

Safety Requirements Specification Guideline

Comments on this report are gratefully received by
Johan Hedberg
at SP Swedish National Testing and Research Institute
mailto:johan.hedberg@sp.se

Summary

Safety Requirement Specification, SRS, is a documentation for requirements stated in the safety standards e.g. the standard IEC61511 “Functional safety – Safety instrumented systems for the process industry sector”. A SRS must be developed during a project that involves Safety Instrumented Systems, SIS.

IEC 61511 specifies the general requirements for the SRS. These requirements serve as a reference to achieve functional safety for the SIS.

The SRS set-up is one of the most important activities during the life-cycle since it collects all-important information necessary to design and build functional safety in process applications.

Most companies must develop their own format of SRS, this document provides a simple guideline on how to write a SRS.

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

Table of contents

1.	Introduction	4
1.1.	SRS definition	4
1.2.	SRS objective	4
1.3.	SRS during validation or verification	4
2.	Definitions and abbreviations	5
3.	General SRS requirements	6
3.1.	Documentation	6
3.2.	SRS personnel	7
3.3.	SRS format	7
3.3.1.	SRS input information	7
4.	General requirements	9
4.1.	Safe state	9
4.2.	Proof test intervals	9
4.3.	Response time	9
4.4.	Reset	10
4.5.	Spurious trips	10
4.6.	SIS process measures and trip points	10
4.7.	SIS process output actions	10
4.8.	Manual shutdown	10
4.9.	Interfaces	11
5.	SIF specification	12
5.1.1.	Functional requirements	12
5.1.2.	Integrity requirements	12
5.2.	Software safety requirements	12
Appendix 1: General SRS guide for safety instrumented functions		13
1	Functional description	13
2	Primary actions/ sequence (for bringing the process to the defined safe state)	14
3	Secondary actions (for operational reasons)	14
4	Demand rate and Safety integrity	14
5	Triggering/Tripping	15
6	Reset/ restart	15
7	Overriding, Inhibiting and Bypassing	16
8	Spurious trips and reset failures	16
9	Final elements description	16
10	Fail-safe process output description	17
11	Fail-safe process input and trip limit description	17
12	BPCS and other systems interface	17
13	Requirements for proof test intervals	17
14	Relationship between process inputs and outputs	18
15	Operator interfaces (HMI)	18
16	Requirements for protecting the SIF from special environmental conditions	18
17	Requirements for protecting the SIF from major accidents	19
18	Consequential hazards (due to implementation of the SIF)	19

1. Introduction

In order to fulfil the requirements of the standard IEC 61511 a Safety Requirement Specification, SRS, is needed. Most companies must develop their own format of SRS, this document provides a guideline on how to write a SRS. In order to fulfil the requirements the standard IEC 61511 has to be used.

The main purpose with the safety requirement specification is to identify and present the safety requirements for the Safety Instrumented Functions.

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

1.1. SRS definition

The definition of the SRS is given in the standard IEC 61511:

“specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems”

1.2. SRS objective

The objective for the SRS is stated in the standard IEC 61511:

The SRS shall specify all requirements of safety instrumented systems, SIS, needed for detailed engineering and process safety information purposes.

The development of the SRS is one of the more important activities during the design of safety instrumented systems. If important information regarding safety issues is missing the design of the SIS may not be performed in a safe way.

1.3. SRS during validation or verification

The SRS is an important document for personnel dealing with the validation process (or validation activities). Validation personnel have often no detailed knowledge about the design of the SIS and therefore, the SRS must cover all safety aspects for the actual SIS. During the validation phase the SRS is used as a reference to check that the safety requirements are implemented in the SIS.

2. Definitions and abbreviations

Abbreviations used throughout this guide are given in table 1:

Table 1 Abbreviations

Abbreviation	Full expression
BPCS	Basic process control system
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification

Explanation of definitions [IEC 61511-1:2003].

basic process control system (BPCS)

system which responds to input signals from the 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 but which does not perform any safety instrumented functions with a claimed SIL 1

safety instrumented function (SIF)

safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function

safety integrity level (SIL)

discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest

safety instrumented system (SIS)

instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s)

safety requirements specification (SRS)

specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems

3. General SRS requirements

The requirements need to be documented during the safety planning. The SRS (3) is created after the hazard and risk analysis (1) and the allocation of safety functions to protective layers (2) in the safety life cycle according to IEC 61511-1. See figure 1.

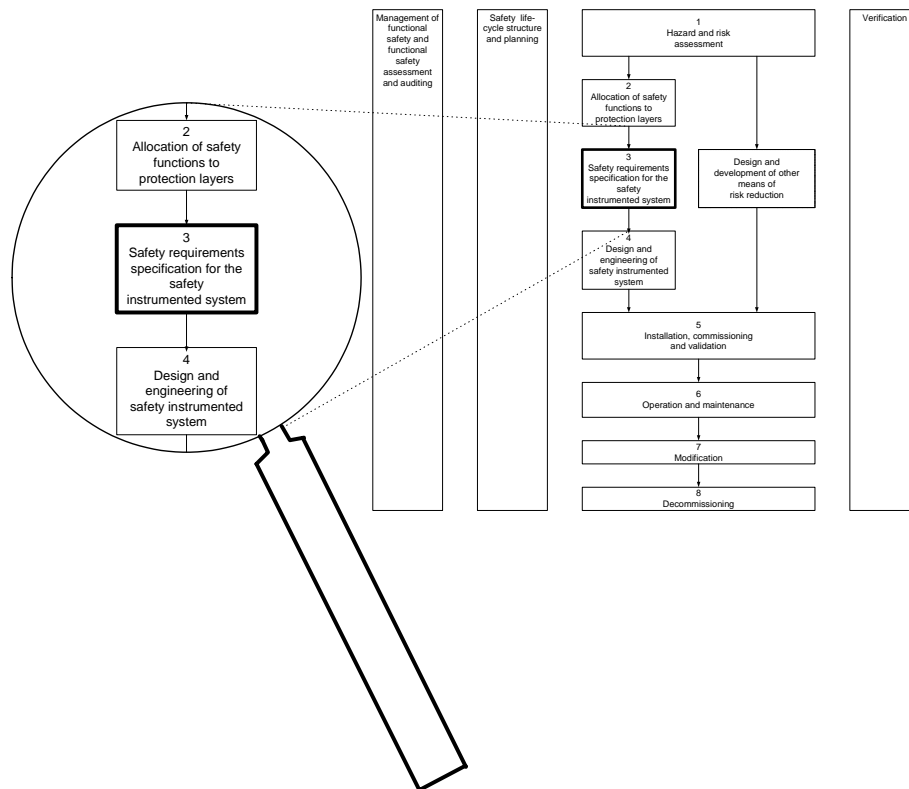


Figure 1. SIS safety life-cycle phases, IEC 61511-1:2003

The safety requirements shall be derived from the allocation of safety instrumented functions.

3.1. Documentation

IEC61511 does not specify if the SIS safety requirements specification is a single document or a collection of several documents. According to IEC61511 the requirements regarding the SRS documentation may be developed by the Hazard and Risk Assessment team or the project team.

It is important that the documentation covers all safety aspects to be addressed during the safety life-cycle. The need of documentation depends on the complexity of the application. Typically, a SIS safety requirements specification includes requirements for:

1. design and architecture
2. reliability (nuisance trip rate)
3. availability (SIL)
4. support systems
5. installation, testing and maintenance
6. hardware specification
7. software development, Security

8. human machine interface

3.2. SRS personnel

When the SRS documentation phase has started an important question may arise, who put the SRS together? The development of the SRS is an iterative process carried out by e.g. the instrument engineer in co-operation with the plant design team and any associated safety specialists.

3.3. SRS format

The requirements for the SRS format could be divided in three components:

- general requirements
- functional requirements
- safety integrity requirements

The input information and general requirements are applicable on all SIFs included in the SIS. Each SIF must fulfil specified functional requirements and integrity requirements.

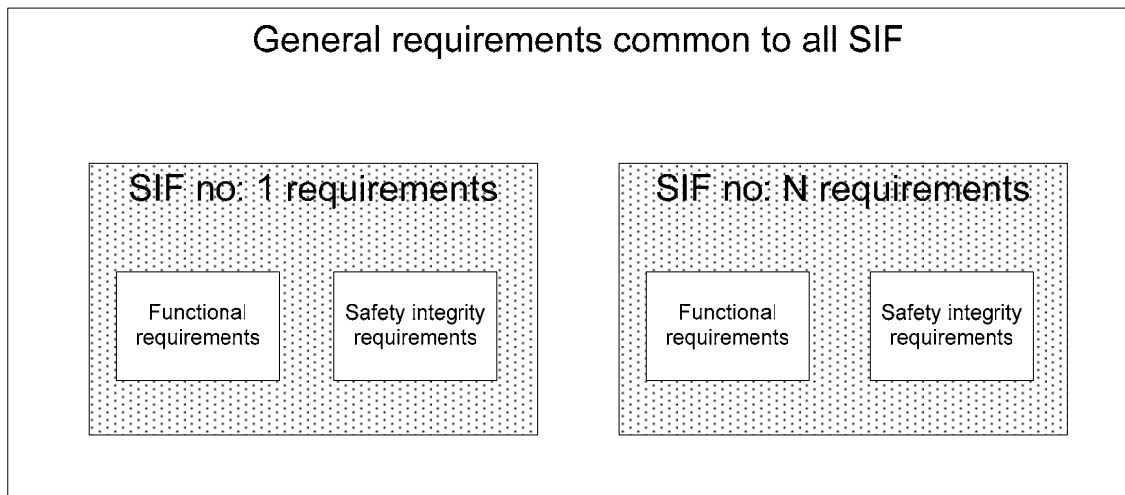


Figure 2. Requirements

3.3.1. SRS input information

The safety requirements specification is carried out after SIL selection in the safety life-cycle. In order to create a comprehensive SRS it is important that the required information is accessible for the personnel dealing with the SRS documentation. A typical set of input information includes:

- **Process information and process conditions**
The process itself shall be described in order to give detailed information regarding the process parameters to the personnel dealing with the SRS documentation. Drawings that support the description of the process itself are useful. Later on this process information is important for the personnel dealing with implementation of SIS and SIF. Specific process conditions that are important for the safety must be addressed.
- **Process and hazard report (PHA)**
The PHA report is needed. This report gives valuable information about the hazards and the hazardous events for the intended Safety Instrumented System. Important information are also the hazard frequencies and hazard consequences.

- **Required Safety Instrumented Systems**
A specification of the required Safety Instrumented Systems
- **Required Safety Instrumented Functions**
A specification of each individual Safety Instrumented Function.
- **Target SIL**
The target SIL shall be defined for each SIF.
- **Regulatory requirements**
If there are any regulatory requirements that affect the design of the SIS, the SRS shall include these requirements.
- **Common cause failures**
The possibilities of common cause failures must be taken in account. These failures could reduce or eliminate the redundant safety measures applied in the SIF or SIS. Sometimes it is tricky to find the common cause failures that affect the safety measures. The personnel involved in the design of the SIS or SIF must identify possible common cause failures.

4. General requirements

4.1. Safe state

The safe state is defined as “state of the process when safety is achieved” [IEC 61511 -1:2003]. In order to set a process to a safe state the knowledge of the process is very important. In some cases the safe state exists only if the process is continuously running, in other cases the process may have to go through a number of states before the process enters the final safe state.

Actions necessary to achieve or maintain a safe state in the event of detected fault(s) shall be described [10.3.1 IEC 61511-1:2003]. The relevant human factors that can affect the safe state shall be taken in account.

The description shall address safe state details regarding process actions needed e.g.:

- sequential shutdown
- which process valve(s) is needed to perform a specific action during the safe state. Shall the valve open or close?
- which flows should be started or stopped
- stop, start or continue operation of rotating elements (motors, pumps etc)

4.2. Proof test intervals

The proof-test interval shall be defined [10.3.1 IEC 61511-1:2003]. It is important that the proof-test interval is taken in account during the design of the process application since the proof-test interval affects the design of the application. The proof test idea is to test the function as far as possible. It is more advisable to perform a proof test is when the process (factory) is stopped.

Important activities:

- describe the proof test procedures
- investigate if additional safety measures (monitoring, redundancy etc.) has to be adapted during the proof test interval.
- investigate if human aspects (forgotten bypass etc) could affect the safety during the proof test especially if the consequences could be catastrophic if the proof test goes wrong
- specify the required proof tests during the life-cycle
- the proof test activity shall be documented (the final result of the proof test)

4.3. Response time

The response time requirements for the SIS, to bring the process to a safe state, shall be stated. [10.3.1 IEC 61511-1:2003]. Parameters that affect the response time are:

Process related

- time constants in the process itself
- dead time in process response

Control system (electrical)

- time delay in control system
- the sampling time of the controller

Other (mechanical)

- inertia

- friction
- wear

4.4. Reset

The reset after shutdown shall be defined [10.3.1 IEC 61511-1:2003].

4.5. Spurious trips

Define the maximum allowable spurious trip rate[10.3.1 IEC 61511-1:2003].

4.6. SIS process measures and trip points

Describe SIS process measurements and their trip points [10.3.1 IEC 61511-1:2003];

Information regarding the inputs to the SIS, a description of:

- every measurement circuit
- the architecture
- number of inputs
- type of input
- range of measurement
- accuracy of measurement
- trip levels

4.7. SIS process output actions

Describe SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves [10.3.1 IEC 61511-1:2003].

Information regarding the outputs from the SIS, a description of:

- every measurement circuit
- the architecture e.g. block and bleed
- the number of outputs
- type of input
- range of measurement
- trip levels
- feedback

Describe the need of feedback. What will happen if the response does not occur?

4.8. Manual shutdown

The requirements for manual shutdown shall be described [10.3.1 IEC 61511-1:2003].

Operator actions shall be defined. For example, if there is a requirement that the operator is able to manually shut down the process this action shall be defined.

Specify requirements for independence of manual shutdown devices. For example, the manual shutdown concerns only some parts of the plant. Give a detailed description of the involved parts.

Specify the location of manual shut down devices (e.g. control room, field location).

The manual shutdown command from the operator shall not create any other hazards.

4.9. Interfaces

All interfaces between SIS and any other system (including BPCS and operators) shall be described.

5. SIF specification

The requirement is quite clear in the IEC 61511-1 standard, chapter 10 part one. The SIS safety requirements specification shall include:

a description of all the safety instrumented functions necessary to achieve the required functional safety [10.3.1 IEC 61511-1:2003];

The IEC 61511-1 standard does not give precise instructions for the design of the SRS other than the SRS shall be expressed in a clear, precise, verifiable and maintainable way.

5.1.1. Functional requirements

The functional requirements for the SIF shall be described. The SRS input requirement documentation is used to give detailed information regarding functional requirements. The functional requirement describes, "How it should work":

- definition of safe state
- process inputs and their trip points
- process parameters normal operating range
- process outputs and their actions
- relationship between inputs and outputs
- selection of energize-to-trip or de-energize-to-trip
- consideration for manual shutdown
- consideration for bypasses
- action on loss of power
- response time requirements for the SIS to bring the process to a safe state
- response actions for overt fault
- operator interface requirements
- operator actions
- reset functions
- response time requirements

5.1.2. Integrity requirements

The integrity requirements are also described. The SRS includes:

- the requested SIL for each SIF
- requirements for diagnostics coverage to achieve the required SIL
- requirements for maintenance and testing to achieve the required SIL
- reliability requirements if spurious trips may be hazardous
- high or low demand mode
- requirements for proof testing
- environmental stress

5.2. Software safety requirements

The application software safety requirements shall be specified [10.3.1 IEC 61511-1:2003]. This specification shall be sufficiently detailed to allow the design and implementation to achieve the required safety integrity and to allow an assessment of functional safety [12.2.2 IEC 61511-1:2003]

Appendix 1: General SRS guide for safety instrumented functions

According to the requirements stated in the standard IEC 61511 all safety instrumented functions shall be described.

For each safety instrumented function the following guide provides information that can be used. In order to fulfil the requirements listed in the standard IEC 61511, the standard has to be used.

This appendix is a support to the Safety Requirement Specification (SRS), SIF specification form. The following chapters use the same index as the SIF specification form e.g. chapter 1 “Functional description” use the number 1 in the SIF specification form.

Page 1 in the SIF specification form deals with identification, organization and revision history.

1 Functional description

Each identified SIF shall be expressed in a general way since the description shall be easy to understand by other persons involved during the safety life-cycle. Below is a list of important issues to be taken in account during the creation of the SRS:

Functional description

A functional description shall describe why the SIF is needed [10.3.1 IEC 61511-1:2003]. The functional description of the SIF includes words such as “prevent”, “protect” or “mitigate”

Example: “The SIF protects the tank from overpressure by opening the release valve on high pressure”.

Defined safe process state

Define the safe state for each SIF [10.3.1 IEC 61511-1:2003]. The description of the safe state for the SIF describes the process action needed to prevent an accident and additional actions needed to maintain the safe state.

The description shall explain safe state details regarding needed process actions e.g.:

- if sequential shutdown is needed
- the process valve(s) needed to perform a specific action (open or close)
- which flows should be started or stopped
- stop, start or continue operation of rotating elements (motors, pumps etc)

Example: When an abnormal situation occurs (hazardous event), which measure should be taken e.g. “On low level alarm the valve V10 shall be closed”

Which measures must be taken when:

- power supply is missing
- air supply is missing
- fault/ faults occur (hardware or software)

Example: If the air supply is missing the valve has a mechanical return spring that close the valve and prevents overflow.

2 Primary actions/ sequence (for bringing the process to the defined safe state)

The actions that are needed to prevent the hazardous event shall be described [10.3.1 IEC 61511-1:2003]. The primary actions describes the measures that are necessary to bring the process to the defined safe state. A primary action could be *“open the relief valve in order to reduce too high pressure”*.

Some more examples:

- *“reduce the pressure within a specific time”*
- *“reduce the flow by 10%”*
- *“open or close the valve”*
- *“measures to prevent additional hazardous conditions”*

The threshold value of the parameter at which an action should be taken is also needed. This value will need to be outside the normal operating range and less than the value that will result in an hazardous condition. The response time of the system must also be taken into account, allowance will need to be made for the response of the system and the accuracy of measurement.

3 Secondary actions (for operational reasons)

In some cases actions for operational reasons are needed. These actions may involve other measures e.g. *“stop the inlet flow to the tank in order to eliminate overflow and give an operator alarm”*.

Some more examples;

- *actions that enables faster start up*
- *shut down of upstream or downstream units to reduce demands on other protection systems*
- *operator alarm*

4 Demand rate and Safety integrity

Specify the estimated demand rate and the target safety integrity level, SIL, for the SIF. The assumed sources of demand and demand rate on the safety instrumented function shall be specified [10.3.1 IEC 61511-1:2003].

Estimated demand sources

Sources of demand are the source of events leading to the hazardous event.

Some examples:

- *“malfunction of the inlet valve V6, valve jammed in open position, leading to over pressure”*
- *“malfunction of the temperature transmitter T2 e.g. too low indication, leading to over temperature”*

Estimated SIF demand rate:

Specify the SIF demand rate.

Low Demand, High Demand or Continuous mode of operation.

Specify if the SIF uses demand or continuous mode of operation

Demand mode:

The “need” of safety appears when a certain level is reached. In demand mode, the safety is not always dependent on the SIF

Example: “A SIF is used to protect a tank for over- pressure “when the pressure is above 5 bar the relief valve is opened”

Continuous mode:

In continuous mode of operation the safety entirely depends on the SIF. If the SIF gets some kind of failure it will result in a hazardous event.

In the process industry the SIFs are generally of demand mode type.

Established target SIL (Safety Integrity Level)

Specify the target SIL for the SIF. Describe the used SIL- selection method:

5 Triggng/Tripping

The tripping modes (automatic, manual) for the SIF and tripping detection need to be explained. The goal of this activity is to describe the conditions that affect the tripping of the SIF.

Automatic mode of tripping and tripping detection:

Explain briefly, what shall be detected? Describe the level for detection and accuracy.

Example: “High pressure in the extractor tank shall automatically open the relief valve V14. The set point for maximum pressure is 5 bar and the accuracy must be within +/- 0.2 bar”

Manual mode of tripping:

The manual trig mode of the SIF needs to be described. Are there any restrictions to activate the manual tripping? Describe the use of manual tripping during different modes.

Example: “Manual tripping, pushbuttons mounted near the control panel, shall open the relief valve. The relief valve shall automatically close when the pressure is below 1 bar. During process shutdown the manual tripping shall be disabled. In all other modes the manual tripping is needed.”

Tripping response and delay time requirements

Specify the requirements regarding response and time delay.

6 Reset/ restart

Describe the reset functions (automatic mode, manual mode)[10.3.1 IEC 61511-1:2003].

Explain the conditions that affect the reset.

Automatic reset:

Example: “The relief valve shall automatically close when the pressure is below 1 bar”

“The emergency draining shall stop when low level switch L2 is affected”

Manual reset:

Explain the conditions that affect the manual reset.

Reset response and delay time requirements

Specify response time requirements. The response time shall not affect the reset or restart.

Example: The relief valve V23 shall close within 5 seconds when the pressure in tank T22 is below 1 bar.

7 Overriding, Inhibiting and Bypassing

In some process applications the need of overrides/inhibits and bypass may appear. Describe the requirements regarding overrides, inhibits and bypasses including how they will be cleared [10.3.1 IEC 61511-1:2003].

Important issues regarding overrides, inhibits and bypass functions:

- how should the SIF be tested during normal operation
- are there any requirements regarding key lock or password
- the need of instructions

8 Spurious trips and reset failures

The SRS shall include the maximum allowable spurious trip rate [10.3.1 IEC 61511-1:2003].

Estimated conscience of nuisance trips

The maximum allowable spurious trips is an economical issue. Describe the losses. Specify the estimated consequence and the effort to restore the process to normal conditions.

Maximum allowable reset failure rate

Specify maximum allowable reset failure rate if the SIF uses automatic reset function. The reset function is important in case of preventing hazards during trip conditions e.g. avoid complete draining of the vessel.

9 Final elements description

Provide a final elements description.

Description of output actions

Give a brief explanation of the output action.

Defined fail safe position of final elements

Describe the final element and its fail-safe position (open or close)

Justification of the defined fail-safe positions

Explain why the final element has to be in the defined fail safe position.

Final elements specification

Specify the final element:

- TAG name
- type
- required number
- actuator action.

Requirements for successful operation of final elements

Specify if there are any specific requirements regarding environmental quality (e.g. temperature, humidity) of the final element.

10 Fail-safe process output description

Describe each fail- safe output.

- number of outputs
- I/O name, the name of output
- device, the connected device to the output
- trip action (energize, de-energize)

Output circuit requirements

Specify requirements regarding the output circuit safety measures:

- periodic tests
- alarm actions
- feedback

11 Fail-safe process input and trip limit description

Describe each fail-safe inputs:

- type (digital, analogue)
- number of inputs
- name
- voting
- open or closed work circuit (digital input)
- trip limit (analogue input)

Input circuit requirements

Specify requirements regarding the input circuit safety features:

- the need of wire break detection
- the need of failure detection

12 BPCS and other systems interface

Give an explanation of the BPCS and other system interface (non fail safe). Describe the digital outputs, digital inputs, analogous inputs and other output/ input signals.

13 Requirements for proof test intervals

Specify the desired proof test interval (months).

Is it possible to execute a fully proof test during operation (Yes/No). If no, is it possible to execute a partial proof test (Yes/No).

Special proof test design requirements

Specify the requirements for the proof test.

Describe the test sequence.

14 Relationship between process inputs and outputs

Give a logical description of the SIF. The description shall be easy to understand.

Triggering and reset:

- describe the architecture (1oo1, 1oo2, 2oo3 etc)
- describe the conditions that trig the SIF (inputs or other communication signals that trig the SIF)
- describe the conditions that reset the SIF (inputs or other communication signals that reset the SIF)
- provide time and delay requirements

Actuating:

- describe the actuating of the output
- provide time ad delay requirements
- forced energized or de-energized
- describe bypass modes

15 Operator interfaces (HMI)

Panels/ buttons:

Describe the use of pushbuttons, key switches, indicators etc included in the SIF.

Graphics

Provide a description of the graphics representation (picture) of the SIF. The graphic representation shall indicate:

- included components (switches, transmitters etc)
- the position of the included components
- abnormal modes
- alarms/ warnings

Generation of alarms

Describe the different failure modes that activate alarms (high temperature, low level, high pressure, abnormal conditions, detected errors, valve in a abnormal position, hardware or software errors etc.)

Generation of events

Important events shall be displayed for the operator e.g automatic or manual trig of the SIF, affected switches, bypasses, valve position.

Alarm and event logging

Provide a description of alarm and event logging.

16 Requirements for protecting the SIF from special environmental conditions

Describe the requirements regarding environmental aspects that affect the SIF (temperature, humidity etc.).

17 Requirements for protecting the SIF from major accidents

Specify the requirements that protect the SIF in case of major accidents (fire, explosion etc.):

- resisting fire in XX minutes
- the need of instrumentation air
- the need of redundancy (air supply, power supply etc.)
- safety devices (relief valves etc.)
- manual safety devices

18 Consequential hazards (due to implementation of the SIF)

Discovered consequential hazards

Describe consequential hazards that could occur e.g.:

- mechanical faults (e.g. valve jam)
- human behaviour (e.g. operation by accident, lack of knowledge)

Hazards due to concurrently occurring events:

Describe possible hazards due to concurrently occurring events e.g.:

- fire (pool fire, flash fire, jet fire)
- explosion (fireball, physical explosion, vapour cloud explosion)

Possible risk reducing measures:

Describe possible risk reducing measures e.g.

- indicators (level, pressure, temperature etc)
- monitoring of manual bypasses