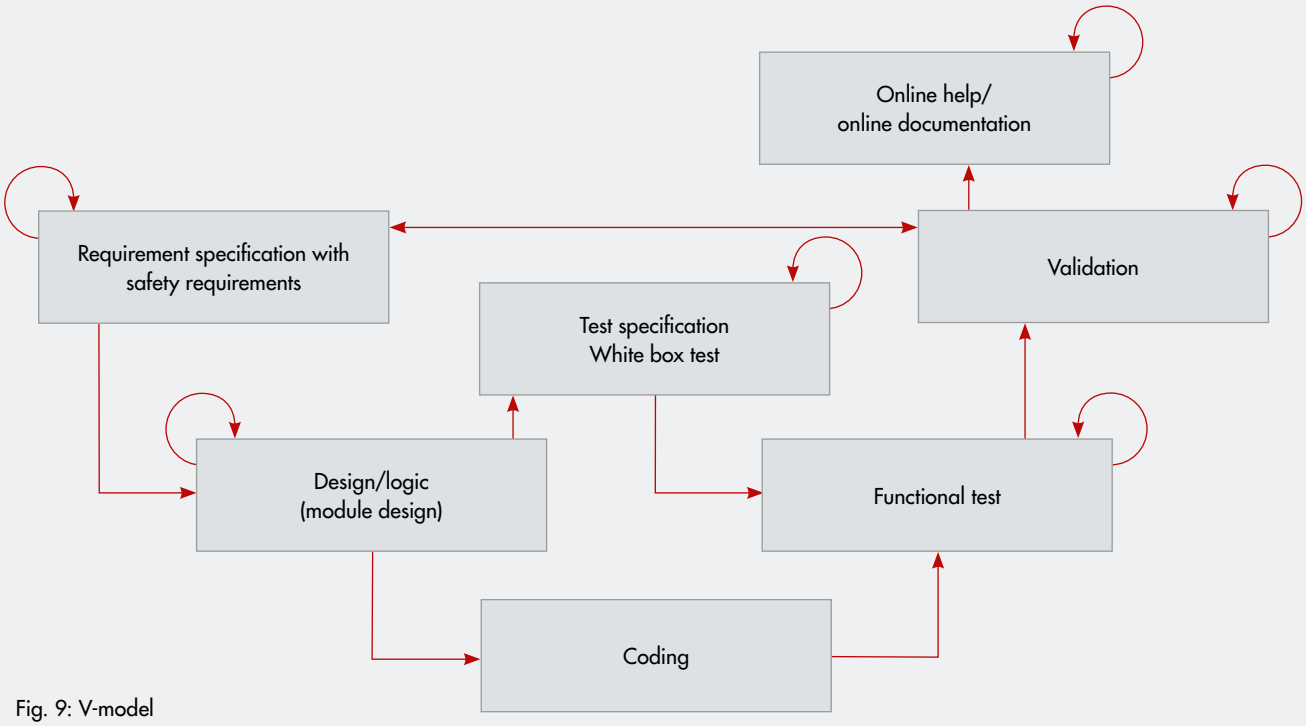

Fig. 9: V-model

[7]. The formulas in VDI/VDE 2180 are approximate formulas which may only be used under the marginal conditions listed in the standard. This makes it easy to calculate the basic structures. For mixed structures (e.g. redundant sensor circuit and single-channel final element circuit) the systems must be traced back to the basic structures step by step.

7.2. Example of a PFD calculation

The structure shown in Fig. 11 is simplified step by step. For this purpose, all blocks in line are summarized at first by adding the PFD or lambda values. Fig. 12 shows the resulting simplified structure. Finally, the diverse redundant sensor subsystem is summarized in a block in which the PDF of this subsystem is calculated using the formula for a 1oo2 system. Here, it is important to note that the formulas from the previously mentioned sources only apply to identical redundant systems. For diverse redundant systems, a worst-case assessment is recommended, applying the data of the channel with the higher failure rate. When the system has been simplified this far, the PFD values only need to be added up (Fig. 13). The final result is then assigned to a SIL with the help of Table 3 in IEC 61511-1.

Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers

SIL	Minimum hardware fault tolerance (see 11.4.3 and 11.4.4)
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

Fig. 10: IEC 61511-1, Table 6, architecture requirements

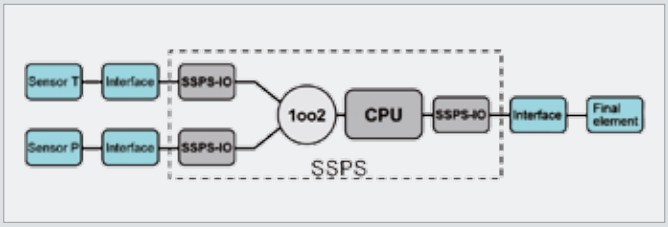

Fig. 11: Safety-instrumented system with diverse redundant sensor subsystem

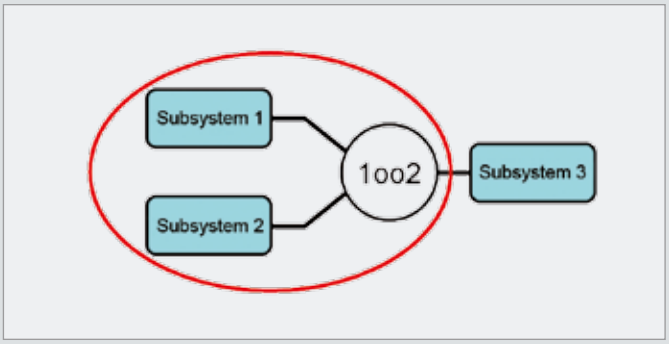

Fig. 12: Simplified structure. Serial branches are summarized

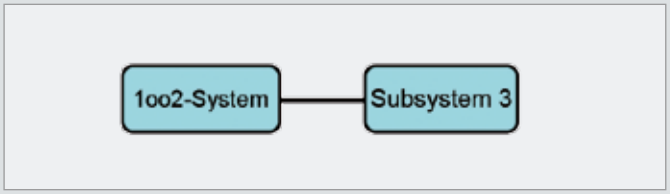

Fig. 13: Penultimate stage of the simplification. Only the two PFD values of the 1oo2 system and the subsystem 3 need to be added up.

7.3. SIL verification at a glance

The technical requirements for assessing a safety-instrumented system can be summarized as follows:

1. Check whether all devices used are suitable for the claimed SIL (manufacturer's declaration).
2. If this is the case, perform PFD calculation and assess the result based on IEC 61511-1, Table 3.
3. If item 1 is not met, use a redundant system. Where structure requirements are concerned, the next highest SIL can be achieved by increasing the HFT. However, it must be taken into account that, when using the same devices containing software, this software must be suitable for the higher SIL.
4. If item 2 is not met, a lower PFD can be achieved either by shortening the proof-test interval or by using a redundant architecture. If there is already a redundant structure, an improved PFD may also be achieved by reducing the faults with a common cause.
5. All analyses or calculations according to items 1 to 4 must be verified and documented in compliance with the requirements of the QM sy stem according to IEC 61511 (four-eyes principle). An audit must be possible at all times.

The use of software tools can support the described process and make documentation easier.

8. Limits of SIL analysis

8.1. Functional safety management system

IEC 61511 calls upon every process plant operator to introduce a functional safety management system. In the simplest case, the operator follows the requirements stipulated in this standard, which are described in detail by the safety life cycle.

In all cases, it is necessary to appoint a planning team and a separate assessment team during which the following has to be taken into account:

Planning team

- Technical knowledge of
  - Process engineering
  - Technologies used
  - Methods used
- Safety knowledge of
  - Laws, standards and guidelines
  - State of the art in safety technology

Assessment team

- Determines which other safety expert groups are to contribute to the assessment
- Determines which means are necessary to completely perform the assessment
- Is independent from the planning team

The planning and assessment teams must consist of different people, i.e. the four-eyes principle must be observed throughout. Fig. 14 shows a possible structure for a management system.

8.2. Staff qualification

Further training of staff and regular exchange of experience are essential to ensure a continuously high quality standard. It makes sense to use the same staff for comparable tasks to ben-

efit from their existing experience. The soft factors, however, cannot be ignored either. These include:

- How can the quality of staff performance be advanced?
- Are further trainings performed on a regular basis?
- How high is staff satisfaction?
- What is the working atmosphere like?
- Are there problems concerning staff recruitment?

The best risk reduction can only be achieved using safety-instrumented systems when the three areas of management system, technical requirements and staff qualification are considered. However, even when these criteria are observed, restrictions in sizing safety-instrumented systems still exist:

8.3. Calculation of safety loops

During the PFD calculation of safety loops, the following points must be observed in particular:

- On which data is the calculation based?
- How were the data obtained?
- Are generic values from a given source really transferable?
- Which requirements are linked to the application?

What use are generic values measured in a clean room for a safety loop calculation in a rough refinery environment?
What use are safety loops that must be tested on a daily basis to safeguard a SIL 3 risk, for example?

8.4. Verification of required qualification

Devices can be qualified according to [7] as follows for use in safety-instrumented systems:

- SIL verification according to IEC 61508
- Proven-in-use verification by manufacturer or operator
- Verification of suitability by type testing [8] or
- Unit verification [8]

8.5. Constructional practice

In addition to the verifications concerning device suitability, the following points, for example must be considered:

- Are the process connections large enough and safeguarded against being shifted by the process medium?
- Has fail-safe been observed in the wiring?
- Are short circuits and interruptions in the signal lines recognized?

1 Objective/purpose
2 Terms and abbreviations
3 Scope
4 Organization in the safety life cycle
4.1 Safety plan (safety life cycle
4.2 Delegation of responsibility
4.2.1 Planning team
4.2.2 Assessment team
4.3 Risk analysyis
4.3.1 Assessment of risks regarding HAZOP
4.3.2 Assignment of the scope of the relevant standard
4.4 Creation of the product requirement document
4.5 Creation of the functional specification document
4.6 Implementation of the software
4.7 Verification of the software
4.8 Mounting and commissioning
4.9 validation
4.10 Operation and maintenance
4.11 Decommissioning
5 Revision management
6 Tests in the safety life cycle
6.1 Purpose
6.2 Tests/checks performed
6.2.1 Checking of the product requirement document
6.2.2 Checking of the functional specification dokument
6.2.3 Verification of the software
6.2.4 Check to ensure proper mounting and commissioning
6.2.5 Validation

Fig. 14: Elements of a management system

For these points, there are no calculation values. In this case, the expertise of the planning team is called for. Corresponding considerations and decisions are to be documented.

Summary

To summarize, plant safety can be achieved by the familiar elements:

- Management: drawing up a safety management system
- Technology: observation of recognized codes of practice during selection and use of necessary devices and systems
- Preferable use of certified or proven-in-use components for safety-instrumented systems
- Standardization: hardware and software standardization as far as possible
- Staff: use of qualified staff

References:

[1] Hablawetz, Dirk; Matalla, Norbert; Adam, Gerhard BASF AG: IEC 61511 in der Praxis - Erfahrungen eines Anlagenbetreibers, atp 10/2007
[2] Smith, David J.: Reliability, Maintainability and Risk, Elsevier Butterworth-Heinemann, Burlington, 2003
[3] Karte, Thomas; Nebel, Eugen; Dietz, Manfred; Essig, Helge: Reliability data and the use of control valves in the process industry in accordance with IEC 61508/61511, atp 2/2005
[4] Karte, Thomas; Kiesbauer, Jörg: Partial Stroke Testing For Final Elements, Proceedings of "Petroleum and Chemical Industry Conference (PCIC) Europe 2005", Basle, Switzerland
[5] Karte, Thomas; Schärtner, Karl-Bernd: Partial-stroke testing on final elements to extend maintenance cycles, atp 4/2005
[6] IEC 61511, Parts 1 – 3, Berlin 2005
[7] VDI/VDE 2180, Parts 1 – 4, Berlin 2007
[8] Internal notice on functional safety published by the Technical Committee 6.13 of VDI/VDE Society for Measurement and Automatic Control (GMA)

Dr. Arno Götz (46) is head of the Product Safety Department and the Test Center at Endress+Hauser GmbH+Co. KG, Maulburg. His main fields of activity include functional safety and explosion protection. In addition, he is member of the DKE Joint Committee 914.

Address: Endress+Hauser GmbH+Co. KG,
Hauptstr. 1, 79689 Maulburg, Germany,
Phone: +49 7622 28-1645,
E-mail: arno.goetz@pcm.endress.com

Dr. Andreas Hildebrandt (48) has been head of the Training and Committee Work at Pepperl+Fuchs GmbH, Mannheim since 2006. His main activities include explosion protection and functional safety. In addition, he is head of the EMC working group at ZVEI and is member of the DKE Subcommittee 921.3 and Committee 767.0.4 as well as the Technical Committee 6.13 at the VDI/VDE Society for Measurement and Automatic Control (GMA).

Address: Pepperl+Fuchs GmbH,
Königsberger Allee 87, 68307 Mannheim, Germany,
Phone: +49 621 776 -1454,
E-mail: ahildebrandt@de.pepperl-fuchs.com

Dr. Thomas Karte (52) is responsible for application engineering of electropneumatic devices at SAMSON AG in Frankfurt. He is member of the Technical Committee 6.13 at the VDI/VDE Society for Measurement and Automatic Control (GMA) and DKE Joint Committee 914.

Address: SAMSON AG,
Weismüllerstr. 3, 60314 Frankfurt, Germany,
Phone: +49 69 4009-2086
E-mail: tkarte@samson.de

Dipl.-Ing. (FH) Bernd Schäfer (41) has worked at HIMA since 1996. He started as project manager in the engineering department. Since 2004, he has been product manager in the field of OPC and SCADA and deals with asset management and special applications, such as training simulation.

Address: HIMA Paul Hildebrandt GmbH & Co KG,
PM Dept., Albert-Bassermann-Str. 28,
68782 Brühl near Mannheim, Germany,
Phone: +49 6202 709-453,
E-mail: b.schaefer@hima.com

Dipl.-Ing.(FH) Johann Ströbl (54) has worked at TÜV SÜD Industrie Service since 1980. He is currently head of the Electrical and Building Technology Department as well as Firing and Heat technology at the Regensburg branch office. His main fields of activities cover the assessment of safety equipment in process plants and complex industrial thermal process plants.

Address: TÜV SÜD Industrie Service GmbH,
Friedenstraße 6, 93051 Regensburg, Germany
Phone: +49 941 9910-402,
E-mail: johann.stroebl@tuev-sued.de

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

2006-06 DR · WA 233 EN