A PRACTICAL APPROACH TO A

# S R S

## S A F E T Y REQUIREMENT SPECIFICATION

A PUBLICATION OF THE
DUTCH SIL PLATFORM

nen

SIL Platform

NOVEMBER 2021

# A PRACTICAL APPROACH TO A SAFETY REQUIREMENT SPECIFICATION

SIL PLATFORM
WORKING GROUP SRS

## LIST OF ABBREVIATIONS

| | |
|---|---|
| **BPCS** | Basic Process Control System |
| **FSA** | Functional Safety Assessment |
| **HAZID** | Hazard Identification (Study) |
| **HAZOP** | Hazard and Operability (Study) |
| **LOPA** | Layer of Protection Analysis |
| **MOC** | Management of Change |
| **PHA** | Process Hazard Analysis |
| **PSA** | Process Safety Analysis |
| **RRF** | Risk Reduction Factor |
| **SIL** | Safety Integrity Level |
| **SIF** | Safety Instrumented Function |
| **SIS** | Safety Instrumented System |
| **SRS** | Safety Requirement Specification |

# WHAT IS THE SIL PLATFORM?

The SIL Platform is an independent group of experienced users or adopters of the SIL philosophy, according to the IEC standards 61508 and 61511, in the Dutch process industry. The SIL Platform is linked to the Royal Dutch national standardization committee NEC 65 that follows the international work of IEC/TC65, industrial measurement, control, and automation.

At the time of release of this document, over 50 people, representing end-users, engineering companies, suppliers, manufacturers, and consultancy firms, are members of the SIL Platform. They frequently get together to share specific topics and challenges that occur when implementing SIL in applications in the process industry. One of which is the correct use of risk levels and matrices. This paper explains the adoption of a Safety Requirement Specification.

# PURPOSE OF THIS GUIDE

The SIL platform receives questions on how to deal with different safety issues, especially how to handle the 29 positions requirements of the Safety Requirement Specification as defined in the NEN-EN-IEC 61511-1:2017 further indicated as IEC 61511-1.

An SRS Working Group was formed with the task of formulating a guideline:

- Make a clear and understandable description of the requirements of the SRS (Do's and do not's).
- Indicate in a transparent way, preferably by using templates, how to deal with the various requirements as mentioned in the SRS.
- If possible, give practical examples how to deal with challenges.
- Give examples specifying advantages and disadvantages of practical tools available in the market.

Members of the SIL platform have provided technical support to the work group while writing the guide, and also reviewed the final version.

# CONTENT

# 1 GENERAL DESCRIPTION

A Safety Requirement Specification (SRS) is a document in which specific requirements of a Safety Instrumented Function (SIF) are collected.

This document describes the process of how to design, build and achieve a Safety Instrumented Function which conforms to the SRS as described in the IEC 61511-1. Safety functions which are not Safety Integrity Level (SIL) rated, shall be limited to the Basic Process Control System (BPCS) and shall not be mixed with SIL rated safety functions.

In this SRS the details of the various process conditions must be specified by quantitative terms whenever possible. These specific process conditions shall be collected by studies like PHA, PSA, HAZID, HAZOP and LOPA and filled in the SRS document / format. In addition, the SRS shall contain or refer to all functional and integrity requirements for each SIF of the Safety Instrumented System (SIS). After completion, the SRS shall be the main reference document to design, install, verify, validate and operate the system.

## 1.1 BUILDING A SAFETY REQUIREMENT SPECIFICATION

The creation of the SRS is part of the Functional Safety Management plan. Developing an SRS will give additional input to the definition of the safety related scope and costs.

When setting up an SRS it is of utmost importance to ensure that all collected information is clear and complete, there should be no ambiguity and potential for misinterpretation of the mentioned data and requirements. Especially related to the safety related applications, it is critical to use abbreviations. A list of abbreviations needs to be provided with a definition as clear and concise as possible.

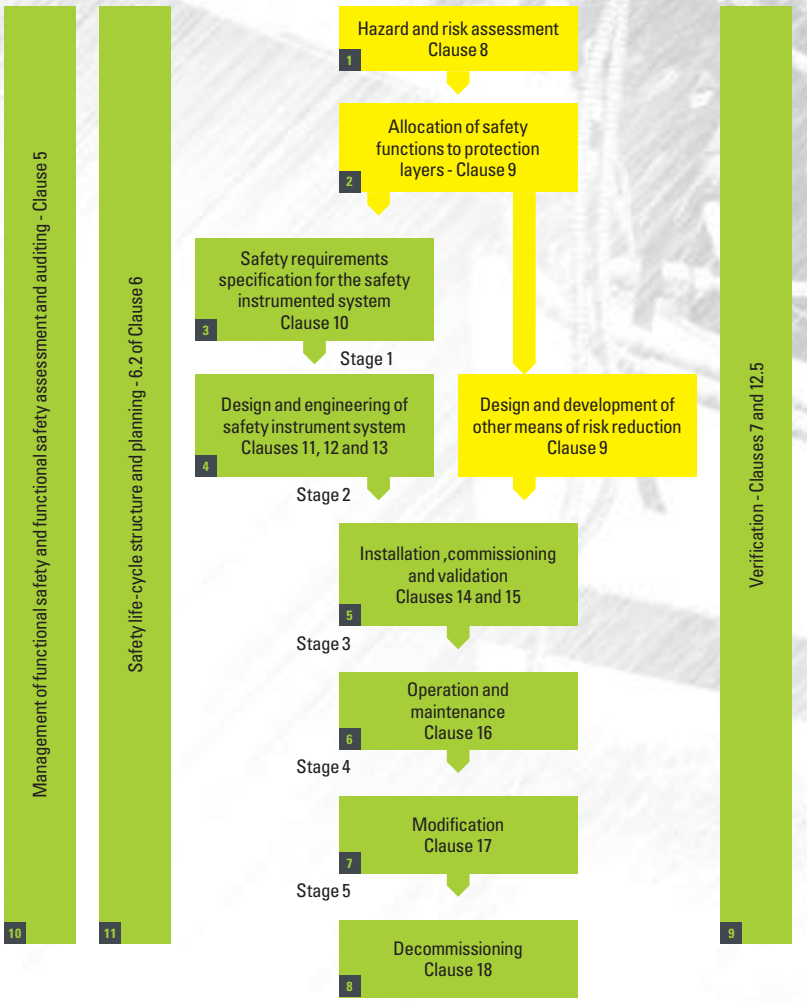
The IEC 61511-1 standard gives normative requirements when writing an SRS; the standard requires for each SIF an intend and approach of 29 specific positions. These 29 positions in the SRS documentation shall provide all information to design the SIF's and to meet the specific SIL requirements of the various safety loops (IEC 61511-1, Ed. 2.0, Section 10.3.2).

Unfortunately risks like software patching, updates, human factor, cyber security and unexpected software related failures are not included in the mentioned 29 requirements.

### An SRS is completed in two sections:

- Generic part for the SIS.
- Specific part for each SIF.

*Figure 7: SIS safety life cycle phases and FSA stages*




Typical direction of information flow

No detailed requirements given in this standard

Requirements given in this standard

NOTE 1: Stages 1 through 5 inclusive are defined in 5.2.6.1.4

NOTE 2: All references are to Part 1 unless otherwise noted.

For the various mentioned Lifecycle Phases reference is made to figure 7, a copy of SIS safety life cycle phases and FSA stages in the IEC-61511-1.

The following section discusses phases 3 to 8.

## Lifecycle Phase 3: SRS, Preliminary

The SRS is filled with the information collected from safety studies like HAZOP, HAZID, PHA and LOPA. A practical guide to check the completeness of the collected information can be found in the 29 requirements as mentioned in the IEC61511-1.

The SIS requirements shall be expressed and structured in such a way that they are

- clear, precise, verifiable, maintainable, and feasible.
- written to aid comprehension and interpretation by those who will utilize the information at any phase of the safety life cycle.

The quantified numbers shall give concise and clear information about the process, which will avoid misunderstanding and misleading interpretations. Some typical examples of information that can, and must, be clearly numerically expressed are: Required Risk Reduction Factor (RRF) and SIL, demand rates, proof-test intervals and test coverage factors, SIF response time, process safety time, process measurements and accuracy, trip point, mean time to restoration, mean repair time, etc. The SRS documentation shall contain all the functional and integrity requirements related to each and every SIF of the system. Before the design and engineering can be started, the Preliminary SRS should be subject of a review or Functional Safety Assessment (FSA) per SIF and for the entire SIS.

## Lifecycle Phase 4: SRS, Basic (Design and engineering)

In the 'design and engineering phase' the technical design is checked against the requirements as specified in the SRS. Both the requirements from the IEC standard and the SRS shall be met with proven traceable evidence. In addition, the required Systematic Capability, the planned procedures, techniques, and measures shall meet the requirements and will have been applied effectively.

## Lifecycle Phase 5: SRS, Final (Installation, commissioning and validation)

Before Installation and commissioning, a verification of the design needs to be done against the updated SRS to verify that the SIF is effective in preventing the identified hazard scenarios as part of the FSA.

## Lifecycle Phase 6: SRS, Final (Operation and maintenance)

The SRS shall be updated with the relevant information collected during the design, detailed engineering phase, and after the commissioning phase. Any change that could affect the hazard rate, demand rate, consequences or the response of equipment must be checked. Even small modifications may have an impact on the risk reduction requirements. Any additional identified hazards shall be reviewed for example by the HAZOP team and shall be solved. During the writing of the SRS the SIL should meet the requirements for the specific SIF meeting the Safety Life Cycle. The related information should be collected from various parties, like suppliers and stakeholders who could be responsible for parts of the SIF. The SIL of the SIF as described in the SRS can be maintained with the collected information.

## Lifecycle Phase 7: SRS, Temporary (MOC)

Any deviation on the process has to be checked for impact on the SRS to ensure the risk reduction specified for each SIF is not compromised. All related documentation like construction and installation drawings, engineering specifications and procedures are to be reviewed for consistency with the goal to ensure all identified risks are mitigated to a tolerable level. The SRS shall be verified at the detailed design HAZOP study where any changes or modifications to the system are documented, as part of a Management of Change (MOC), and revision control procedures. The approved SRS will now become part of the process safety information as a demonstration of the risk analysis or functional safety assessment of the system.

## Lifecycle Phase 8: SRS, Final (Decommissioning)

In the Decommissioning phase the control, the authorization and the implementation of modifications, reference to the earlier phases is made. This phase shall start before the modification starts on site. It must be clear that the planned modification has been properly planned and designed to identify possible hazards and failures that could occur during the changes. This phase will be completed by an FSA after the modification is completed and the applicable SIF has been verified and validated.

# RESPONSIBILITIES

Responsibilities over the different SRS Lifecycle Phases:

| IEC61511-1 ED2 Clause SIS | SIS Specialist | Poject Manager | Plant Manager | Operations Rep | Maint/Elec Rep | Process Safety Engineer | Process Engineer | SIS System Engineer | SIS Instrument Engineer | Construc-tion | Project SIS Contract | FS Auditor (Clause 5.2.6) | FS Assessor (Clause 5.2.6) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Clause 10 - SIS safety requirement specification (SRS) | C | A | | S | S | C | S | S | R | | | | S |

| Descriptor | Tasks |
|---|---|
| R Responsible | **Responsible (also recommender)** Those who do the work to complete the task. There is at least one role with a participation type of responsible, although others can be delegated to assist in the work required (see also Support) |
| A Accountable | **Accountable (also approver or final approving authority)** The one ultimately answerable for the correct and thorough completion of the deliverable or task, the one who ensures the prerequisites of the task are met and who delegates the work to those responsible. In other words, an accountable must sign off (approve) work that responsible provides. There must be only one accountable specified for each task or deliverable. |
| S Support | **Support** Resources allocated to responsible. Unlike consulted, who may provide input to the task, support helps complete the task. |
| C Consulted | **Consulted (sometimes consultant or counsel)** Those whose opinions are sought, typically subject-matter experts; and with whom there is two-way communication. |
| I Informed | **Informed (also informee)** Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication. |

# MANAGEMENT OF FUNCTIONAL SAFETY 1.2

| Management of Functional Safety IEC 61511-1 | Question description |
|---|---|
| **5.2.1 General**<br>The policy and strategy for achieving functional safety shall be identified together with the methods for evaluating their achievement and shall be communicated within the organization. | Is the policy and strategy for development of SRS available?<br>Is the SRS development specification in place with details the structure and requirements of the SIS? |

| Management of Functional Safety IEC 61511-1 | Question description |
|---|---|
| **5.2.2 Organization and Resources** | Are all individuals responsible for and involved with SRS, clearly identified and is the responsibility communicated formally? |

# SRS TEMPLATE 02 - A

## REQUIREMENTS AND EXPLANATIONS FOR THE SRS

The following section provides an explanation in English and Dutch on the 29 SIS safety requirements as listed in the IEC 61511-1 clause 10.3.2

| Explanatory note: | |
|---|---|
| **G** | Generic or universal requirements counts for all the SIFs and non-SIF related parts of the SIS. |
| **S** | Specific requirements are described for each individual SIF. |
| **G+S** | If both G and S are stated, special requirements also apply in addition to the general requirements. |

| No. | SIS safety requirements IEC 61511-1 clause 10.3.2 | Explanation in English. What to do. | Uitleg in het Nederlands. Wat te doen. | G/S |
|---|---|---|---|---|
| 1 | A description of all the SIF necessary to achieve the required functional safety (e.g., a cause and effect diagram, logic narrative) | ▶ Define in a concise description how each unsafe situation is recognized by the defined safety function and what actions are taken by this safety system to eliminate this threat. Record this action in a description, a cause and effect diagram or a functional logic diagram. | ▶ Geef een bondige omschrijving hoe de veiligheidsfunctie de onveilige situatie detecteert en welke acties hij neemt om het gevaar af te wenden. Leg dit vast in een beschrijving, cause and effect diagram of logische schema's. | S |
| 2 | A list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list) | ▶ Create an overview of all field equipment that are part of the safety loop, like transmitters and actuators.Identify the equipment by giving the equipment a unique tag number.<br>▶ Analogue and digital inputs: detectors (transmitters, switches), position switches (open / closed), alarms etc.<br>▶ Output: Valves, solenoids, pumps, compressors, fans, circuit breakers, relays, alarms etc. | ▶ Maak een overzicht van de sensoren en actuatoren welke deel uitmaken van de van de afzonderlijke veiligheid functies, identificeer deze objecten d.m.v. hun unieke tag code.<br>▶ Ingangen: opnemers (transmitters, schakelaars et), terugmeldingen, alarmen.<br>▶ Uitgangen: kleppen, pompen, compressoren, ventilatoren, Circuitbrekers, magneetschakelaars, alarmen etc. | S |
| 3 | Requirements to identify and take account of common cause failures | ▶ Define a summary of possible process conditions that could introduce a possible failure of one or more safety related components (common cause failures). Identify the Beta factor. For example, temperature, humidity, dirt, forming of hydrates, vibrations, overvoltage etc.<br>▶ How are these common cause failures are identified? | ▶ Geef een opsomming van mogelijke invloeden (proces condities) die de werking van twee of meerdere veiligheid componenten negatief kunnen beïnvloeden (Common cause failures). Denk hierbij aan temperatuur invloeden, vocht, vervuiling, verstopping, bevriezing, kristalliseren, polymeriseren, trillingen, brand etc.<br>▶ Hoe gaan we gemeenschappelijke fouten identificeren? | S |

| No. | SIS safety requirements IEC 61511-1 clause 10.3.2 | Explanation in English. What to do. | Uitleg in het Nederlands. Wat te doen. | G/S |
|---|---|---|---|---|
| 4 | A definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated | ▶ For each safety function a safe state must be defined to eliminate the dangerous situation for the process. (stop supply line, stop heating, stop drain, release pressure, start cooling down etc.).<br>▶ Define in detail under which conditions (clearly formulated and measured) a safe condition is achieved, and how the danger is reduced or mitigated in such way that the actual situation is acceptable.<br>▶ Define the safest situation in each phase of the process. | ▶ Definieer voor elke afzonderlijke veiligheidsfunctie de veilige staat waar het proces naar toe gebracht moet worden om een gevaarlijke situatie af te wenden. (Stop toevoer, stop verwarming, stop afvoer, druk ontlasten, drainen, koelen, killer doseren, spoelen, etc.)<br>▶ Geef aan onder welke voorwaarden (helder geformuleerd en meetbaar) de veilige proces condities zijn bereikt en hoe de gevaarlijke situatie daarmee is afgewend dan wel voldoende gemitigeerd.<br>▶ Beschrijf wat de meest veilige situatie in elke fase van het proces is. | S |
| 5 | A definition of any individually safe process states which, when occurring concurrently, create a separate hazard (e.g., overload of emergency storage, multiple relief to flare system) | ▶ Define if applicable which combination of process conditions could create a dangerous situation if these occurred at the same time. For example, overloading and activating a release at the same time.<br>▶ Describe the possible secondary impact / consequences of the action of the SIF | ▶ Geef aan, indien van toepassing, welke proces condities bij gelijktijdig optreden een gevaarlijke situatie creëren. (Te denken valt aan: Overvullen van noodopslag, gelijktijdig aanspreken van aflaten naar het afblaas systeem).<br>▶ Beschrijf wat de secundaire gevolgen kunnen zijn van het ingrijpen door de SIF. | S |
| 6 | The assumed sources of demand and demand rate on each SIF | ▶ What are the possible reasons for a demand of a safety function?<br>▶ Give an indication of the possible frequency of the demand.<br>▶ How do we define the demand rate of the event? | ▶ Wat zijn de oorzaken voor het aanspreken van de veiligheidsfunctie en wat is de verwachte frequentie van aanspreken.<br>▶ Welke bron (database) wordt gebruikt voor het bepalen van ernst van het event | S |
| 7 | Requirements relating to proof test intervals | ▶ How often can we, or should we test the system? | ▶ Hoe vaak kan of moet de functionele test worden uitgevoerd. | S |
| 8 | Requirements relating to proof test implementation | ▶ Are special requirements defined to execute the functional tests?<br>▶ What are the basic conditions to execute the test?<br>▶ What are the test conditions?<br>▶ Can or do we have to execute the test during normal operation?<br>▶ How do we interpret the test results?<br>▶ Who is approved to validate the test results?<br>▶ Is the aging time of the installed components in line with the proof test interval? | ▶ Zijn er aanvullende eisen voor het uitvoeren van de functionele test.<br>▶ Wat zijn de voorwaarden voor het uitvoeren van de functietest.<br>▶ Wat zijn de testvoorwaarden.<br>▶ Kan en of moet de test tijdens bedrijf worden uitgevoerd.<br>▶ Hoe worden de testresultaten beoordeeld.<br>▶ Wie mag de testresultaten beoordelen.<br>▶ Is de levensduur van de componenten in overeenstemming met de testinterval. | S |

| No. | SIS safety requirements IEC 61511-1 clause 10.3.2 | Explanation in English. What to do. | Uitleg in het Nederlands. Wat te doen. | G/S |
|---|---|---|---|---|
| 9 | Response time requirements to bring the process to a safe state within the process safety time; | ▶ What is the time limit to bring the process in a safe state after a demand and before the process becomes a dangerous situation? | ▶ Welke tijd is maximaal beschikbaar om het proces in de veilige positie/staat te brengen nadat het foutsignaal is gedetecteerd en voordat de gevaarlijke situatie werkelijkheid wordt. | S |
| 10 | The required SIL and mode of operation (demand/continuous) for each SIF | ▶ Define the risk reduction factor for each independent safety function and indicate the operational mode, demand or continuous.<br>▶ Demand Mode: The safety function is activated if the control system cannot control the process variables within safe process conditions.<br>▶ Continuous Mode: The safety function continuously controls the process condition; a failure in the SIF will automatically lead to an unsafe situation.<br>▶ Define the required SIL.<br>▶ Define the RRF.<br>▶ Define if the SIF has a high or low demand rate. | ▶ Geef voor elke afzonderlijke veiligheid functie aan wat de risico reducerende factor dient te zijn. Geef daarbij ook de mode van operatie aan (demand of continuous)<br>▶ Demand Mode: de veiligheid functie wordt alleen aangesproken als veilige proces condities niet langer gewaarborgd kunnen worden door de regeling.<br>▶ Continuous Mode: De veiligheid functie houdt actief (continue) het proces in de veilige condities, het falen van de veiligheid functie leidt direct tot een onveilige situatie.<br>▶ Wat is het vereiste SIL-level.<br>▶ Wat is de RRF.<br>▶ Bepaal of de SIF een Low of High demand rate heeft. | S |
| 11 | A description of SIS process measurements, range, accuracy and their trip points | ▶ Provide a description of the process measurements, the measuring principle, the measuring range, the accuracy and the switching points.<br>▶ Describe for the SIF which requirements the measuring signals need to fulfil. Consider the type of measurement, the signal, the accuracy, mode of failure when the signal becomes out of range, and the setpoints.<br>▶ Is there an automatic check of the signal condition during operations? | ▶ Geef een beschrijving van de proces metingen, het meet principe, het meetbereik, de nauwkeurigheid en de schakelpunten.<br>▶ Beschrijf voor de SIF aan welke eisen de meetsignalen moeten voldoen. Denk aan het type meting, het signaal, de nauwkeurigheid, de faalmodus bij overschrijden en of onderschrijden van het meetbereik en de setpoints.<br>▶ Is er een automatische controle van het signaal tijdens bedrijf. | S |
| 12 | A description of SIF process output actions and the criteria for successful operation, e.g., leakage rate for valves | ▶ Describe the actions to be executed by the final elements.<br>▶ Describe the requirements for proper functioning of these final elements. (Should the valve be tight shutoff, or what is the allowable leakage rate?<br>▶ Can it be tested before process start-up, during normal operations, and what are the actions when activated by trip condition? | ▶ Beschrijf de acties die door het corrigerend orgaan uitgevoerd moeten worden.<br>▶ Beschrijf wat de criteria zijn voor het correct functioneren van de actuatoren. Dient een klep helemaal lekdicht te zijn of wat is de maximaal toelaatbare lekkage?<br>▶ Denk aan testen op functie voor het opstarten van het proces, testen welke tijdens bedrijf uitgevoerd kunnen worden en de actie bij het signaleren van het event. | S |

| No. | SIS safety requirements IEC 61511-1 clause 10.3.2 | Explanation in English. What to do. | Uitleg in het Nederlands. Wat te doen. | G/S |
|---|---|---|---|---|
| 13 | The functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissive for each SIF | ▶ Provide the relation between the process input signals (sensors), the potential enabling signals, the logic with the decision to intervene and the output signals (final elements).<br>▶ Define the functionality in the logic flow schemes and in mathematical functions.<br>▶ Determine the architecture of the SIF (1oo2, 2oo3). | ▶ Geef het verband/de relatie aan tussen de proces ingangssignalen (sensoren), eventuele vrijgave-signalen, de logica met het beslismoment van ingrijpen en de uitgangssignalen (actuatoren).<br>▶ Leg dit vast in logische afloop schema's en in de wiskundige functies.<br>▶ Bepaal de architectuur voor de SIF (1oo2, 2oo3) | S |
| 14 | Requirements for manual shutdown for each SIF | ▶ Specify if the SIF also needs to be activated manually, and if so, specify the associated conditions. | ▶ Beschrijf of de SIF handmatig bediend moet kunnen worden, zo ja, aan welke voorwaarden moet dan worden voldaan. | S |
| 15 | Requirements relating to energize or de-energize to trip for each SIF | ▶ Determine for every SIF if the trip shall be energized or de-energized. | ▶ Bepaal voor elke SIF of de "trip" energized of de-energized uitgevoerd moet worden. (arbeidsstroom of ruststroom) | S |
| 16 | Requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semiautomatic, or automatic final element resets after trips) | ▶ What are the conditions to allow the reset of a SIF after tripping?<br>▶ Consider automatic reset, local manual reset or remote manual reset.<br>▶ What activities need to be executed before the reset can be applied?<br>▶ Which checks need to be executed before the reset is allowed. | ▶ Wat zijn de eisen voor het resetten van de SIF na een trip.<br>▶ Denk aan: automatische reset, lokaal handmatige reset, afstand handmatige reset.<br>▶ Welke handelingen moeten gedaan worden voordat er gereset kan worden.<br>▶ Welke controles moeten uitgevoerd worden voor de reset. | S |
| 17 | Maximum allowable spurious trip rate for each SIF | ▶ Specify how often at the most the SIF may unnecessarily initiate a trip due to a failure in the SIF itself. | ▶ Geef aan hoe vaak de veiligheidsfunctie maximaal mag ingrijpen door een fout in de SIF. | S |

Explanatory note:

| | |
|---|---|
| **G** | Generic or universal requirements counts for all the SIFs and non-SIF related parts of the SIS. |
| **S** | Specific requirements are described for each individual SIF. |
| **G+S** | If both G and S are stated, special requirements also apply in addition to the general requirements. |

| No. | SIS safety requirements IEC 61511-1 clause 10.3.2 | Explanation in English. What to do. | Uitleg in het Nederlands. Wat te doen. | G/S |
|---|---|---|---|---|
| 18 | Failure modes for each SIF and desired response of the SIS (e.g., alarms, automatic shutdown) | ▶ Specify which failures could occur in the individual SIF functions. Determine how the SIS can detect potential failures (e.g. using diagnostics).<br>▶ Specify how the SIS should respond to these detected failures (alarm or shutdown).<br>▶ Describe for each SIF what conditions will initiate a trip. Consider setpoints, accuracy out of range detection, loss of electrical power, loss of pneumatic power, loss of hydraulic power.<br>▶ Describe what actions are necessary after a trip. Consider local alarming, remote alarming, start-up of spare unit. | ▶ Geef aan welke fouten kunnen optreden in de afzonderlijke veiligheid functies.<br>▶ Bepaal hoe het veiligheidssysteem fouten kan detecteren/dient vast te stellen (bijv. d.m.v. diagnostische functies).<br>▶ Geef aan hoe het veiligheidssysteem op deze fouten moet reageren, bijvoorbeeld door middel van een alarm of automatische afschakeling. Beschrijf voor elke SIF onder welke condities de trip zal worden uitgevoerd. Denk aan setpoints, nauwkeurigheid, onder of overschrijding van het meetsignaal, uitval elektrische voeding, uitval stuurlucht, uitval hydraulisch systeem.<br>▶ Beschrijf welke acties nodig zijn na een trip. Denk aan alarmering lokaal, alarmering op afstand, opstarten reserve unit. | S |
| 19 | Any specific requirements related to the procedures for starting up and restarting the SIS | ▶ Describe the manual and automatic start-conditions or process actions, and/or procedures for a cold start, a cold re-start, a restart after shutdown during normal operations. Consider removal of products, flushing of pipelines, inerting of areas with explosive gasses (e.g. flue gasses). | ▶ Beschrijf de handmatige en automatische startvoorwaarden procesacties en of procedures voor een koude start, een koude herstart, een herstart na uitval tijdens normaal bedrijf. Denk aan afvoeren product, spoelen van product leidingen, inertiseren van explosieve gassen. (b.v. rookgassen) | G |
| 20 | All interfaces between the SIS and any other system (including the BPCS and operators) | ▶ Describe how all interfaces between the SIS and other process control systems are implemented. Consider hardwired, type of bus connection, secured internet connection. Specify also which system is the master in the communication. | ▶ Beschrijf van alle verbindingen tussen de SIS en overige besturingssystemen hoe deze zijn uitgevoerd. Denk aan hardwired, type busverbinding, via beveiligde internetverbinding. Geeft ook aan welk systeem de master is. | G |
| 21 | A description of the modes of operation of the plant and requirements relating to SIF operation within each mode | ▶ Describe the modes of the plant and the relationship / conditions that apply to the operation of the safety functions within all the defined plant modes. (Start-up, Normal Operation, Stop, Flush, Standby, Recovery, Cleaning, etc.)<br>▶ Think of difference in product, temperature, pressure, phase transition (solid, liquid, vapor, gas and critical phase).<br>▶ Describe how the SIF should respond to the different conditions. | ▶ Beschrijf de modi van de plant en de relatie/voorwaarden welke gelden voor de werking van de veiligheid functies binnen al de gedefinieerde plant modi. (Opstart, Normaal bedrijf, Stop, Spoelen, Standby, Recovery, Cleaning, etc.)<br>▶ Denk aan verschil in product, temperatuur, druk, faseovergang (vast, vloeibaar, damp, gas en kritische fase).<br>▶ Beschrijf hoe de SIF moet reageren op de verschillende condities. | S |

| No. | SIS safety requirements IEC 61511-1 clause 10.3.2 | Explanation in English. What to do. | Uitleg in het Nederlands. Wat te doen. | G/S |
|---|---|---|---|---|
| 22 | The application program safety requirements as listed in 10.3.3 | ▶ Is the software program according to an approved and structured code.<br>▶ Is the software sufficiently protected against unauthorized overwriting? | ▶ Wordt het softwareprogramma opgesteld volgens een goedgekeurde en gestructureerde code.<br>▶ Is de software voldoende beveiligd tegen onbevoegd overschrijven. | G |
| 23 | Requirements for bypasses including written procedures to be applied during the bypassed state which describe how the bypasses will be administratively controlled and then subsequently cleared | ▶ Describe the necessity of bypassing a safety function.<br>▶ State the conditions that apply to overriding a safety function and under which conditions it is allowed.<br>▶ Indicate the authorization procedure and which procedures apply when the bypass is active.<br>▶ Indicate how overriding will be registered administratively. | ▶ Beschrijf de noodzaak voor het overbruggen van een veiligheid functie.<br>▶ Geef de voorwaarden die gelden voor het overbruggen van een veiligheid functie en onder welke condities het is toegestaan.<br>▶ Geef in de autorisatieprocedure aan welke procedures gelden op het moment dat de overbrugging actief is.<br>▶ Geef aan hoe de overbrugging administratief wordt geregistreerd. | G+S |
| 24 | The specification of any action necessary to achieve or maintain a safe state of the process in the event of fault(s) being detected in the SIS, taking into account of all relevant human factors | ▶ Describe what actions must be taken if errors are detected in the safety system so that the safe state of the process can be assured.<br>▶ Describe the necessary actions to be taken by the SIF in the event of error messages reported by the SIS through automatic internal testing. | ▶ Beschrijf welke acties moeten worden genomen indien fouten in het veiligheid systeem worden gedetecteerd zodat de veilige staat van het proces kan worden geborgd.<br>▶ Beschrijf de nodige acties welke de SIF moet uitvoeren bij foutmeldingen die door automatische interne testen door de SIS worden gemeld. | G |
| 25 | The mean repair time, which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints | ▶ Indicate the expected repair time of the individual components and the total repair time including SIF test after the repair.<br>▶ Take into account driving times and availability of technicians, stock management components, service contracts. | ▶ Geef aan wat de te verwachten reparatietijd is van de afzonderlijke componenten en de totale reparatietijd inclusief SIF test na de reparatie.<br>▶ Denk aan rijtijden en beschikbaarheid van technici, voorraadbeheer van componenten en servicecontracten. | G+S |
| 26 | Identification of the dangerous combinations of output states of the SIS that need to be avoided | ▶ Determine whether dangerous process conditions can occur due to the simultaneous failure of several outputs in the safety system as a result of one failure in the SIS. This can lead to specific I / O allocation, e.g. Block & Bleed malfunctioning. | ▶ Bepaal of gevaarlijke proces condities kunnen optreden door het gelijktijdig falen van verschillende uitgangen in het veiligheid systeem als gevolg van één storing in de SIS. Dit kan leiden tot specifieke I/O allocatie, bijv. Block & Bleed | G+S |

| No. | SIS safety requirements IEC 61511-1 clause 10.3.2 | Explanation in English. What to do. | Uitleg in het Nederlands. Wat te doen. | G/S |
|---|---|---|---|---|
| 27 | Identification of the extremes of all environment conditions that are likely to be encountered by the SIS during shipping, storage, installation and operation. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (emi/rfi), shock/vibration, electrostatic discharge, electrical area clasSIFication, flooding, lightning, and other related factors | ▶ Identify the extreme values of the environmental conditions to which the safety system is exposed during the entire life cycle of the safety system (from transport to storage, installation and operation).<br>▶ The following factors are mentioned by way of example: humidity, temperature fluctuations, air pollution by nearby industry or agricultural companies, pollution by insects, contamination by sea air, EMC radiation, vibration, risk of flooding, solar radiation, etc. | ▶ Identificeer de extreme waarden van de omgevingscondities waaraan het veiligheid systeem wordt blootgesteld tijdens de gehele levenscyclus van het veiligheid systeem (van transport tot opslag, installatie en bedrijf).<br>▶ Als voorbeeld worden de volgende factoren genoemd: luchtvochtigheid, temperatuurschommelingen, vervuiling van de lucht door nabijgelegen industrie of agrarische bedrijven, vervuiling door insecten, aantasting door zeelucht, EMC-straling, trillen, overstromingsgevaar, zonnestraling etc. | G |
| 28 | Identification of normal and abnormal process operating modes for both the plant as a whole (e.g., plant start-up) and individual plant operating procedures (e.g., equipment maintenance, sensor calibration or repair). Additional SIFs may be required to support these process operating modes | ▶ Identify the normal and abnormal process conditions for the plant as a whole, but also for the individual process parts. Determine whether additional safety functions are required to support these process conditions.<br>▶ Describe the normal and incidental process situations. Think of starting up, stopping, cleaning, flushing, restarting, testing sensors and valves, etc.<br>▶ Check whether additional SIFs are needed so that the process is sufficiently safe under all circumstances. | ▶ Identificeer de normale en afwijkende proces condities voor de plant als geheel maar ook voor de individuele proces onderdelen. Bepaal of aanvullende veiligheidsfuncties nodig zijn om deze proces condities te ondersteunen.<br>▶ Beschrijf de normale en de incidentele processituaties. Denk aan opstarten, stoppen, schoonmaken, spoelen, doorstarten, testen van opnemers en afsluiters etc.<br>▶ Ga na of er nog extra SIF's nodig zijn zodat het proces onder alle omstandigheden voldoende veilig is. | G+S |
| 29 | Definition of the requirements for any SIF necessary to survive a major accident event, e.g., time required for a valve to remain operational in the event of a fire. | ▶ Describe whether additional requirements must be imposed on the SIF in the event of a possible incident.<br>▶ Consider, for example, extra facilities during a fire to continue to guarantee the operation of a valve. | ▶ Beschrijf of er nog extra eisen aan de SIF gesteld moeten worden in geval van een mogelijk incident.<br>▶ Denk bijvoorbeeld aan extra voorzieningen tijdens brand om de werking van een klep te blijven garanderen | S |

| Explanatory note: | |
|---|---|
| G | Generic or universal requirements counts for all the SIFs and non-SIF related parts of the SIS. |
| S | Specific requirements are described for each individual SIF. |
| G+S | If both G and S are stated, special requirements also apply in addition to the general requirements. |

# SRS TEMPLATE 02 - B

## SRS-TEMPLATE FOR A SPECIFIC SIF

| TAG NUMBER | SIF-12-001 | IEC ref. * |
|---|---|---|
| **SIF IDENTIFICATION** | | |
| Document | SIF-12-001-SRS.docx | |
| Revision | 0 | |
| Date of revision | 29-10-2019 | |
| Reason of revision | First issue | |
| SIF description | Overfill protection of vessel 12-B-301 | 1 |
| P&ID reference(s) | Drawings PID-XXX-12-300/301 | |
| HAZOP reference(s) | Report HAZOP-XXX-12, item YYY | |
| SIL allocation reference | Report LOPA-XXX, SIF-12-001 | |
| Other references | Cause & Effect Diagram XXX | 1, 13 |
| **HAZARD ASSESSMENT** | | |
| Hazardous event/scenario | Level control loop failure | 6 |
| Safe state of process | Block valves in supply line being closed | 4 |
| Expected demand rate | Once per 10 years | 6 |
| **PROCESS DETAILS** | | |
| Design limit to be protected | 100% level | |
| Process Safety Time (PST) | 25 seconds | 9 |
| Process lag time | 0 seconds | |
| Trip value | 95% level | 11 |
| Process state(s) to be avoided | Vessel completely empty or completely full | |
| Closing time of valves | 10 seconds to prevent water hammer | |
| Allowable leak rate of valves | Not applicable (non-TSO) | 12 |
| Other requirements | None | |
| Assumptions/calculations | Maximum filling rate of vessel is 0.2% per second | |
| **SIF SPECIFICATION** | | |
| Required SIL | 1 | 10 |
| Required Risk Reduction Factor | 20 | |
| Desired proof test interval | Once per 4 years (to be confirmed) | 7 |
| Mode of operation | Low demand | 10 |
| Max. spurious trip rate | Once per 10 years | 17 |
| Max. SIF response time | 13 seconds | 9 |
| Safety Margin time | 12 seconds | |
| Mean Time To Repair | 48 hours | 25 |
| Fouling/plugging/tracing | Clean service, winterization | |

| TAG NUMBER | SIF-12-001 | IEC ref. * |
|---|---|---|
| Energize/de-energize to trip | De-energize to trip | 15 |
| Manual shutdown required | No | 14 |
| Reset SIF after activation | Manual | 16 |
| Operational Overrides | No | |
| Maintenance Overrides | Yes | |
| Operator Interface | Trip pre-alarm | |
| Mission time (overhaul interval) | 4 years | |
| SIS lifetime | 20 years | |

| TAG NUMBER | SIF-12-001 | | | | IEC ref. * |
|---|---|---|---|---|---|
| **SIF IN/OUTPUTS** | | | | | 2 |
| **SENSORS** | **TAG** | **TYPE** | **RANGE** | **FAILURE** | 11 |
| Sensor 1 | 12-LZHH-300A | Level | 0-100 % | Low | |
| Sensor 2 | 12-LZHH-300B | Level | 0-100 % | Low | |
| Sensor 3 | 12-LZHH-300C | Level | 0-100 % | Low | |
| Voting configuration | 2oo3 | | | | |
| Bad PV handling | Voting will be reduced to 1oo2 (or 1oo1) | | | | 18, 24 |
| Common mode failure | Beta = 10% | | | | 3 |
| Proof test requirements | Test procedure XXX (with coverage factor xx%) | | | | 8 |

| LOGIC SOLVER | TAG | TYPE | SIL |
|---|---|---|---|
| | 12-SIS-001 | PLC | 3 |

| FINAL ELEMENTS | TAG | TYPE | CRITICAL | FAIL POSITION | |
|---|---|---|---|---|---|
| Final element 1 | 12-XV-301A | Block valve | Yes | Closed | |
| Final element 2 | 12-XV-301B | Block valve | Yes | Closed | |
| Final element 3 | 12-XV-302 | Block valve | No | Closed | |
| Final element 4 | 12-FIC-300 | Controller | No | Manual/closed | |
| Voting configuration | 1oo2 (critical elements only) | | | | 12 |
| Common mode failure | Beta = 10% | | | | 3 |
| Proof test requirements | Full stroke, see Test procedure XXX | | | | 8 |

# REMARKS ON SRS REQUIREMENTS

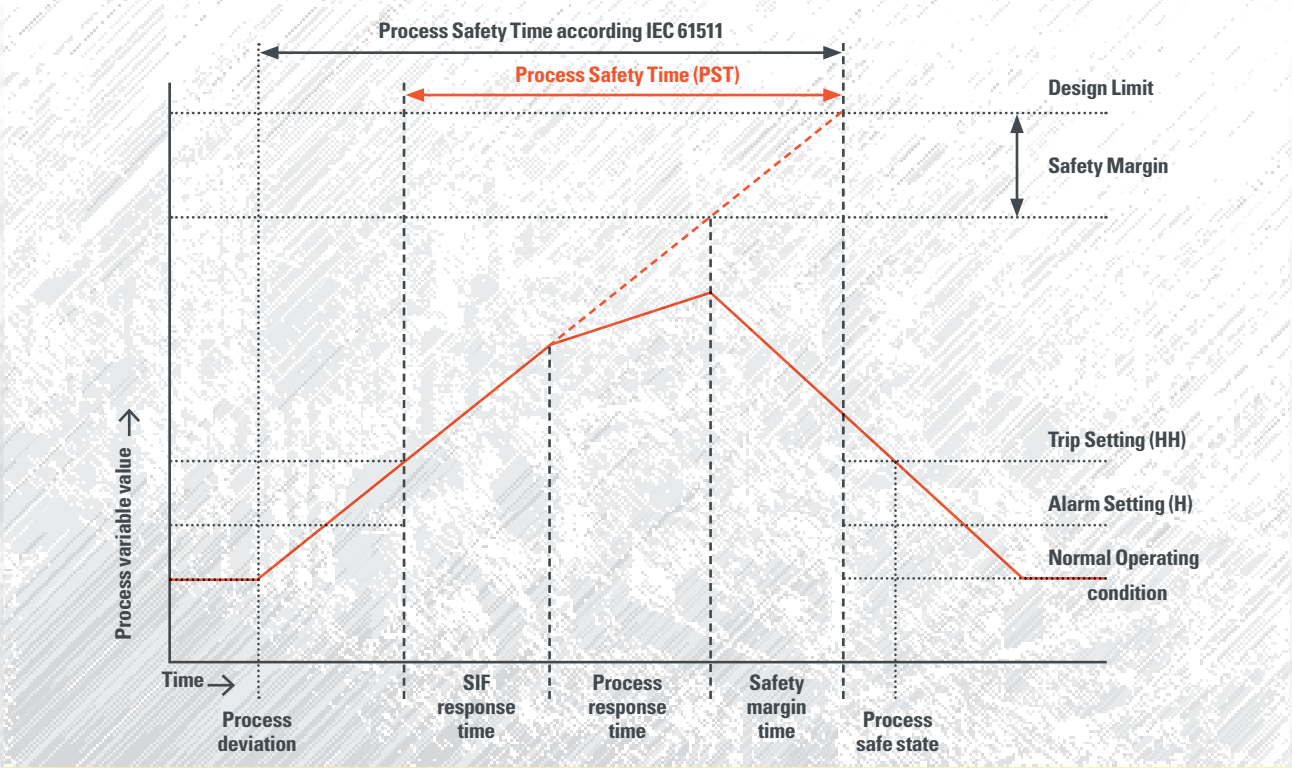
1. These SRS requirements are split in generic and specific requirements; the generic requirements are applicable for all SIFs and should be documented in a common technical specification / narrative for a process unit or plant; the specific requirements can be different for each specific SIF and are covered in the SRS template above for each individual SIF.

2. The risks of cybersecurity, human factor, software updates and unexpected failures are not covered by the 29 items listed in section 2a but should be added in the generic part of the SRS as well.

3. Examples for item 26:
   - I/O allocation for outputs (and inputs) e.g., double block and bleed valve combinations, pump and spare pump combinations, double block valves depending on voting (1oo2 or 2oo2).
   - Computer-HAZOP study to evaluate the Logic Solver redundant power supplies, fuses, busses, and fiber optic converters, etc.

4. Process Safety Time definition in the SRS:
   - Process Safety Time (PST) in the SRS is defined as the time between the trip setting and the design limit.

5. Process Safety Time definition according to IEC 61511-1:
   IEC 61511-1, section 3.2.52.1: Process safety time is defined as the time period between a failure occurring in the process or the BPCS (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed.
   - Note: This is a property of the process only. The SIF has to detect the failure and complete its action soon enough to prevent the hazardous event, while taking into account any process response time (e.g., cooling of a vessel) and a safety margin time (e.g. 25% of Process Safety Time).




*SIF respons time = sensor response time + logic solver response time + final element response time (i.e. time between receipt of signal and full closure or opening of final element).*
*=< Process Safety Time – Process Response Time – Safety Margin Time*

# EXPLANATION OF ADVANTAGES AND DISADVANTAGES OF SRS FORMATS

03

## METHODS

Several methods of documenting an SRS are available. This section compares them:

- Word format
- Excel format
- Combi of Excel / Word format
- Life cycle tools like aeShield, Dymenzions, exSILentia

## WORD FORMAT

A Word format is useful for a flat simplified list of data combined with text. Standard formats in Word should be created with fixed defined fields to fill out the 29 requirements. To get standardized data and to improve the speed of filling out a form, pull down menus / Macros could help. This might lead to quite complex Word formats.

**Advantages:**

- No additional Software license fees needed.
- Minor training needed.
- Local knowledge improving.

**Disadvantages:**

- Inconsistency of data could be a threat due to storage of the same information on different forms / platforms.
- In case of an MOC a lot of different documents might need to be updated.
- Handover of information for Design, Verification and commissioning is time consuming.
- Authorization of changing documents needs organization.

## EXCEL FORMAT

An Excel format is useful for a more structured way to handle SRS data. Standard formats in Excel should be created with fixed defined fields to fill out the 29 requirements. To get standardized data and to improve the speed of filling out a form, pull down menus / Macros could help.

**Advantages:**

- No additional Software license fees needed.
- Minor training needed.
- Local knowledge improving.

**Disadvantages:**

- Inconsistency of data could be a threat due to storage of the same information on different forms / platforms.
- In case of an MOC a lot of different documents might need to be updated.
- Handover of information for Design, Verification and commissioning is time consuming.
- Authorization of changing documents needs organization.

## COMBI OF EXCEL AND WORD FORMAT

Excel format will be filled out. By means of a macro a Word format is generated.

**Advantages:**

- No additional Software license fees needed.
- Minor training needed.
- Local knowledge improving.
- Consistency of data is improved.
- Generation of SRS Word format is less time consuming.

**Disadvantages:**

- Inconsistency of data could be a threat due to storage of the same information on different forms / platforms.
- In case of an MOC a lot of different documents might need to be updated.
- Handover of information for Design, Verification and commissioning is time consuming.
- Authorization of changing documents needs organization.

# LIFE CYCLE TOOLS

A life cycle tool could cover the complete or a part of the entire Safety Lifecycle: PSA, PHA, HAZOP, Risk Classification, allocation, LOPA, SRS, mechanical safety, instrumental safety, procedural safety, explosion safety, operate and maintain, calculation, verification and MOC.

Typical examples for lifecycle tools are aeShield, Dymenzions and exSILentia.

**Advantages:**

- Inconsistency of data can be improved by using a centralized database.
- In case of an MOC only the relevant data is changed once and will be updated automatically on the several information formats.
- Time taken for handover of information for Design, Verification, commissioning, planning and execution of testing is reduced.
- Optimization of working procedures by automatic hand over of information from PSA, HAZOP to Risk Classification, Allocation, LOPA, SRS, Design, Verification, Validation, maintenance, planning and execution of testing.
- Dashboard functionality can give real-time information on compliance.

**Disadvantages**:

- Software license fees.
- Training needed for all engineers.
- Sustainability of the software.
- Changes in the standard need to be followed.

# REFERENCES

NEN-EN-IEC 61511-1:2017, Ed. 2.0

# AUTHORS

**Leon Heemels** RMT-Solutions N.V.
**André Fijan** Fluor B.V.
**Anton Prins** NRG Consultancy & Services
**Teun Top** N.V. Nederlandse Gasunie

Proofread by Russell Spencer, Versatec Energy B.V.

# DISCLAIMER


SIL Platform