The purpose of this SAMPLE document is to show in the public domain a typical Safeguarding Requirements document developed by:

LIUTAIO

“FUNCTIONAL SAFETY SERVICES”

A document like this should be prepared according with the plant design and project scope of work. And it should include requirements for safeguarding organization, SIS-DCS integration, SRS, SIL verification, Maintenance Override Switches (MOS), etc.

This sample document is focused only in “Safety Requirements Specification” (SRS) and “SIL verification” requirements.

NOTE: these are typical requirements in the Petrochemical industry, nevertheless, the same principles can be applied to any other industry.

Table of Contents

1. Definitions

CLIENT, CUSTOMER
shall mean SIS owner, and also CONTRACTOR in the cases when a decision has to be made by CONTRACTOR.

CONTRACTOR
the Company responsible for the SIS development and installation. The term PURCHASER when referred in Codes and Standards shall also mean CONTRACTOR.

SUPPLIER
shall mean the Person, Firm, or entity to whom an SIS order is issued to provide Supplies and Services, and shall include its representatives, successors, assignees and employees. The term MANUFACTURER/SUPPLIER when referred in Codes and Standards shall also mean SUPPLIER.

Sub-SUPPLIER
shall mean the Person, Firm, or entity to whom SUPPLIER or CONTRACTOR issues the order to provide Supplies and Services required for SUPPLIER to deliver the final Supplies and Services, and shall include its representatives, successors, assignees and employees. The term SUB SUPPLIER when referred in Codes and Standards shall also mean Sub-SUPPLIER.

3rd Party Certifier (or LIUTAIO)
Service company or agency, other than SUPPLIER and Sub-SUPPLIER, which can achieve certification of SIS functionality based on the Safety Requirements Specification (SRS) and the IEC-61508 / IEC-61511 functional safety standards.

2. Document introduction

Initial project documents include: Safeguarding Philosophy and Safeguarding Specifications.

The Safeguarding Philosophy describes the main directives to organize the development of Safeguarding in the project.

The Safeguarding Specification describes the technical requirements to develop and implement the "Safety Instrumented System" (SIS), according to the plant owner technology practices and adaptions to the plant location environment conditions.

In practice both Safeguarding Philosophy and Safeguarding Specifications DO NOT include the project requirements for developing the "Safety Requirements Specification" (SRS) and SIL verification.

This sample document lists and describes the typical requirements for developing the "Safety Requirements Specification" (SRS) and SIL verification in the Petrochemical industry. Nevertheless, the same principles can be applied to any other industry.

3. References

[1] LITUATIO – Consulting and Engineering Services
0418D10SD01 Functional Safety Abbreviations

[2] LITUATIO – Consulting and Engineering Services
0418D10SD02 Functional Safety Glossary

[3] LITUATIO – Consulting and Engineering Services
0418D18SD03 SIF General Design Background - Sample Document

4. (SRS) Safety Requirements Specification

4.1 Description

The SRS is a document, or collection of documents, that records all conclusions of the analysis done during the Risk Assessment, HAZOP/PHA and LOPA reviews, and how the user wants the "Safety Instrumented Functions" (SIFs) to be designed and integrated to achieve the required functional safety.

All SIFs of "SIL 1" rating or above shall be implemented in a "Safety Instrumented System" (SIS) separate from the DCS (or BPCS). It is a project decision to implement the "SIL a" SIF (or Non-SIL SIFs) in the SIS or DCS.

NOTE: for practical implementation reasons and to avoid confusions, the SRS for "SIL a" SIFs (or not implemented in SIS) should be described in a separate SRS document.

The SRS shall fall into two types: an initial Conceptual SRS, often referred to as the "Process Safety SRS"; and a Detailed Design SRS which contains all the detailed design information.

As in any SRS, how well and how concisely information is conveyed to the designer is essential to ensure that there is no ambiguity and potential for misinterpretation of the requirements. This is especially true for safety-related process applications using SIS, where it is critical to convey the requirements in as clear and concise manner as possible; avoiding jargon and/or TLAs (Three Letter Acronyms) is another important requirement.

NOTE: However, if TLAs are used, then a list of abbreviations and a glossary of terms shall be included to assist in comprehension.

Another very important requirement is that the quality of the document **SHOULD NOT BE** a measure of the number of pages or thickness, **BUT** in the way the reader can efficiently understand and extract the information.

4.2 SRS structure

Since the SRS shall record design information for ONLY SIFs, the SRS structure shall be oriented to indicate the required information per SIF, and SIF integration requirements when they are needed.

NOTE: If the project includes general requirement for SIFs' design and implementation, that are applicable for ALL SIFs, a reference shall be made at the beginning of the SRS document, and the related below listed item shall be removed from the SRS documentation.

NOTE: The requirements to perform the "Proof Test" in the "Logic Solver" shall be included as part of project general requirement for SIFs' design and implementation.

Any SIF includes the "Initiator(s)", "Final Safety Element(s)" (FSEs) and safety logic. Nevertheless, additional component shall be included in the SIF implementation to apply good engineering practices, and to satisfy the nowadays safety standards (IEC 61508, ISA 84.00.02). Refer to "APPENDIX B" for an brief description.

Based on "APPENDIX B", the Main SRS sections per SIF shall be as follow:

1) SIF Tag number and short description.
2) Hazardous even description that the SIF is protecting from.
3) SIF related process description, operation and actions to achieve the required functional safety.
4) SIF Devices' List
5) Safety integrity targets, constraints and other requirements.
6) Additional Initiators and Input Channels description.
7) Manual shutdown requirements.
8) Startup Bypass requirements.
9) SIF Decision Logic and Calculations.
10) Interlock management requirements.
11) Additional "Final Safety Elements" (FSEs) and Output Channels description.
12) Reset function requirements, actions after shutdowns and/or before startup.
13) Operation and DCS HMI, alarms and even messages.
14) Integration with Control and operation startup
15) "Proof Test" requirements and use of MOS
16) Fault detection capabilities (Diagnostics) and required actions.
17) Maintenance provisions.
18) Adjustments and Modifications according to operation modes and/or the project phases.

NOTE: it is recommended to include ALL above sections in the SRS document, even though the section does not apply for an SRS. In this case the abbreviation N/A ("Not Applicable") shall be indicated to record that the required functionality was reviewed, and it is not needed.

4.2.1 SIF Tag number and short description.

Indicate project Tag number for SIF and short description. Example:
SIF Tag: 72-SIF-213
Short description: Steam Turbine K-1122 maximum speed protection

4.2.2 Hazardous even description that the SIF is protecting from.

Provide a short description of:

a) Normal operation description of the machine, equipment or process plant short that is affecting by the SIF.
b) Hazardous even that SIF is protecting from.
c) SIF action(s) to protect the machine, equipment or process plant when hazard happens.

This description should be no longer than half page. Less is better.

For example:
Steam Turbine K-1122 operates in the 0-100% speed range.
To protect the Steam Turbine K-1122 from over speed operation, 72-SIF-213 shall close the steam inlet safety valve 72-ESDV-213 when any of the high-speed trip initiators 72-SI-213/214 measurement reach the value of 110%.

4.2.3 SIF related process description, operation and actions to achieve the required functional safety.

This description shall include:

- Which are the used instrument to measure and monitor the SIF "Initiators".
- Indicate if a Manual Initiator is required.
- Actions to avoid Hazardous even and related instrument "Final Safety Elements" (FSE).
- Describe clearly which are the conditions of the SIF Devices in NORMAL and SAFE states.
- Additional actions, that are not required to avoid Hazardous even, but they are of benefit for the next operation steps.
- Simplified SIF sketch if it will make easier SIF design understanding.
- Short description of any other SIF facility(ies) for "Proof Test" and/or MAINTENANCE. Refer to section 4.2.17 for further details.

4.2.4 SIF Devices' List

This list shall include:

- Device project Tag number
- SIF Device Type: Initiator, Input Channel, Logic Solver, Output Channel, FSE, Support.
- Device signal I/O type: HART, 4-20mA, 24VDC, Pulse, N/A, Pneumatic, Hydraulic, etc.
- Indicate condition for NORMAL/SAFE state, like: Energize or De-Energize, Pressurize or De-Pressurize, Open or Close, etc.
- Device short description.
- Reference drawing where the Device is shown.

4.2.5 Safety integrity targets, constraints and other requirements

This section shall indicate the safety integrity requirements and constraints for the design and implementation of the SIF. It shall include:

- SIF type: Low Demand (Demand mode) or High demand (Continuous mode).
- Initiators and Trip setting values.
- "Process Safety Time" (PST) and "SIF Response Time" (SRT, or MART).
- Safety Integrity targets.
- Safety design constraints and default values.
- Other requirements.

4.2.5.1 Safety Integrity targets

The Safety Integrity targets define the required risk reduction that the SIF design/installation **MUST** satisfy in terms of probability of Failure (IEC-61508/61511), and/or reliability (ISA-84.00.01/02). In other word, this is an index to indicate the required QUALITY of the SIF design/installation.

Nowadays practice defines the integrity targets as:

CASE 1: a) Safety shall apply for LOW DEMAND or HIGH DEMAND (Continuous) systems,
b) Required SIL rating: SIL 0, SIL a, SIL 1, SIL 2, SIL 3 or SIL 4, and
c) "Maximum SIL Safety Design Limit" (MSSDL) value in the range 0-100%.
Typical MSSDL values are 70% and 80%.

CASE 2: For LOW DEMAND systems:
Required maximum SIF "Average Probability of Failure on demand" (PFDavg) value in [1/year].

For HIGH DEMAND (Continuous) systems:
Required maximum SIF "Average Frequency of dangerous failure" (PFHavg) value in [1/hour] or $[h^{-1}]$.

CASE 3: a) Safety shall apply for LOW DEMAND or HIGH DEMAND (Continuous) systems,
b) Minimum required "Risk Reduction Factor" (RRF), and
c) "Maximum SIL Safety Design Limit" (MSSDL). (see above CASE 1)

Some projects consider the nuisance trip, and in those cases, it is included a requirement to limit:

a) The "Spurious Trip Rate" (STR),
-- OR --
b) "Mean Time to Failure Spuriously" (MTTFspurious).

By default, it is understood that the SIF "Proof Test Period" (TI) shall be optimized. It means, to calculate the maximum TI value(s) for SIF's devices to satisfy "Safety Integrity Targets".

4.2.5.2 Safety design constraints and default values

The safety design times **MUST** be consistent with the "Safety integrity targets, constraints and other requirements".

For example:

Example 1: In the "Oil & Gas" industry sometimes to perform a "Proof Test" it is required a momentary significant production reduction, near to a partial or total production shutdown. So, "Low Demand" SIF design is preferred.

"Low Demand" means that a SIF demand may occur at least every year. So in practice, it shall be required to design SIF for a TI of 4-6 months at least. It SHALL NOT be accepted a "Proof Test Period" (TI) of every week, or something like that.

Example 2: In the massive production industry, for example a "Soft Drink Factory", it may be required to shut down a production train every month for MAINTENANCE. In this case the safety requirement is for a High demand (Continuous mode) SIF, so a "Proof Test Period" (TI) lesser than one month can be acceptable, BUT greater than one month has no sense.

The times to specify are: MTTR, TD, MRT, TI, SLf and time constraints.

These times have a direct impact on the MAINTENANE effort to keep the SIF installation in good shape. This is the reason these times are sometimes named "MAINTENANCE times". Table 1 show a typical "MAINTENANCE times" requirement for a project.

Table 1 – Typical constraint and default "MAINTENANCE times"

No.	Description	Abbreviation	Default value	Constraint value	Remark
1	Proof Test Period	TI	6 months	≥ 4 months	Initiators
				≥ 4 months	SOVs
				≥ 6 months	Safety valves
2	Service Life	SLf	24 months	≥ 12 months	
3	Mean Time To Restoration	MTTR	72 hours	≥ 24 hours	
4	Proof Test Duration	TD	4 hours	≥ 1 hour	
5	Mean Repair Time	MRT	24 hours	≥ 8 hours	

Other constraints can include:

1) Regarding to calculation of Beta values for "Common Cause Failure" (CCF):

a) For any "**Decision Logic**" or "**Safety Channel Architecture**" (SCA) equal to "XooN(D)" (N>X and N>1), the CCF effect **MUST BE** calculated. ZERO(0.0) values **ARE NOT** accepted for CCF effect and respective "Beta" (β) values.

CCF effect is ZERO(0.0) ONLY for 1oo1D and "NooN" logic.

b) Default methodology to calculate Beta values for "Common Cause Failure" (CCF) effect shall be IEC-61508-6, Annex D.

c) **Rule to handle Devices Diversity for CCF effect calculation:**

When devices diversity is applied, and those elements are used in parallel safety channels, the project PRINCIPAL (or Customer) shall decide the rule to apply to calculate CCF effect.

"Diversity" can appear from the use of devices from different manufacturer, or devices of different technologies.

d) To estimate the CCF effect the "Geometric Average" is the default method to estimate the combined failure rates from devices.

In a group of devices to consider for CCF effect calculation, when one or some of them has "Dangerous" failure rate (λ_{DD}/LdDD, (λ_{DU}/LdDU) value(s) equal to ZERO(0.0) and other devices **DO NOT**, then:

d.1) The "Geometric Average" shall be applied ONLY to the failure rate values other than ZERO(0.0), or

d.2) The "Maximum" value of the Failure rates set to consider shall be applied.

NOTE: "SIL verification" results with application of one of the above points "d.1" or "d.2", **MAY NOT** be the same ones:

- Requirement "d.1" is balanced among the SIF devices.
- Requirement "d.2" is focused in higher level of safety.

e) When devices with different "Proof Test Periods" (TI) are involved in the same "Proof Test", the CCF effect calculation **MUST BE** done to force the CCF's TI to meet each device's TI value.

4.2.5.3 Other requirements

Other possible requirements for this SIL verification can be:

1) "SIL verification" calculations **MUST** consider individual failures of all devices, as well as all possible combined failures, that will make the "Safe Instrumented Function" (SIF) to fail on demand.

2) By default, "SIL verification" shall consider "Fault Detection Capabilities" (Diagnostics) of the indicated SRS SIF devices.

3) Calculate the SIF's "STRavg" (and "MTTRspurious").

NOTE: this requirement could be required per each SIF operation mode or condition

For "Conceptual SRS" (final design data and installation details **ARE NOT** available):

4) If target SIL rating is no satisfied, propose possible actions/solutions to improve the SIF design.

5) The indicate methodology in above section 4.2.5.2 point "1.b" shall be used to calculate Beta values for the following cases:

- SIF **simple** Design/Installation quality is representative of high Beta values (or Worst values).
- SIF **enhanced** Design/Installation quality is representative of low Beta values (or best values).

And, "SIL verification" shall be developed by calculating and reporting "Beta" values (β, β_D) corresponding to BOTH the **Simple** (Greater CCF effect) and the **Enhanced** (Lower CCF effect) SIF's Design/Installation cases.

6) Verify SIL rating in the cases of SIF's **simple** and **enhanced** implementation quality, but with **NO** Maintenance effect (MTTR, TD, MRT all equal to 0.0 hours).

7) Verify SIL rating in the same condition as described in above point No.6), but including Maintenance effect (MTTR, MRT).

8) Verify if application SIF Devices' "Diagnostic" in the design can improve "PFDavg" and "STRavg".

For "Detail Design SRS" (final design data and installation details are available):

9) If target SIL rating is no satisfied, propose possible actions/solutions to solve the problem.

10) The indicate methodology in above point No.1) shall be used to calculate precise Beta values for the related SIF.

11) Verify SIL rating for the SIF's implementation, but with NO Maintenance effect (MTTR, TD, MRT all equal to 0.0 hours).

12) Verify SIL rating in the same condition as described in above point No.11), but including Maintenance effect (MTTR, MRT).

13) Clearly indicate benefits of SIF devices "Diagnostic", and consequences of losing SIF devices "Diagnostic" in the verified SIF SIL rating.

4.2.6 Additional Initiators and Input Channels description

Include additional detailed information that is required to complete the "Initiators and Input Channels description".

4.2.7 Manual shutdown requirement (Manual Initiator)

A "Manual Initiator" applies ONLY when the SIF's "Safety Response Time" (SRT) is long enough to allow time to the Console Operator to react to manually initiate the SIF action on time to avoid the related SIF's Hazard.

"Manual Initiator" function is normally provided to high-level safety trip in the plant safety hierarchy ONLY, **BUT** it may be provided lower plant safety hierarchy levels if SRT is low and the "Manual Initiator" is a design requirement.

NO "Manual Initiator" shall be provided for lower plant safety hierarchy levels if SIF's SRT is lesser than 5 min, ELSE the below description can be applied.

A "Manual Initiator" push button shall be included as an independent input to the "SIF Decision Logic", as indicated in the Figure 2, "APPENDIX B".

A "Manual Initiator" can be implemented via a Soft-button or Hard-button. The minimum requirements SHALL BE:

- The button **MUST COMMAND** a two states Boolean signal to set the SIF in the SAFE or NORMAL states.

- For Hard-Buttons, to use Push Button with Light SPDT Push-to-make-and-Remain to initiate TRIP. Console Operator SHALL push button again to cancel manual TRIP command.

  By default, the Hard-Button NORMAL state shall correspond with the button position to keep the circuit in the "Energized" condition.
- For Soft-Buttons, HMI push button with confirmation message.

4.2.8 Startup Bypass requirements

Describe the instrument signals, limit values and process conditions that **MUST BE** satisfied to allow the Machine, Equipment or process plant to startup.

For all those instrument signals that are also SIF "Initiators", describe:

a) Logic that will bypass SIF "Initiators".
b) Criteria or process condition (setting limits) to declare bypass over and to disable "Startup Bypass"
c) Indicate if a "Manual", "Automatic", or both functionalities will be implemented.
d) Indicate to use Soft-buttons, Hard-buttons, or both.

4.2.9 SIF Decision Logic and Calculations

The "SIF Decision Logic" includes the criteria to initiate TRIP and set the FSE in the SAFE state. This Logic implementation can include:

- Single "Initiator" input,
- Several "Initiator" inputs with "Decision Logic",
- Calculation to identify if the selected process variables are in the condition to request TRIP. Example: compressor surge.
- Manual Initiator (if it applies).
- Higher priority SIF or TRIP command initiation.

4.2.10 Interlock management requirements

An Interlock is equivalent to some process variables or other logic/equipment conditions that **MUST** be satisfied to avoid undesirable states in the normal operation of an associated machine, equipment or process plant, and such conditions MUST be satisfied before Startup and/or the FSE is set in NORMAL state.

Indicate Interlock's related process variables, other logic/equipment conditions and criterion to determine if the Interlock is Enabled or Disabled.

4.2.11 Additional "Final Safety Elements" (FSEs) and Output Channels description

Include additional detailed information that is required to complete the "FSE and Output Channels description".

4.2.12 Reset function requirements, actions after shutdowns and/or before startup

Indicate the Reset requirements. These ones can include or not:

- "Reset Logic" or "Local Reset", or both.
- Automatic, or Manual "Reset Logic".
- "Reset Command" location": Field, or Panel, or Operator Console, or combination.
- Reset function condition after SIS power up.

4.2.13 Operation and DCS HMI, alarms and even messages

Refer to "APPENDIX A" for DCS-SIS HMI typical tie-ins per SIF.

Indicate if the HMI shall include a panel with buttons @ control room, or @ Field, or @ DCS-SIS, or a combination.

An Alarm is a message that requires the Console Operator attention and subsequence actions.

NOTE: an ALARM can be implemented ONLY if by design enough time is foreseen to allow the Console Operator to react and manually initiate a corrective action in DCS or SIS. **ELSE NO ALARM IS REQUIRED**, because it is useless in practice.

A "Trip Pre-Alarm" follows the same requirements of an ALARM.

An ALARM can be implemented in DCS, in SIS, or both. Project directive or philosophy shall indicate which is the preferred location for ALARMs' implementation.

There is a difference between ALARM implementation and ALARM log:

- ALARM implementation refers to the location (DCS, SIS, other) where the logic to identify the ALARM is locate.
- ALARM log refers to the location where the alarm is notified and recorded. Normally DCS.

An event messages LOG shall be implemented for further review in case investigation/review of operation situations or "Near miss".

List all the messages/alarms related to the described SIF.

4.2.14 Integration with Control and operation startup

This section shall include:

1) Automatic actions on related control loops and "Final Control Elements" (FCE) when the SIF is set in SAFE state.
2) Operation procedure, sequence logic, operation actions and requirements to allow Console Operator to move the SIF from SAFE to NORMAL state.
3) Operation procedure, sequence logic and operation actions to set associated control loops back in normal operation.

Refer to below section 4.2.17, for integration requirements and provisions for MAINTENANCE of ALL SIF devices.

4.2.15 "Proof Test" requirements and use of MOS

Indicate to which SIF's Devices "Proof Test" can be applied, or not.

For each SIF's Device, or group of SIF devices, where "Proof Test" applies, indicate:

1) Related MOS tag number.
2) Procedure to Lock/Unlock the "Proof Test".
3) "Proof Test" target, or Fail/Success completion criterion.
4) Description of "Proof Test Logic" implementation: in DCS, in SIS, in external facility, or hybrid.
5) Associated procedure to execute "Proof Test" in the Field (if any).
6) Procedure to operate the "Proof Test".
7) Can the "Proof Test" be manually declared UNSUCCESSFUL?
8) "Proof Test" actions in case of "FAIL SAFE" test completion status.

Each "Proof Test" shall include a "Completion status", as described below:

- SUCCESSFUL Fail/Success completion criterion was met, or "Proof Test" target was reached.
- UNSUCCESSFUL Opposite result as SUCCESSFUL.
- FAIL SAFE "Proof Test" was interrupted by a SIF demand.

If there is a SIF demand while a "Proof Test" is in progress:

a) All automatic "Proof Test" actions **MUST** stop, and "Proof Test" actions for "FAIL SAFE" **MUST** apply.
b) The "Final Safety Element" (FSE) that is involved in the test (or being tested) **MUST BE** set in SAFE state.
c) The "Proof Test" completion status is declared as "FAIL SAFE",
d) In case of "Proof Test" associated procedure in the field, an indication SHALL BE given in DCS to Console Operator to communicate field personnel to apply "FAIL SAFE" procedure.

In some cases, a "MOS Logic" may not be required.

When "MOS Logic" is required, for each "Proof Test Logic" a "MOS Logic" shall be implemented, regardless if full, or just a portion, of "Proof Test Logic" is implemented in the "Logic Solver".

If it is specified to include a SIF "Manual Initiator" ONLY when SIF MOS is active, then a soft-button shall be provided to allow Console Operator to manually initiate a SIF demand, regardless if that action can avoid the Hazard the SIF is protecting from, or not.

ALL SAFETY and PERMISSION procedures **MUST BE** completed and approved before operating any MOS and performing the related "Proof Test".

Refer to below section 4.2.17 for more information about MOS management and MAINTENANCE activities.

4.2.15.1 "Proof Test" LOG requirements

DCS shall be able to record as a minimum the following data per "Proof Test":

a) Tested Device (or Devices if an "Input/Output/Both Channel(s)" is tested) Tag ID.
b) MOS activation time.
c) "Proof Test" start time.
d) "Proof Test" completion time, or time when the tested Device (or Devices if an "Input/Output/Both Channel(s)" is tested) reached the SAFE state.
e) "Proof Test" completion status: SUCCESSFUL, UNSUCCESSFUL or "FAIL SAFE"
f) Was "Proof Test" manually declared as UNSUCCESSFUL?
g) MOS de-activation time.
h) Was MOS de-activated before MTTR?
i) Was the MOS in "Activated" state operation time extended for MRT additional time?
j) Was MOS de-activated before MRT?

"Proof Test" implementation shall include a "Proof Test Record" (PTR).

PTR is a dedicated view, or report, that lists ALL performed "Proof Test" sessions in a SIF, equipment, unit or plant. Console Operator shall be able to review the list of performed "Proof Test" sessions and to select any of them for further review per "Proof Test" basis.

DCS shall include a simple HMI to allow Console Operator to locate a PTR item of a selected SIF. If several "Proof Tests" are implemented to test several SIF devices in the same SIF, PTR items **MUST BE** populated and addressed accordingly.

Any item in PTR shall include:

1) "Static Data Section" (SDS), and
2) "Sequential Action Log section" (SALS).

The "Static data section" (SDS) is used to identify the "Proof Test". It shall include "Proof Test" tag, related SIF tag, a list of involved SIF elements, description of "Proof Test" Fail/Successful completion criteria, Start/End date/time, etc.

The "Sequential Action Log Section" (SALS) shall show in a chronological order all changes that can be monitored by DCS, or manually recorded in DCS. For example, any of the "a to j" above listed items.

DCS shall keep PTR items for the last three(3) performed "Proof Test" on the same SIF.

Any other "Proof Test" data record requirement shall be performed manually by operation personnel.

4.2.15.2 Input Channel "Proof Test"

For the 1oo1 "Decision Logic", the "Input Proof Test Logic" can be applied only when all the following conditions are satisfied:

a) A control measurement of the same 1oo1 SIF "Initiator" exist, and this one can be used by the Console Operator to monitor the process safeguarding while the "Input MOS" is in the Activated state.

b) A Manual initiator push button is implemented to allow Console Operator to manually initiate the SIF action.

c) The SIF's "Process Safety Time" (PST) is long enough to allow time to the Console Operator to react to manually initiate the SIF action on time to avoid the related SIF's Hazard.

For the XooN "Decision Logic" (X≤N), the "Input Proof Test Logic" **MUST BE** applied to each "Initiator".

The implementation of an "Input Proof Test" shall include:

- For an XooN "Decision Logic", the physical means to isolate the related "Initiator" from the SIF for independent test purposes.
- For an 1oo1 "Decision Logic", the physical means may not be required. "Initiator" isolation is handled by the "Input MOS". See next section 4.2.15.2.1.

By default, is assumed that "Proof Test" applies to each "Initiator" and the respective devices in the "Input Channel" at the same "Proof Test Period" and frequency. If this statement is FALSE, then for devices with different "Proof Test Period" and frequency:

1) Additional "Proof Test Logic" shall be implemented.
2) Additional physical means may be required to isolate the device test from the other devices.

"Proof Test Logic" functionality can be implemented in SIS, DCS, both, or in an external installation. And this logic depends on the Device type where the "Proof Test" is applied.

The MOS implementation for each input of an XooN "Decision Logic" (X<=N) SHALL set in SAFE state the related "Input Proof Test Logic" output when the MOS is activated. In addition, the related "Decision Logic" (within the "SIF Decision Logic") shall be degraded. For example:

- From 2oo2 to: 1oo2,
- From 2oo3 to: 2oo2 or 1oo2 (project decision), etc.

The MOS implementation for 1oo1 "Decision Logic" **SHALL NOT** set the "Input Channel" in SAFE state. It **MUST** remain in NORMAL state when the "Input Channel" MOS is activated. The 1oo1 "Decision Logic" output **WILL BE** set in SAFE state by the "Proof Test Logic" when the "Proof Test" is in progress.

4.2.15.2.1 Input MOS integration with Diagnostic capabilities

If the "Initiator", "Input Channel" and "Logic Solver" can handle Diagnostics, in order to identify "Detected Failures", the SIF implementation can take advantage of these capabilities in order to:

a) Warn Console Operator when a "Detected Failure" (Safe or Dangerous) occurs.
b) Avoid "Spurious Trips" when a "Safe Detected Failure" appears.
c) When it is required, make "Dangerous Detected Failures" to initiate a TRIP.
d) Improve the SIL rating and "Spurious Trip Rate" of the "Safety Instrumented Function" (SIF).

If it is required to implement 1oo1D and/or (N-1)ooND "Decision Logic" in the "Logic Solver", the related "Input Channel" MOS (or "Initiator") can be activated automatically. This MOS AUTOMATIC activation:

1) Shall be accounted as one of the activated MOS in the "MOS Group",
2) Can override the rule of maximum amount of activated MOS in the "MOS Group", and

3) It shall generate a warning for Console Operator.

In practice the 1oo1ND and (N-1)ooND "Decision Logic" can be performed ONLY by the "Logic Solver".

Nevertheless, when any of these "Decision Logics" is implemented in the "Logic Solver", the 1oo1D functionality can be inherited to other devices in the "Input Channel", if those devices can notify to the "Logic Solver" when a "Detected Failure" has been occurred. This is the way the above 1 to 3 benefits can be extended to the other Devices in the "Input Channel".

NAMUR NE 43 or "NAMUR sensor" (EN-60947-5-6:2000 and IEC-60947-5-6:1999) are the simplest ways to allow an "Initiators" to communicate to "Logic Solver" when a "Detected Failure" has been occurred. ONLY in this case the single "Initiator" (or Device) can perform the 1oo1D "Decision Logic".

4.2.15.3 Output channel "Proof Test"

"Proof Test" on the "Output Channel", or "Output Proof Test Logic" can be implemented on SIS, DCS, both or as a separate testing facility. The designed implementation depends on the type of each Device in the "Output Channel".

When the "Output Proof Test" is in progress, if the "Output Proof Test Logic" input changes from NORMAL to SAFE state and remains, the logic output **MUST CHANGE** to SAFE state as well, regardless in which state or condition the "Output Proof Test" progress is.

In Figure 2, "APPENDIX B", it is shown that the "Output Proof Test Logic" is located downstream the "Reset Logic". This means that a "Proof Test" can be performed even after a TRIP (or before Startup) when the SIF is setting the FSE in the SAFE state. This is done in this way because for some designs just before startup is the right time to perform "Proof Test" in the "Output Channels".

NOTE: it is the Operation responsibility to authorize, or not, the activity to perform "Proof Test" in the "Output Channel".

If "Output Proof Test Logic" is implemented for a Device and this logic is partially or completely implemented in the "Logic Solver", then "Output MOS" implementation is a **MUST**, else "Output MOS" is not required.

Regardless of the location(s) where, and how, an "Output Proof Test Logic" is implemented, if the "Logic Solver" sets the "Final Safety Element" (FSE) in SAFE state, this action MUST BE executed, regardless the "Proof Test" in progress, and the related MOS condition.

4.2.16 Fault detection capabilities (Diagnostics) and required actions

The following statement apply for both "Safe Detected Failures" and "Dangerous Detected Failures".

The benefits of considering the "Fault detection capabilities" (Diagnostics) capabilities in the SIF design are:

- In 1oo1D "Decision Logic", a "Safe Detected Failure" **SHALL NOT** create a "Spurious TRIP", because the SIF design will be able to notify Console Operator, and delay TRIP action for MTTR time.

- In (N-1)ooND "Decision Logic", a "Safe Detected Failure" **SHALL NOT** create a "Spurious TRIP", because the SIF design MUST request to degrade the "Decision Logic" to (N-2)ooND, and the Machine, Equipment or process plant will continue protected during operation.

In the above listed cases, the "Safeguarding requirements" can indicate other choices for applying TRIP after MTTR, a shorter time, or NOT.

This section shall indicate the "Fault detection capabilities" (Diagnostics) scope of work for the project. This requirement can be specified in many ways. Following are listed some possible requirements:

a) "Fault Detection capabilities" (Diagnostics) capabilities **SHALL NOT** be considered in SRS.
b) "Fault Detection capabilities" (Diagnostics) capabilities shall be considered in "Logic Solver" ONLY.
c) "Fault Detection capabilities" (Diagnostics) capabilities shall be considered in "Initiator", Input Channels", and "Logic Solver", BUT not in "Output Channels" and "FSE(s).
d) The initial Conceptual SRS **MAY NOT** include the Devices' "Fault Detection capabilities" (Diagnostics) VENDOR information, **BUT** it shall include a revision to identify and to quantify benefits for:
    - Finalizing "Fault Detection capabilities" (Diagnostics) requirements in the Detailed Design SRS, and/or
    - Improve selection of the SIF's Devices.

NOTE: By default, a "Dangerous Detected Failure" **SHALL NOT** initiate a TRIP, BUT the "Safeguarding requirements" could indicate if this kind of failure shall be managed in the same way (or different) as "Safe Detected Failures" after considering "Fault detection capabilities" (Diagnostics) in the SIF design.

4.2.17 Maintenance provisions

This section shall indicate:

1) Which is (are) the procedure(s) to apply MAINTENANCE to each SIF Device or group of them.
2) Per Device:
    - Can MAINTENANCE be applied while the SIF related device(s) in the machine, Equipment and/or process plant is in normal operation?
    - How to apply MAINTENANCE while SIF device is normal operation, without compromising the Machine, Equipment or process plant safety.

3) MOS management and MAINTENANCE activities.
4) OOS management and MAINTENANCE activities.

4.2.17.1 MOS management and MAINTENANCE activities.

The MAINTENANCE activities **MUST NOT** last longer than the MTTR and/or MRT maintenance times.

When a MOS is activated, a timer shall start to account the expended time in "Proof Test" activity.

Before “Proof Test” execution, the maximum time to allow a MOS to remain in the “Activated” state **MUST BE** equal or lesser than the MTTR (Mean Time To Restoration) of the associated SIF.

If the MOS remains in the “Activated” state for more than MTTR time and before “Proof Test” execution, the MOS shall be deactivated AUTOMATICALLY.

After “Proof Test” execution and if the “Proof Test” completion status was UNSUCCESSFUL, the MOS time in “Activated” state can be extended by MRT time if the tested device can be repaired. SIF implementation shall provide the measure to allow Console Operator to extend the MOS allowed time.

After the MOS allows time was extended, if the MOS remains in the “Activated” state for more than MRT time, the MOS shall be deactivated AUTOMATICALLY.

If more time than MTTR+MRT is requires for MAINTENANCE activities, MAINTENANCE personnel shall notify Console Operator to activate the related “Out Of Service” (OOS) state. Refer to below section 4.2.17.2 for more information.

ALL SAFETY and PERMISSION procedures **MUST BE** completed and approved before operating any OOS and performing the related MAINTENANCE activities.

4.2.17.2 OOS management and MAINTENANCE activities.

When MAINTENANCE can be applied to a SIF device(s) while the SIF protected machine, Equipment and/or process plant is in normal operation, then an “Out Of Service” (OOS) function shall apply.
Every OOS function has an associated tag number.

MAINTENANCE activities for a SIF device can be required:

a) According to scheduled MAINTENANCE, or
b) As a consequence of an UNSUCCESSFUL “Proof Test” when MTTR+MRT times are not enough for MAINTENANCE activities.

Some manual actions in the field and control room may be required before activation an OOS tag.

Activation of a SIF device(s) OOS tag:

1) Requires SAFETY and PERMISSION procedures already completed and approved.
2) MAY initiate automatic actions in SIS to set the affected SIF related devices in the SAFE state.
3) When the related OOS automatic actions are completed, the related MOS shall be deactivated.

After MAINTENANCE activities finish, and SIF device(s) are ready to be used in operation, the procedure to put those device(s) in service may require the execution of normal machine, equipment or process plant startup procedure.

The procedure to put the SIF device(s) back in normal operation will dictate when the related OSS tag is deactivated.

4.2.18 Adjustments and Modifications according to operation modes and/or the project phases

The Machine, Equipment or process plant that the SIF is protecting can:

- Work in several operation modes, or
- The project development can consider different production stages for the production life.

If any of the above listed situation occurs, the related impact and resolution(s) in the SIF **MUST BE** described in this section.

5. SIL Verification process

5.1 Description

The "SIL verification" is an activity that shall review the SIF design (Conceptual SRS), or final implementation (Detailed Design SRS); and will determine if such SIF design/implementation satisfies, or NOT, the SIF's "Safety integrity targets, constraints and other requirements" (see above section 4.2.5).

By default, the "SIL verification" shall consider:

a) To determine the optimum SIF's "Proof Test Period" (TI).

NOTE: the same or different TI values could apply for SIF Devices.

b) Individual failure of each SIF Device that can make the SIF to fail on demand, and

c) Combinations of Devices in failure that can make the SIF to fail on demand,

The "SIL verification" activity shall generate a report to document and record the whole verification assessment and results.

If the "SIL verification" results indicate that the SIF design/implementation **DOES NOT** satisfy the SIF's "Safety integrity targets, constraints and other requirements" (see above section 4.2.5), means that the SIF **WILL NOT** be able to provide the required RISK reduction to protect the related machine, Equipment or process plant against the SIF's identified HAZARD.

In this case, modifications/adjustments **MUST BE DONE** to SIF design/implementation, and next the "SIL verification" assessment **MUST BE DONE** again.

5.2 SIL Verification Requirements (Safety integrity targets, constraints and other requirements)

By default, the "SIL verification" requirement is to verify if the indicated SIF satisfies the "Safety integrity targets, constraints and other requirements" (see above section 4.2.5).

Additional default "SIL verification" requirements can be specified for all SIF in a project.

When it is required, specific "SIL verification" requirements shall be indicated per SIF.

Possible "SIL verification" requirements for a Conceptual SRS are:

1) Determine the "Beta" values corresponding to the Simple (Greater CCF effect) and the Enhanced (Lower CCF effect) SIF's implementation/Installation.
2) Verify SIL rating in the cases of SIF's simple and enhanced implementation quality, but with NO Maintenance effect (MTTR, MRT).
3) Verify SIL rating in the same condition as described in above point No.2, but including Maintenance effect (MTTR, MRT).
4) Verify impact of applying, or not, "Diagnostic" (where it is possible) to improve SIL/STR requirements.
5) For a specific SIF Device, a "Proof Test Effectiveness" (Et) of 70% shall be considered.
6) "Proof Test Period" (TI) for the Logic Solver shall be fixed to 10 years.

7) Report and optimize "Proof Test Period" (TI) for all SIF Devices, no lesser than every 3 months.
8) Warn the Console Operator when a "Safe Detected" failure is identified by "Diagnostics" in the indicated SIF Device in the "Input Channel" and start a timer. If the timer expires and the related Device in failure has not been repaired yet, then initiate a SIF demand to set the SIF FSE in the SAFE estate. Refer to below section 5.4.1 for further details.
9) When a "Dangerous Detected" failure is identified by "Diagnostics" in the indicated SIF Device in the "Input Channel", then initiate a SIF demand to set the SIF FSE in the SAFE estate. In this way the SIF will never fails on demand. Refer to below section 5.4.1 for further details.

Possible "SIL verification" requirements for a Detailed Design SRS are:

1) Determine the "Beta" values for "Common Cause Failure" (CCF) effect.
2) Verify if implemented SIF satisfies the "Safety integrity targets, constraints and other requirements" (see above section 4.2.5).
3) Warn the Console Operator when a "Safe Detected" failure is identified by "Diagnostics" in the indicated SIF Device in the "Input Channel" and start a timer. If the timer expires and the related Device in failure has not been repaired yet, then initiate a SIF demand to set the SIF FSE in the SAFE estate. Refer to below section 5.4.1 for further details.
4) When a "Dangerous Detected" failure is identified by "Diagnostics" in the indicated SIF Device in the "Input Channel", then initiate a SIF demand to set the SIF FSE in the SAFE estate. In this way the SIF will never fails on demand. Refer to below section 5.4.1 for further details.
5) Check list to verify SIF installation @ FAT/SAT.

5.3 Device data for SIL verification

"Reliability data" and "MAINTENANCE times" shall be provided for each SIF device.

5.3.1 Reliability data

The "Reliability data" shall include:

a) Device type "A" or "B", according to IEC-61508-4 (2010), section 3.6.15.
b) Device failure data, according to IEC-61508 failure rate model.

"Reliability data" is normally provided as a part of a "SIL certificate".

If "Reliability data" is not available for a SIF Device, estimation methods can be applied, or data from available databases can be used, after approval from CLIENT and/or CONTRACTOR.

NOTE: If the "Device Type" is not provided for a SIF Device, by default the Device is "Type B".
"Proven in use" data ("Route 2H") could apply to justify to apply "Type A".

The Device failure data can be provided in one of the following format:

Format 1:	λ_{SD}, or LdSD	Safe Detected failure rate
	λ_{SU}, or LdSU	Safe UnDetected failure rate
	λ_{DD}, or LdDD	Dangerous Detected failure rate
	λ_{DU}, or LdDU	Dangerous UnDetected failure rate
	Et, or PTC	"Proof Test Effectiveness" (Et), or "Proof Test Coverage" (Et)

Format 2:	λ_{S}, or LdS	Safe failure rate
	DC_S	Diagnostic Coverage Safe
	λ_{D}, or LdD	Dangerous failure rate
	DC, or DC_D	Diagnostic Coverage Dangerous
	Et, or PTC	"Proof Test Effectiveness" (Et), or "Proof Test Coverage" (PTC)

NOTE: The "Failure Rate" engineering unit can be [FIT], [1/y], etc.

NOTE: "Reliability data" for each SIF Device can be provided in any other format, **ONLY** if the provided data is enough to convert it in any of the above formats 1 or 2.

5.3.2 MAINTENANCE times

CLIENT and/or CONTRACTOR shall define default "MAINTENANCE time" and constraints for each SIF Device. See Table 1.

ONLY in the cases where it is required, "MAINTENANCE times" values shall be specified for indicated SIF Devices.

The "SIL verification" process WILL review the specified "MAINTENANCE times" and report if they satisfy or not the required SIF's "Safety integrity targets, constraints and other requirements". See section 4.2.5.

Typically, the "SIL verification" shall optimize:

- Each SIF device "Proof Test Period" (TI), and
- It may optimize each SIF Device "Service Life" (SLf).

Normally, "TI" and "SLf" times are provided in [months or years], and the other "MAINTENANCE times" in [hours].

5.4 Reliability Data validation

The IEC-61508 failure rate model states that if a SIF Device includes "Fault Detection Capabilities" (Diagnostics), then the Safe and Dangerous failure rates have a portion for failures that can be detected by Diagnostics, and the other portion not. This distribution has positive credit in the "SIL verification" process in favor to make the SIF implementation to easier satisfy the "Safety integrity targets, constraints and other requirements".

Nevertheless, even though if the related SIF Device includes "Diagnostics", BUT such "Diagnostics" **ARE NOT** used, or **NOT** considered, in the SIF implementation/installation, then there **IS NOT** credit on "Diagnostics" in the "SIL verification" process.

For example, Table 2 shows the "Failure Rate" data for a SIF Device. It is indicated that the SIF Device includes "Fault Detection Capabilities" (Diagnostics).

BUT, if the SIF implementation **DOES NOT** use, or **DOES NOT** take advantages of, the Device Diagnostics, then the Device "Fault Detection Capabilities" have **NO CREDIT** in the "SIL verification" process. In this case, data in Table 3 shall be used for "SIL verification", instead of data in Table 2.

Table 2 – Example of "Failure Rate" information of a SIF Device

	Safe	**Dangerous**	
Detected	λ_{SD}, or LdSD = 75.0 FIT	λ_{DD}, or LdDD = 170.0 FIT	**Type B** device SFF = 95.2% Max CLAIM SIL 2
UnDetected	λ_{SU}, or LdSU = 150.0 FIT	λ_{SU}, or LdDU = 20.0 FIT	

*Table 3 – Adjusted data from Table 1 for "SIL verification", if the SIF implementation **DOES NOT** use, or **DOES NOT** take advantages, of the Device Diagnostics*

	Safe	**Dangerous**	
Detected	λ_{SD}, or LdSD = 0.0 FIT	λ_{DD}, or LdDD = 0.0 FIT	**Type B** device SFF = 54.2% Max CLAIM SIL 0
UnDetected	λ_{SU}, or LdSU = 150.0 + 75.0 **= 225.0 FIT**	λ_{SU}, or LdSU = 20.0 + 170.0 **= 190.0 FIT**	

Since the maximum SIL rating that a device can CLAIM is determined by SFF (See IEC 61508-4:2010, section 3.6.15), after adjustment in Table 3 the referred SIF device **MAY NOT** satisfy the required SIL rating.

From above paragraph, change in a SIF device SFF will affect SIF's SIL rating, because the maximum SIL rating a SIF can CLAIM is determined by "Route 1H (or 2H)" (See IEC-61508-2:2010 section 7.4.4).

5.4.1 Additional data validation for "Spurious TRIP Rate" (STR) verification

Strictly speaking, the "Spurious TRIP Rate" (STR) calculation for a SIF depends ONLY on:

a) ALL SIF "Decision Logics" where the SIF Device is used (use MTTR in calculation), and

b) The SIF Device "Safe Detected" and "Safe UnDetected" failure rate values.

Nevertheless, if "Fault Detection Capabilities" (Diagnostics) are used in the SIF implementation, then one(1)or both of the following considerations may apply:

Consideration 1: By default, when a "Safe Detected" (SD) failure occurs in a SIF device, Operator is notified, and then this device condition shall change to initiate a SIF "Spurious TRIP" as well.

If the SIF Device "Fault Detection Capabilities" (Diagnostics) are used to detect SD failures in a Device located in the "Input Channel", then SIF implementation can STOP the "Spurious TRIP" and still warn the Operator. Technically, NO "Spurious TRIP" occurred. This action decreases the SIF STR, making it more reliable

Consequence of application: SIF Device "Safe Detected" failure rate (λ_{SD}, or LdSD) **IS NOT** used on "Spurious TRIP Rate" (STR) calculation, BUT it is included in the SIL rating calculation, then reliability data from Table 2 shall be adjusted as shown in Table 4 for "SIL verification" calculation.

Table 4 – Adjusted data from Table 2 for "SIL verification", when SIF implementation/Installation uses "Diagnostics" to identify SD failures in an "Input Channel" device to STOP the "Spurious TRIP"

	Safe	Dangerous
Detected	λ_{SD}, or LdSD = 0.0 FIT	λ_{DD}, or LdDD = 75.0 + 170.0 **= 145.0 FIT**
UnDetected	λ_{SU}, or LdSU = 150.0 FIT	λ_{SU}, or LdSU = 20.0 FIT

NOTE: By design, MAINTENANCE shall have a chance of MTTR time to repair detected SD failure, else safety shall apply. This means that If the "Consideration 1" applies in the SIF design/implementation, when a SD failure occurs in the referred SIF device, SIF implementation shall STOP "Spurious TRIP", BUT a demand shall be initiated to set the SIF FSE in the SAFE state after MTTR time.

Consideration 2: By default, when a "Dangerous Detected" (DD) failure occurs, then Operator is notified, and the normal operation continues. SIF WILL fail on demand. NO "Spurious TRIP" occurs.

At this point, SIF design/implementation has the following choices:

a) (NOT RECOMMENDED, "Target System" is unprotected) Operator is notified and SIF waits forever until MAINTENANCE is applied to repair SIF device in failure.

b) To allow operation to continue for MTTR time, and Operator is notified. When MTTR expires, SIF implementation shall initiate a demand to set the SIF FSE in the SAFE state. Technically, NO "Spurious TRIP" occurred.

c) SIF implementation shall initiate a demand at once the DD failure is detected, Operator is notified. Technically, and a "Spurious TRIP" occurred.

ONLY in the above point "c" the SIF implementation behavior is the default one as when a SD failure occurs (see above "Consideration 1"), BUT such choice increases the SIF STR.

<u>Consequence of application of Choice 'c':</u> Let's assume the referred SIF device "Reliability data" is shown in Table 2. SIF Device "Dangerous Detected" (DD) failure rate (λ_{DD}, or LdDD) is IN FACT used on "<u>Spurious TRIP Rate</u>" (STR) calculation, but **NOT** in "SIL verification". As consequence of this consideration, reliability data from Table 2 shall be adjusted as shown in Table 5.

Table 5 – Adjusted data from Table 2 for "SIL verification", when SIF implementation/Installation uses "Diagnostics" to identify DD failures in a SIF device, and when DD failure occurs a "Spurious Trip" is initiated at once

	Safe	**Dangerous**
Detected	λ_{SD}, or LdSD = 75.0 + 170.0 **= 145.0 FIT**	λ_{DD}, or LdDD = 0.0 FIT
UnDetected	λ_{SU}, or LdSU = 150.0 FIT	λ_{SU}, or LdSU = 20.0 FIT

5.5 SIL verification required calculation methodology

"SIL verification" calculation shall be done in two(2) calculation steps:

- Step calculation No.1.
- Step calculation No.2.

5.5.1 Step calculation No.1.

The "<u>SIL verification</u>" activity on the verification of the SIF "<u>Probability of Failure on Demand Average</u>" (PFDavg) shall calculate:

a) The SIF "PFDavg" according to the SIF "<u>Reliability Block Diagram</u>" (RBD), and

b) The maximum SIL rating to claim according to IEC-61508-4 (2010), section 3.6.15. This "Device" data is used to calculate the whole SIF maximum SIL rate to claim by using "<u>Route 1H</u>".

<u>NOTE:</u> "<u>Route 2H</u>" can supersede "<u>Route 1H</u>" if "<u>proven in use</u>" data is available.

Typical methodologies to calculate the SIF "<u>Probability of Failure on Demand Average</u>" (PFDavg) are:

1) IEC-61508 Simplified equations,
2) Basic probability theory according to the IEC-61508 PFDavg calculation principles,
3) Fault tree analysis, and
4) Markov modeling.

ONLY the simplified equations calculate the "PFDavg", all the other methodologies calculate the "Probability of Failure on Demand" punctual value [PFD(t)]. So for methodologies 2, 3 and 4, additional computations are required to obtain "PFDavg" value over the time period of interest (SLf).

The preferred methodologies for "PFDavg" calculation shall the listed No.1 and No.2 above.

Basic probability theory according to the IEC-61508 shall be the used methodology for verification of the SIF "Spurious TRIP Rate Average" (STRavg), if STR calculation is required.

5.5.2 Step calculation No.2.

The SIF "PFDavg" shall be the lesser value from the following ones:

1) Calculated SIF "PFDavg",
2) Maximum SIL rating to claim according to "Route 1H", and
3) Maximum SIL rating to claim according to "Maximum SIL Safety Design Limit" (MSSDL).

The SIF "STRavg" shall be the lesser value from the following ones:

1) Calculated SIF "STRavg", and
2) "Maximum STR Safety Design Limit" (MSSTRDL)

5.6 SIL Verification report structure

The SIL Verification report may include the following sections:

1) Assessment Summary.
2) SIF description
3) Safety integrity targets, constraints and other requirements.
4) Premises and Assumptions.
5) Reliability data validation.
6) Reliability Block Diagram (RBD).
7) Assessment results.
8) (FMEA) Failure Modes and Effect Analysis.
9) Failure modes that DO NOT promote a failure on Demand.
10) SIF Devices' List and data for "SIL verification" (after Reliability Data Validation).

An initial agreement between CLIENT, SUPPLIER and 3rd Party Certifier shall define which of the above section will be included, or not in the "SIL verification" report. The agreement could be different for some SIFs.

5.6.1 Assessment Summary

Indicate project Tag number for SIF, short description, and present an outline of the "SIL verification" activity results. One(1) or tow(2) pages only to show how the referred SIF satisfies, or NOT, the "Safety integrity targets, constraints and other requirements".

5.6.2 SIF description

Refer to SRS document or include a SIF description if no SRS is available.

5.6.3 Safety Integrity targets, constrains and other requirements

Refer to above section 4.2.5 for further details.

5.6.4 Premises and Assumptions

Describe/List the Premises and Assumptions. These ones can be:

- “PFDavg” calculation methodology.
- “STRavg” calculation methodology.
- “Common Cause Failure” (CCF) calculated methodology, and/or previous agreement for “SIL verification” report development.
- Source or estimation methodology for SIF Devices’ data.
- Devices’ “Fault detection capabilities” (Diagnostics) scope of work.
- Any previous agreement about haw to handle the SIF Devices’ data.

5.6.5 Reliability data validation

Describe the result of the “Reliability data validation” process.

Refer to section 5.4.

5.6.6 Reliability Block Diagram (RBD)

For SIFs where each Device contribution to the SIF “PFDavg” is fully additive, or simple to understand, a “Reliability Block Diagram” (RBD) may not be required.

When the SIF Devices’ contribution to “PFDavg” is complex, an RBD shall be provided.

5.6.7 Assessment results

Present the same “SIL verification” results that were shown in the report section “Assessment Summary” (see above section 5.6.1), but including all analyses, explanations, used data, graphics, Charts, etc.

5.6.8 (FMEA) Failure Modes and Effect Analysis

Include and describe all failure modes that were considered for developing the "SIL verification" results.

This section should include all SIF Devices individual and combined failures.

For each individual failure, the following minimum information shall be included:

- Device Tag and short description.
- Device ype or IF location" "Initiator" or "Input Channel", "Logic Solver", "Output Channel", "Support".
- NORMAL state of operation.
- Failure mode.
- Failure effect.
- Failure type: Safe or Dangerous, Detected or UnDetected.
- Diagnostic that identifies the failure.

For combined failures, the following minimum information shall be included:

- List of Tag Devices in combined failure.
- Combined failure description.
- Failure effect.
- Diagnostic that identifies the failure.

5.6.9 Failure modes that DO NOT promote a failure on Demand

Include and describe all failure modes that **WERE NOT** considered for developing the "SIL verification" results.

5.6.10 SIF Devices' List and data for "SIL verification" (after Reliability Data Validation)

Include:

1) The SIF Devices' list, and
2) The Device data that was used in the "SIL verification" activity. Refer to above section 5.3.

Also, it shall be indicated per device the result of "Reliable Data validation", as described in above section 5.4.

The SIF Devices' list shall include as a minimum:

- Device's Tag
- Type: Input, Logic Solver, Output, Support.
- Device data is sued for: "SIL & STR" calculation, or "Only STR" calculation.
- Short description.

APPENDIX A – DCS-SIS HMI typical tie-ins per SIF

			SIS Safety Instrumented System			DCS Distributed Control System		
01		SIF data	Safety Function (SIF) ID	SID	→	SID		
02			MOS Group ID	SID	→	SID		
03			MOS Group Actived / De-Activated state	DO	→	DI		
04	For each INITIATOR, Input Device, or Input Channel		Device / Channel ID	SID	→	SID		
05		Analogue, Boolean, Pulse type signal, and "Trip Criterion"				SID	Control variable ID (Tag)	IF available
06						Inf	Control Measurement value (**NOTE 3**)	
07						Inf	Control Measurement pre-alarm	
08			High Trip Setting	AO	→	AI		
09			Current Initiator Signal value	AO	→	AI		
10			Trip Setting DeadBand	AO	→	AI		
11			Low Trip Setting	AO	→	AI		
12			Current SAFE / NORMAL State	DO	→	DI		
13			Detected Failure State (If applies)	DO	→	DI		
14		"Maintenance Override Switch" (MOS)		PI	← **NOTE 5**	PO	MOS Activate Command	
15				PI	← **NOTE 5**	PO	MOS De-Activatate Command	
16			MOS Activated / De-Activated State	DO	→	DI		
17			MOS Pre-Alarm timer value	AO	→	AI		
18			MOS Pre-Alarm	AO	→	AI	**NOTE 4**	
19			MOS Setting timer value (MTTR)	AO	→	AI		
20			MOS Running timer value	AO	→	AI	**NOTE 1**	
21			MOS timer Expired or Not	DO	→	DI	**NOTE 2**	
22		Proof Test Logic	"Proof Test Logic" Input	DO	→	DI	Logic to record: • When Proof test started/finished. • If process variable passed Trip setting value: TRIP state • If process variable passed (Trip setting + DeadBand) value: NORMAL state.	
23			"Proof Test Logic" Output	DO	→	DI		
24			Logic implementation depends on the Device type where the "Proof Test" is applied.		↔			
25								
26	For Manual Initiator	Pulse Type signal		SID	←	SID	Push button ID	IF it is applicable
27				PI	←	PO	Pulse signal to TRIP	
28				PI	← **NOTE 5**	PO	MOS Activate Command	
29				PI	← **NOTE 5**	PO	MOS De-Activatate Command	
30			MOS Activated / De-Activated State	DO	→	DI		
31			"Manual Input MOS" output	DO	→	DI		
32		SIF Startup Bypass		SID	←	SID	Startup Bypass button ID	IF it is applicable
33				PI	←	PO	Bypass Manual command button	
34			Startup Bypass ID	SID	→	SID		
35			Process Variable Setting value	AO	→	AI		
36			Current Process Variable value	AO	→	AI		
37			Bypass State: Enable/Disable	DO	→	DI		
38	SIF Decision Logic	Per "Decision Logic"	"Decision Logic" output	DO	→	DI		
39			Logic degraded levels: 0, 1, 2, etc.	AO	→	AI		
40			Higher Priority TRIP level: SAFE or NORMAL	DO	→	DI		
41	SIF Interlock Logic	Per "Interlock Input"	Interlock ID	SID	→	SID		
42			Interlock State: SAFE or NORMAL	DO	→	DI		
43			"Interlock Logic" Output: SAFE or NORMAL	AO	→	AI		

ABBREVIATONS:

AI	Analogue Input.
AO	Analogue Output.
DI	Digital Input.
DO	Digital Output.
Inf	Information
PI	Pulse Signal Input.
PO	Pulse Signal Output.
SID	Signal String ID (if it applies).

NOTES:

1 Signal **MUST** generate alarm in DCS before timer expires.
2 Signal **MUST** generate alarm in DCS after timer expires.
3 Process variable that can compared with Initiator meausrement.
4 Typical MTTR value is 72 hr. MOS implementation shall include a recurrent alarm that shall be activated, for example, every 4 hours, in order to warn Console Operator.
5 Applies for Soft-Button or Hart-Button.

	SIS Safety Instrumented System					DCS Distributed Control System		
44		Reset Logic		PI	← NOTE 5	PO	"Reset Command"	44
45			"Reset Logic" Input	DO	→	DI		45
46			"Reset Logic" Output	DO	→	DI		46
47	For each FSE, Output Device, or Output Channel	Analogue, Boolean, Pulse type signal, and "Trip Device"	Device / Channel ID	SID	→	SID		47
48			Current SAFE / NORMAL State	DO	→	DI		48
49			Detected Failure State (If applies)	DO	→	DI		49
50		"Maintenance Override Switch" (MOS)		PI	← NOTE 5	PO	MOS Activate Command	50
51				PI	← NOTE 5	PO	MOS De-Activatate Command	51
52			MOS Activated / De-Activated State	DO	→	DI		52
53			MOS Pre-Alarm timer value	AO	→	AI		53
54			MOS Pre-Alarm	AO	→	AI	NOTE 4	54
55			MOS Setting timer value (MTTR)	AO	→	AI		55
56			MOS Running timer value	AO	→	AI	NOTE 1	56
57			MOS timer Expired or Not	DO	→	DI	NOTE 2	57
58		Proof Test Logic	"Proof Test Logic" Input	DO	→	DI	Logic to record: • When Proof test started/finished. • "Proof Test" duration was equal or lesser than SRT. • "Proof Test" reached target.	58
59			"Proof Test Logic" Output	DO	→	DI		59
60			Logic implementation depends on the Device type where the "Proof Test" is applied.		↔			60
61								61

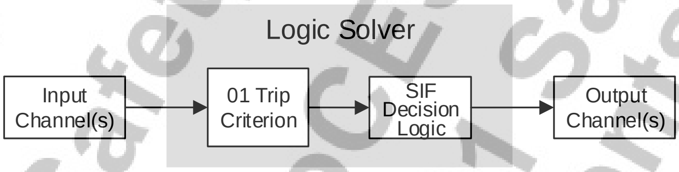
APPENDIX B – Additional SIF components for Project SIF design and implementation

To follow good engineering practices, and to satisfy the nowadays safety standards (IEC 61508, ISA 84.00.02), the implementation of a "Safety Instrumented Function" (SIF) shall include additional components for proper integration with Operation, Control and "Proof Testing" requirements of SIF devices. These Additional SIF components shall be implemented:

- ➢ Within the "Logic Solver",
- ➢ As part of DCS (Logic and/or HMI), and/or
- ➢ As part of design & physical installation of Initiators, Final Safety Elenent(s), Input/Output Channels.

A simplification of a SIF structure is shown in Figure 1. This figure shall be used as reference point for describing the Additional SIF components.

Figure 1 – Minimal description of a "Safety Instrumented Function" (SIF) structure, before including additional SIF components



The Additional SIF components are listed following: (see Figure 2)

Additional components per SIF:

- Manual Initiator
- Manual Input MOS
- Start-up Bypass
- Reset Function
- Interlock Logic

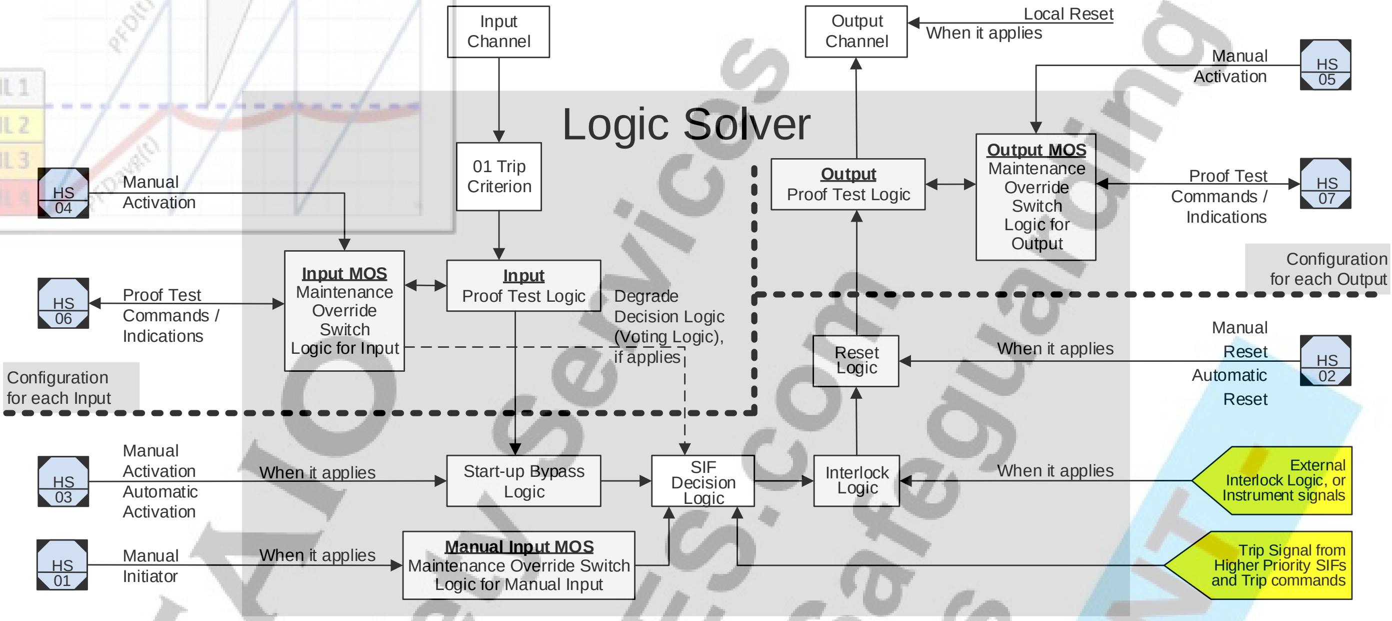
Additional SIF components per Input:

- Input Proof Test Logic
- Input MOS

Additional SIF components per Output:

- Output Proof Test logic
- Output MOS

Figure 2 – "Safety Instrumented Function" (SIF) structure, after including additional SIF components


Logic Solver
Input Channel
01 Trip Criterion
Output Channel
Local Reset
When it applies
Manual Activation
HS 05
Output Proof Test Logic
Output MOS Maintenance Override Switch Logic for Output
Proof Test Commands / Indications
HS 07
Configuration for each Output
HS 04
Manual Activation
Input MOS Maintenance Override Switch Logic for Input
Input Proof Test Logic
Degrade Decision Logic (Voting Logic), if applies
HS 06
Proof Test Commands / Indications
Configuration for each Input
Reset Logic
When it applies
Manual Reset
Automatic Reset
HS 02
HS 03
Manual Activation
Automatic Activation
When it applies
Start-up Bypass Logic
SIF Decision Logic
Interlock Logic
When it applies
External Interlock Logic, or Instrument signals
HS 01
Manual Initiator
When it applies
Manual Input MOS Maintenance Override Switch Logic for Manual Input
Trip Signal from Higher Priority SIFs and Trip commands