SAFETY CRITICAL DEVICES

Doc 252/24

EUROPEAN INDUSTRIAL GASES ASSOCIATION AISBL

AVENUE DE L'ASTRONOMIE 30 • B – 1210 BRUSSELS
Tel: +32 2 217 70 98
E-mail: info@eiga.eu • Internet: www.eiga.eu

Doc 252/24

SAFETY CRITICAL DEVICES

Prepared by WG-21 – Process Safety
Published in July 2024

Disclaimer

EUROPEAN INDUSTRIAL GASES ASSOCIATION AISBL
Avenue de l'Astronomie 30 B 1210 Brussels Tel +32 2 217 70 98
E-mail: info@eiga.eu Internet: www.eiga.eu

Table of Contents

Tables

Figures

1 Introduction

The concept of safety critical elements was introduced in the UK oil and gas sector by the legislation enacted following the Piper Alpha disaster in 1988. After this, the concept has been extended to the rest of process industries, including industrial gases.

A common practice to all process industries is that they manage the safety of their operations using Risk Based Process Safety Management Systems.

The main objective of Risk Based Process Safety Management Systems is preventing the occurrence of Process Safety Incidents (PSI), as defined in EIGA Doc 223, *Monitoring of Process Safety Performance* [1].[1]

Safety critical devices (SCD) are defined specifically as instruments and equipment which mitigate against a safety risk, i.e. not a business or environmental risk. The safety risk should be credible in terms of probable likelihood and potential consequence.

The purpose of this publication is to provide industry guidance for the identification and management of SCD within the industrial and medical gases industry.

2 Scope and purpose

2.1 Scope

This publication provides guidelines for developing management procedures, training, proof testing and performance analysis to improve reliability of safety critical devices to prevent the occurrence of PSIs.

Control of major-accident hazards involving dangerous substances is governed in Europe by Directive 2012/18/EU *on the control of major-accident hazards involving dangerous substances*, that lays down rules for the prevention of major accidents which may result from certain industrial activities and the limitation of their consequences for human health and the environment [2]. This directive is known as Seveso III.

A particular case of PSIs are events related to serious injury or severe damage such as hazardous events as defined in IEC 61511, *Functional safety - Safety instrumented systems for the process industry sector*, Tier 1 incidents as defined by Center for Chemical Process Safety (CCPS) [3], or Tier 1 incidents defined by Conseil Européen de l'Industrie Chimique (CEFIC) [4, 5, 6].

IEC 61511 (adopted by CENELEC) was developed to provide good engineering practices for the application of Safety Instrumented Systems in the process industries sector in response to major incidents [4]. Some industry gas member companies have adopted the concept of IEC 61511 within their own standards and refer to these.

However, there are some industrial gases facilities, that either because of the amount (threshold value) or the nature of the handled products are out of the scope of these regulations and standards. This publication includes guidelines to extend the concept of some SCDs to all facilities.

This publication refers to some of the elements in EIGA Doc 186, *Process Safety Management Systems* [7].

2.2 Purpose

This publication:

- provides definitions of common terms used in safety systems in the process industry;

[1] References are shown by bracketed numbers and are listed in order of appearance in the reference section.

- provides a brief introduction to safety critical devices;
- gives guidance on how to identify SCDs on typical production plants in the industrial gas industry which provide safeguards to prevent PSIs;
- identifies operation, maintenance and testing requirements for SCDs;
- provides guidance on documentation of SCDs; and
- provides guidance related to instrumented protection outside the scope of IEC 61511 [4].

3 Definitions

For the purpose of this publication, the following definitions apply.

3.1 Publication terminology

3.1.1 Shall

Indicates that the procedure is mandatory. It is used wherever the criterion for conformance to specific recommendations allows no deviation.

3.1.2 Should

Indicates that a procedure is recommended.

3.1.3 May

Indicates that the procedure is optional.

3.1.4 Will

Is used only to indicate the future, not a degree of requirement.

3.1.5 Can

Indicates a possibility or ability.

3.2 Technical definitions

3.2.1 Administrative control

Training, procedures, policies, or shift designs that lessen the threat of a hazard to an individual. Administrative controls typically change the behaviour of people (for example factory workers) rather than removing the actual hazard.

3.2.2 Basic Process Control System (BPCS)

A system that responds to input signals from a process, its associated equipment, other programmable systems and / or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner (IEC 61511-1) [4].

3.2.3 Process Safety Incident (PSI)

A release of energy or material in process involvement, with actual or potential consequences above a minimum reporting threshold.

3.2.4 Proof test

Periodic test performed to detect dangerous hidden faults so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition.

3.2.5 Protection layer

Anything that reduces risk by control, prevention or mitigation. It can be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a relief valve, a Safety Instrumented System (SIS), an instrumented protection implemented in the BPCS, or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions.

3.2.6 Reliability of a Safety Critical Device

A measure of fulfilling the intended safety function and is expressed as the probability that a device or system can perform a defined function under stated conditions for a given period of time. For a Safety Instrumented Function (SIF), matching a given Probability of Failure on Demand (PFD) target may be obtained by using Safety Integrity Level (SIL) classified detectors, logic solvers and final element.

3.2.7 Safety Critical Device (SCD)

A mechanical, electro-mechanical or instrumented device or a set of such devices which provide a safeguard preventing a significant PSI. SCDs are typically defined when the unmitigated (i.e. in the absence of safeguards) risk level is high. SCDs are defined specifically as devices which mitigate against a safety risk, i.e. not a business or environmental risk. Examples of these are pressure relief valves, pressure bursting discs, safety relevant check valves, and restriction orifices.

Companies or other publications may reference SCDs as Safety Critical Elements or otherwise.

3.2.8 Safety function

A function to be implemented by one or more protection layers, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazard.

3.2.9 Safety Instrumented Function (SIF)

A protection layer whose objective is to achieve or maintain a safe state of the process when a specific hazardous event occurs and is composed of sensor(s), logic solver(s), and final element(s). The SIF is implemented in the SIS which is normally composed of several SIFs.

An example for a SIF would be a low level switch at a steam boiler, together with a safety PLC as logic solver and a relays actuating block valves in the fuel supply to the burners.

3.2.10 Safety Integrity Level (SIL)

Describes the discrete level allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS.

3.2.11 Safety Instrumented System (SIS)

A separate and independent combination of sensors, logic solvers, final elements, and support systems that are designed and managed to achieve a specified performance. A SIS may implement one or more SIFs.

Recognised methodologies to define the design of SIS include risk graph, Layer Of Protection Analysis (LOPA) and risk matrix.

4 Introduction on safety protection layers

Within each process, risk reduction should begin with the most fundamental elements of process design: selection of the process itself, the choice of the site, plant layout, inherently safe design and decisions about hazardous inventories.

Different layers of risk reduction are required to meet the acceptable frequency of a hazardous event occurring, as shown in Figure 1. Each protection layer consists of process controls, equipment and / or administrative controls.

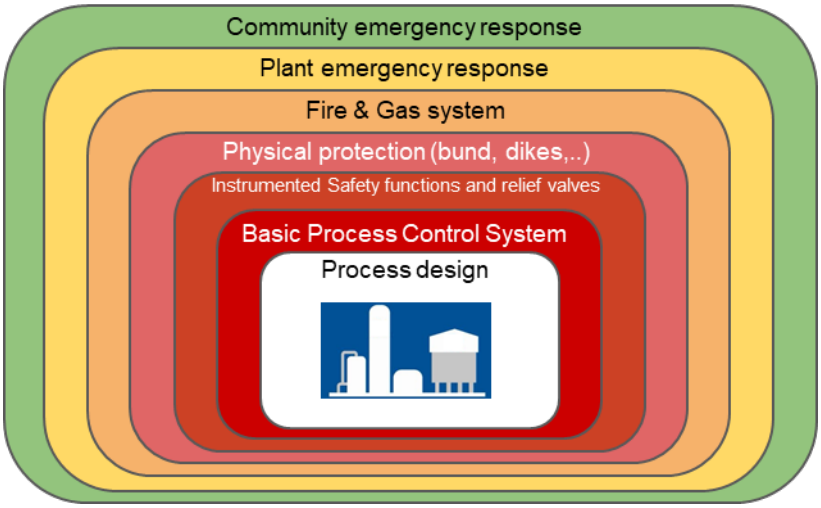

Figure 1 – Safety protection layers

The safety protection layers will typically comprise a combination of preventive and mitigating systems. Preventive systems include but are not limited to mechanical protection systems, non-SIS and / or SIS protection layers. Mitigation systems include but are not limited to bunds, fire / gas detection, emergency response.

Systems considered within this publication include mechanical protection systems (for example a pressure relief device), SIS and mechanical mitigation systems (for example protective barriers, firewalls, dykes etc.).

4.1 IEC 61511 – Safety Instrumented Systems (SIS)

The IEC 61511 series is the international design standard which addresses all SIF life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning [4].

Best practice for new plants with major or significant hazards is to follow a standard, such as IEC 61511, to enable the identification and specification for SISs to be derived [4]. The SIS includes all devices necessary to carry out each SIF from sensor(s) to final elements(s).

Generic major and significant hazards identified should be risk assessed during this process in addition to any plant specific hazards identified at the design stage (such as whilst performing a HAZOP).

During an IEC 61511 review, the SIS life-cycle activities and SIFs should be identified [4]. These SIFs are assigned an appropriate performance level. In terms of establishing common definitions and terminology all instruments should be identified as either as:

- non-safety instrument; or
- safety instrument.

4.2 Safety Integrity Levels (SIL)

Where SILs have been defined to a SIF as an output from an assessment done in accordance with IEC 61511, copies of the assessment documentation shall be included with the equipment maintenance scheduling / recording system for all components of that safety system [4].

SILs may be defined for SIF in high-risk processes according to IEC 61511 methodology [4]. There is no requirement to retrospectively carry out IEC 61511 reviews and identify SILs on existing plants [4].

Specified maintenance and testing requirements as an output to an IEC 61511 assessment shall be strictly adhered to [4].

5 Site specific Safety Critical Devices

5.1 Identifying site specific SCDs

Every new or existing site shall identify the safety critical devices of their site. This may be done by using a Process Hazard Analysis (PHA) (such as a HAZOP/LOPA/Check list/What-if studies etc.) which highlights safeguards against major risks. It is the site's responsibility to maintain this list with any changes, for example from a site change or addition of new equipment.

It is also recommended that a system be implemented to easily identify SCDs (for example onsite or on the P&ID by labelling or tagging).

These devices shall also be listed in the asset list in the maintenance scheduling / recording system. For more information see Section 8.

A company may select different methods based on their process safety management systems, the type of risk assessments available, or on the relative risk in the facility. Different approaches can be applied to identify SCDs:

Approach 1: Qualitative

Using a PHA methodology such as What-If, HAZOP or Failure Mode and Effect Analysis (FMEA):

- Identify the scenarios which could result in a PSI;
- List the preventive and mitigating safeguards against a PSI; and
- Identify the SCDs from the list of safeguards which protect against significant PSIs.

Approach 2: Semi-quantitative

Using semi-quantitative PHA such as Failure Mode, Effect and Criticality Analysis (FMECA), or HAZOP + LOPA / Fault Tree:

- Identify the scenarios which could result in a PSI;
- Identify safeguards or Independent Protection Layers (IPLs) which are preventing or mitigating significant scenarios (the risk level criteria is typically defined by company policy); and
- Use the list of credited safeguards or IPLs to generate a list of SCDs.

Approach 3: Generic

Develop a list of SCDs for standardised processes or facilities based on Approach 1 or 2.

The generic approach of SCDs can be used only on identical or similar facilities (similar P&ID, similar process equipment, similar operating conditions etc.). Additional process risk studies shall be done on gaps.

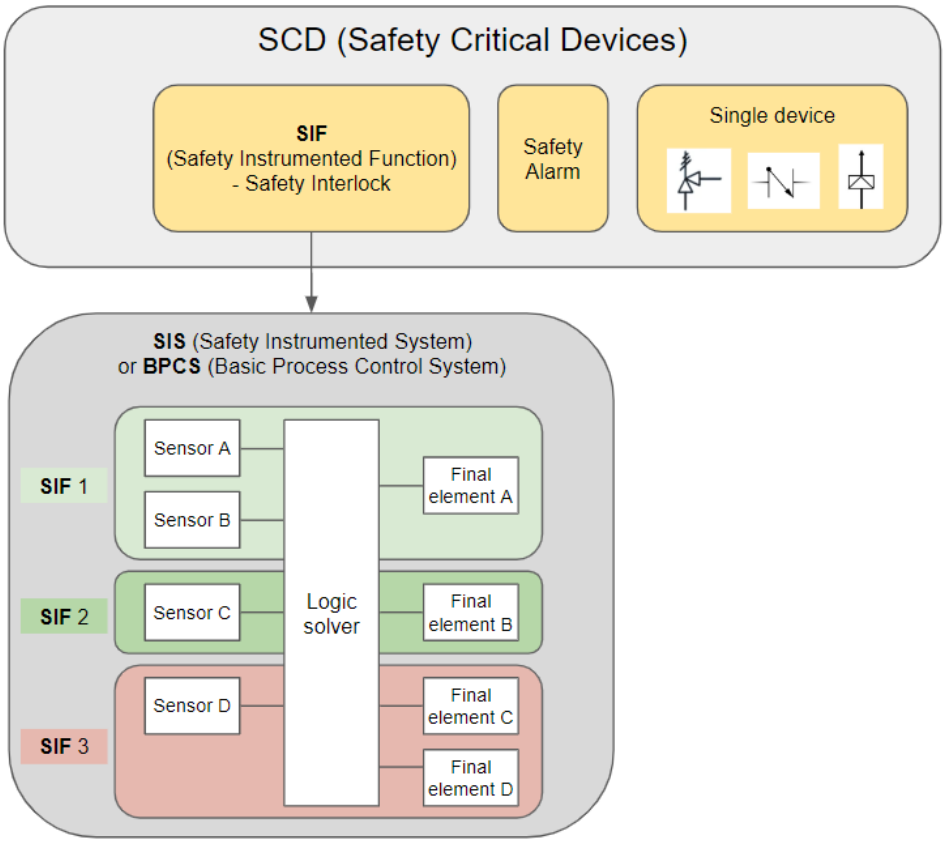

Figure 2 – Identifying SCDs

NOTE When a QRA (quantitative risk assessment) is available for a specific facility, use the list of all safeguards that were considered to provide risk reduction and complete the SCD list when relevant.

5.2 Operations and responsibility of management control

Management shall be accountable to ensure that SCDs are identified, implemented, maintained and operational at each facility and shall provide and document adequate training to local process operators, maintenance personnel, and all remote persons that have operational control of the process.

A process shall be in place to ensure that SCDs are identified and managed. In different phases of plant life the responsibility may lay with different people.

During the project phase, the project manager, a designated project team member or another individual having overall project management responsibility is normally responsible for identification and the implementation of the SCDs.

During the operation phase the plant or operations manager is normally responsible for ensuring that the selected SCDs are operational, regularly maintained and tested.

5.3 Qualification and training

Management shall ensure adequate training is provided to local process operators, maintenance personnel, and all remote persons that have operational control of the process.

Maintenance tasks on SCDs shall be carried out by competent persons authorised to work on safety rated systems to an approved and documented procedure.

6 Design rules for SCDs and SIFs

6.1 Design considerations for SCDs

The design rules for safety critical devices shall consider the same guidelines as for an independent protection layer (IPL). They should be:

- **Independent** of the occurrence of the hazardous event, its causes, and common cause failures. The dependency effects of safeguards already claimed for the same scenario should be considered negligible or already taken into account.

- **Effective** in preventing the scenario when it functions as designed. To be considered effective, a safeguard is able to prevent the process risk scenario from occurring in the absence of all other safeguards (for example relief valve designed to avoid overpressure).

- **Auditable**, credited safeguards can be periodically tested or inspected for proof of functionality. The auditing process confirms the effectiveness of the safety critical device through review of the design, installation, functional testing when relevant, and maintenance systems.

SCDs should preferably not rely on the actions of an operator whether manned / unmanned or attended / unattended, i.e. trip functions are preferred to alarms. In some cases, operator action may be required, for example to initiate an emergency stop. When operator actions are considered, they should be equally independent, effective, and auditable.

6.2 Design considerations for SIFs

SIFs shall be configured to provide independent layers of protection, for example preventing common mode failure of individual components (valves, solenoids, logic controllers etc) or of common utilities (electricity, instrument gas etc). Each trip should ideally have separate sensing elements (for example a level transmitter and a level switch) and separate shut-off devices (for example an emergency shut-off valve and / or a pump trip).

In general, SIFs should be configured as fail safe and preferably latching for all failure scenarios (including loss of input signal, electricity, instrument gas etc.).

6.3 Design considerations for SIL

All instruments related to the SIL rated loop, such as relays, timers within common panels, should be marked as part of a SIS where applicable so that maintenance personnel are aware of implications if maintenance or testing is carried out. Safety loops that require regular testing should be designed for easy testing. For example, test buttons, partial stroke provisions, position / status feedback etc.

Redundancy of equipment may be required to reach the expected SIL level for a SIF. In this case, the redundancy can be provided in the detection system, the logic solver or in the final elements (actuating devices).

For example, multiple level switches installed on a steam drum is a typical case of redundancy. In this case, the safety function reliability of a SIF has been increased by adding a second or third device.

The level of redundancy may be calculated or deduced by different methods. IEC 61511 gives a selection of methods [4].

6.4 Modes of operation of a SIF

The way in which a SIF operates may be either demand mode or continuous mode.

In a demand mode of operation, the SIF is only performed on demand, in order to transfer the process into a specified safe state. The demand mode is identified either by a hazard assessment or practical experience. If the demand frequency is greater than once per year, it should be recognised as a high demand mode. Otherwise, it is a low demand mode. If high demand mode has been identified, consider redesigning the process control such that the SIF becomes a low demand mode.

In a continuous mode of operation, the safety critical function retains the process in a safe state as part of normal operation. Normally continuous mode is not used in the Industrial Gases or Chemical Industry.

6.4.1 Safety integrity parameters

The *Probability of Failure on Demand* (PFD) is the measure of safety integrity for the SCD. It is the probability that the SCD will fail in a manner which will render it incapable of performing its intended safety function. As such, the SCD will be unable to respond to a demand and no safety action (for example shutdown) will be initiated.

Since a SIF is made up of several elements (sensors, logic solver, final elements) it results into an overall PFD.

The Failure Rate (λ) is the number of failures of an element of a SIF, expressed in the number of failures per unit time, for example per million hours. All element failures are divided into safe failures and dangerous failures. All failures that have the potential to cause the SIF to fail to respond to a process demand are categorised as *Dangerous*. The other failures are classified as Safe. Independently, all failures detected on-line while the SIF is operating are classified as *Detected* failures while all failures not detected on-line are classified as *Undetected* failures. The PFD of a SIF is usually derived from the Dangerous Undetected failure rate.

6.4.2 Allocation of safety functions to protection layers

In order to achieve functional safety, two types of requirements are necessary:

- Requirements for the safety function (what the function is required to do); and
- Requirements for the safety integrity (the likelihood of the function being performed satisfactorily).

The safety function requirements are derived from the hazard analysis, while the safety integrity requirements are derived from the risk assessment. The higher level of safety integrity, the lower likelihood of dangerous failure.

Once protection layers are established, it is necessary to define appropriate safety functions in order to achieve the risk reduction required by each protection layer.

The required risk reduction for each SIF for a low demand mode of operation is presented in Table 1. SIL level 4 is not added to Table 1 as it is not commonly used in the Industrial Gases Industry.

Table 1 – Safety integrity requirements for demand mode (average PFD)

DEMAND mode of operation		
Safety Integrity Level (SIL)	**PFD (Probability of failure on demand - average)**	**Required risk reduction**
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1 000 ≤ 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 ≤ 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 ≤ 100

The safety integrity level of the SIF can be determined using various methodologies described in IEC 61511 [4].

Typical probability of failure on demand values can be found in literature, for example from the HSE (www.hse.gov.uk), IEEE (www.ieee.org), OREDA CCPS Process Equipment Reliability Database or local authorities [5].

6.5 Robustness

Robustness is important when selecting SCDs. Robustness is an evaluation using an analytical method in which the results obtained are considered reliable even when performed under slightly different conditions. It is the ability of a SCD to remain unaffected when slight variations are applied. This ability can be affected by several factors including ageing, weather, software degradation or security breaches.

Robustness is important for a safety system to continue execution during normal as well as abnormal or other unanticipated conditions. The capability of a safety system to continue monitoring and controlling a system in such circumstances is vital. Some attributes for robustness include but are not limited to:

- Redundancy
- Preventive maintenance
- Calibration
- Proven reliable components
- Regular software updates
- Cyber security studies
- Replacing obsolete software

6.6 Selection of components

Selection of components of SCDs is also described in:

- IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems* [8]; and
- IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements* [9].

Appropriate evidence shall be gathered that the components are suitable for use as SCDs. The evidence should include adequate identification and specification, consideration about manufacturer's quality and demonstration of the performance in a similar operating environment.

For programmable components, in addition to the previous requirements, all configuration options or/and unused features possibly influencing safety shall be identified and analysed. It should be established that they are unlikely to jeopardise the required SIF. Other evidence of suitability shall be considered in respect with the specific operating environment of the device: I/O signals, modes of operation, functions and configurations, and evidence of prior use in similar operating environments.

7 Documentation of SCDs

Each SCD shall be described and documented including:

- the scenarios that the SCD is protecting against. The scenarios shall consider the stationary and transient plant conditions (for example start-up) and standard and non-standard equipment conditions (for example equipment maintenance, sensor calibration and / or repair);

- the safety limits for the set point;

- the sequence of actions, either manual or automatic;

- the operation of all bypasses / overrides and under what circumstances / limitations these may be used, including detailed step by step instructions for implementing and removing bypasses / overrides;

- a risk assessment and additional safety precautions to be taken when the SCD is bypassed / overridden; and

- the instructions for proof testing, calibration and preventative maintenance.

8 Maintenance and testing of Safety Critical Devices

The integrity of the safety function of the SCD shall be preserved by maintenance and not compromised during operation.

Maintenance includes repair / replacement, calibration and testing of safety critical devices and shall be integrated into the normal plant maintenance scheme.

SCDs shall be uniquely identified as equipment in the maintenance scheduling / recording system.

8.1 Maintenance management system

Organisations shall implement a maintenance management system (MMS) to schedule, monitor, and document asset maintenance, and to manage preventive maintenance programmes. See element 15 in EIGA Doc 186 for more information [7].

SCDs shall be included in the preventive maintenance programmes.

An MMS also supports the recording of all maintenance and testing activities of SCDs. A records retention policy for critical control documents that takes into account government regulations and / or industry standards shall be established. It is a good practice to keep records of maintenance and critical controls for the life of the process equipment. Preventive maintenance of safety critical devices consists of visual inspection, calibration, performance and proof testing.

8.2 Visual inspection

Each SCD should be visually inspected periodically as defined in the risk study to ensure there is no observable deterioration and no obvious unauthorised modification. Visual inspection may also be used to support tracking of maintenance programmes in a way that, for example, tags can be controlled and identify deviation from schedule.

8.3 Calibration

Calibration of SCDs is required on a periodic basis and before placing in service. Calibration is a method of determining an error between the output (or response) of a measuring instrument and the value of the input. The (accuracy) error is determined by applying a traceable standard to the instrument and comparing the instrument reading to the standard. Adjustments are made only if needed to set the accuracy error within a specified tolerance.

Not all instruments are measuring instruments and those that are not, cannot by nature be calibrated and are therefore exempt from calibration. Example are switches and most temperature elements.

8.4 Proof testing and performance

Periodic proof tests shall be conducted to reveal undetected dangerous faults that impair the SCD from operating in accordance with the design. The proof test interval should be selected to achieve the average probability of failure on demand as required in the safety requirements specification. Factors to be considered include:

- the operating constraints (e.g. facility periodic shutdown frequency);
- the outcomes of the process risk assessment; and
- the applicable regulations and standards, notably for pressure relief devices and safety instrumented systems;

When minimum test frequencies have been set, they should not be less demanding than the:

- company minimum test frequency; and
- supplier's recommendations.

The entire SIF should be tested (including the sensors, logic solver and final elements). The elements of the SIF do not need to be tested simultaneously. They can be tested individually and may have different test intervals, provided this is considered in the calculation of the loop probability of failure on demand. The conditions of testing shall be representative to the normal operation conditions of the SIF. During proof testing, the as-found condition of the SIF shall be recorded and any deficiencies found shall be rectified.

The test interval can be extended in case the safety function has been activated during operation of the plant, for example a real trip has been taken place. The shutdown can be treated as a test, but it shall be fully logged and documented.

Additional functional testing of a SIF is required:

- during the commissioning; or
- after any modification to a SIF;

If the specified test frequencies are not met there should be a process in place to define variance based on a risk assessment for example Management of Change (MOC), see EIGA Doc 51, *Management of Change* [10].

During proof testing, the performance parameters of the SCD shall be assessed, for example response time, leak rate as defined in the risk assessment.

8.5 Maintenance bypass

An SCD may be disabled temporarily for troubleshooting / testing. An SCD bypass shall:

- Only be applied for maintenance activities or for process cycle restarts but only when called for in the restart Operating Procedure(s).
- Be used only where strictly required for the minimum time necessary.
- Not be used to intentionally or unintentionally facilitate the existence of the hazard scenario for which the SCD is designed to mitigate. For example, operation of the process cycle outside its established design limitations, ignoring potentially unsafe atmospheres, disabling an emergency trip station, etc. Intentional cases will require a temporary/emergency MOC, unintentional cases will be avoided via use of alternative mitigations (e.g. human surveillance of the process).

In the event of failure of a SCD component that cannot be immediately corrected, temporary alternate hazard control methods shall be implemented to continue plant operations. These temporary changes shall be executed and documented using the MOC procedure.

A SCD design may provide a means to place it in bypass, thereby disabling it to allow activities to be completed without risk or occurrence of a SCD initiated shutdown (or other control action). SCD bypasses may be designed to revert normal operation automatically if left in bypass for a period of time. Human intervention may reset the bypass countdown to allow activities that take longer than that period to complete. For this kind of intervention, a hazard assessment shall be completed and documented.

8.6 Performance indicators

The analysis of the events related to the performance of the SCDs can allow:

- verification effectiveness;
- understanding causes for failure;
- understanding causes for lack of process control (i.e. demand rate on SCDs); and
- improvement of mitigation or protection systems.

The following events should be reported as actual or potential PSI:

- SCD activation on process deviation: Following a deviation of a process parameter from its normal operating range, the activated SCD returns the installation to safe condition as expected.
- SCD failure-to-activate as expected on process deviation: Following a deviation of a process parameter from its normal operating range, the related SCD fails to activate or does not perform fully as expected.
- SCD unintentional or erratic activation: The SCD activates even though there is no deviation of a process parameter.
- SCD found defective during maintenance / testing: The SCD does not perform as expected or only performs partially its safety function during its functional test.
- SCD found bypassed or inhibited: The SCD is found bypassed or inhibited (and so non-operational) and not identified as such with corresponding MOC.
- A SIF is overridden without alternate hazard controls.
- SCD found missing: The SCD not installed or removed for maintenance.
- Breakdown of maintenance on a SIF: Breakdown of the maintenance system on a SIF, where the integrity of the loop is compromised. For example, one instrument in a SIF voting system fails and / or is put in maintenance and is not repaired and put online within the time allowed. The design probability of failure on demand would not be fulfilled.

8.7 Changes involving SCDs

Any modification or addition of SCDs shall undergo an MOC process as described in EIGA Doc 51 [10].

9 References

Unless otherwise specified, the latest edition shall apply.

[1] EIGA Doc 223, *Monitoring of Process Safety Performance*, www.eiga.eu

[2] Directive 2012/18/EU *on the control of major-accident hazards involving dangerous substances*, www.europa.eu.

[3] API 754: Process Safety Performance Indicators for the Refining and Petrochemical Industries, API

[4] IEC 61511, *Functional safety - Safety instrumented systems for the process industry sector*, www.iec.ch.

[5] Center for Chemical Process Safety (CCPS), www.aiche.org/ccps.

[6] Conseil Européen de l'Industrie Chimique (CEFIC), www.cefig.org.

[7] EIGA Doc 186, *Process Safety Management Systems*, www.eiga.eu.

[8] IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*, www.iec.ch.

[9] IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements*, www.iec.ch.

[10] EIGA Doc 51, *Management of Change*, www.eiga.eu.