# Safety Instrumented System (SIS)

A Safety Instrumented System (SIS) is a system comprising sensors, logic solvers and actuators whose purpose is to take a process to a safe state when normal predetermined set points are exceeded, or safe operating conditions are violated

## A. Safety Lifecycle

The Safety Life Cycle (SLC) is a core concept in all recent standards related to Safety Instrumented Systems. The IEC 61508 is a basic safety publication of the IEC and as such, it is an "umbrella" document that covers multiple industries and applications. IEC 61511 is an industry-specific standard for the process industries that is based on IEC 61508.

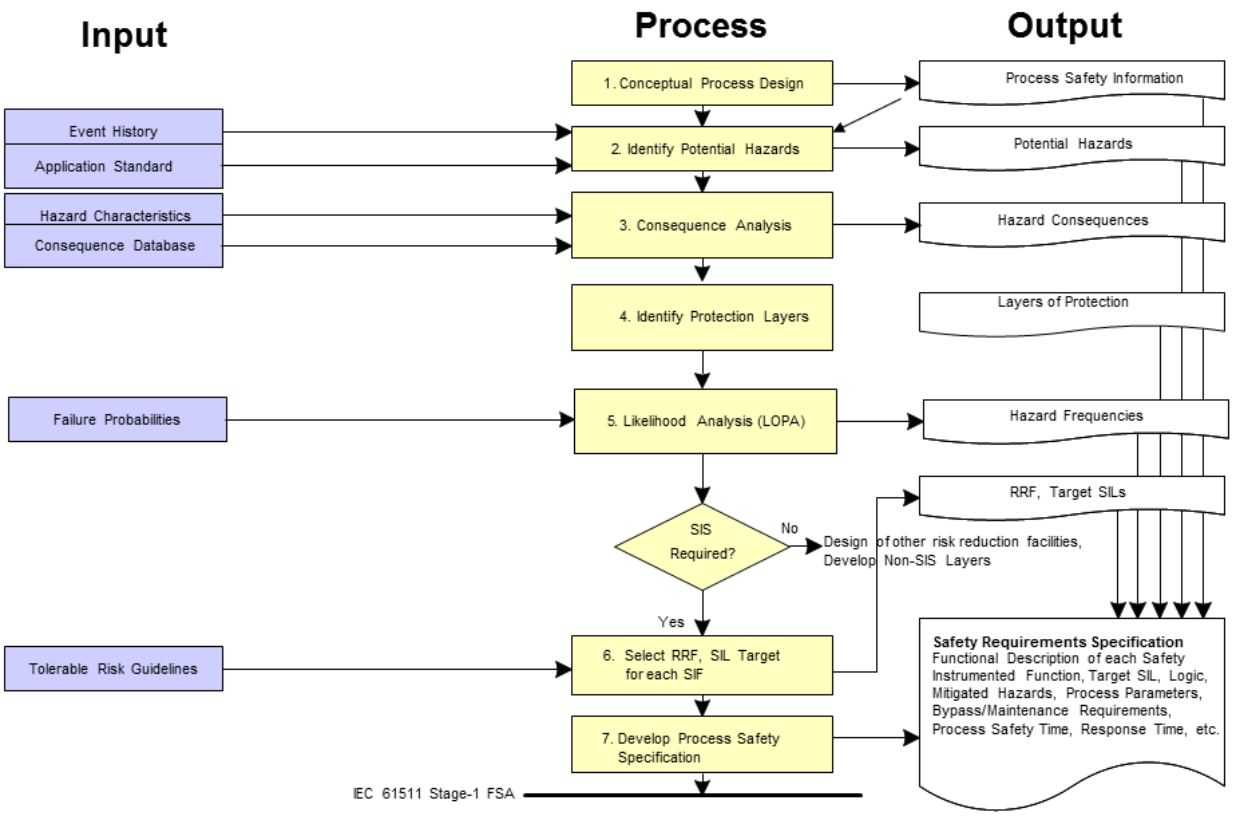
SLC is an engineering process that contains all the steps needed to achieve high levels of functional safety during conception, design, operation, and maintenance of instrumentation systems. It is a plan-do-assess-adjust sort of activity with a clear objective. An automation system designed according to SLC requirements will predictably reduce risk in an industrial process.

The safety life cycle provides:

- A structured and consistent framework for the specification, design, implementation and maintenance of safety instrumented systems
- Guide to risk assessment methodologies
- The performance requirements of each safety instrumented function

### 1. Safety Lifecycle – Analysis Phase

It starts from the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use. The key idea here is that safety must be considered from the very inception of the conceptual process design and must be maintained during all design, operation, and maintenance activities.



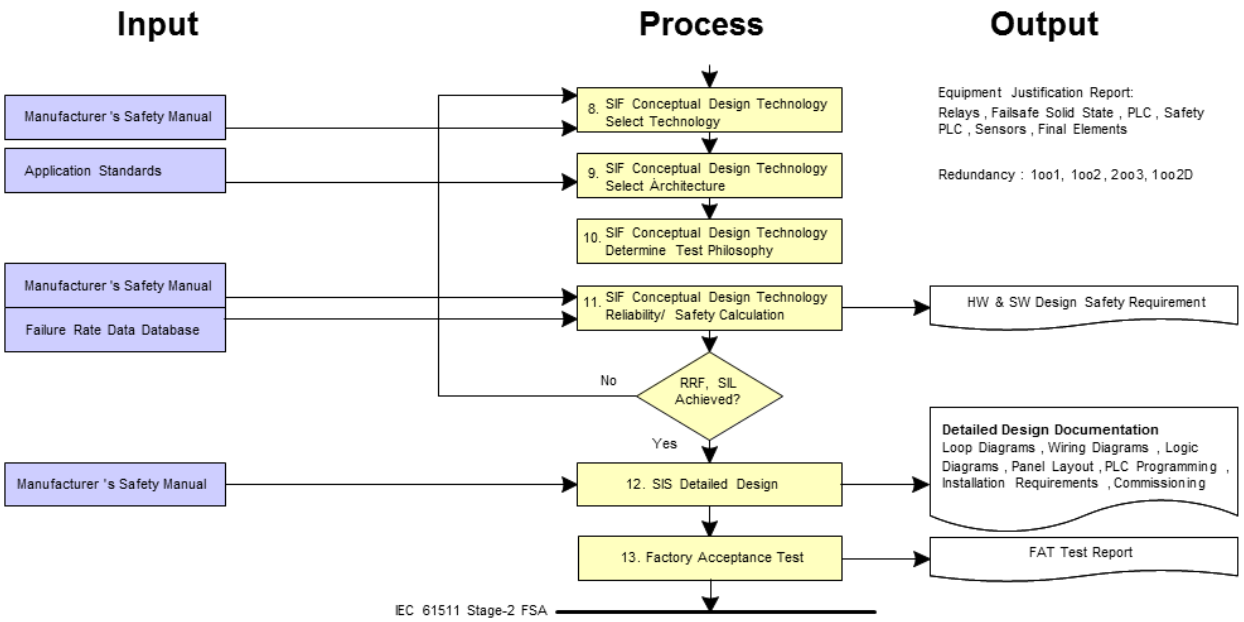

The Figure shown above provides a detailed diagram of activities in the analysis phase of the safety lifecycle. When the conceptual process design is complete, detailed process safety information is available such as:

- Types and quantities of chemicals used
- Pressures, temperatures, and flows of the intended design
- Process equipment used and its design strength
- Control strategy and intended control equipment
- Drawings, diagrams, and other relevant information

Given this information, a hazard and risk analysis is performed that identifies possible hazards and then establishes the consequence and likelihood of each. On some projects, consequence is determined through detailed analysis, and on others it is done by estimation. Likewise, likelihood analysis is sometimes performed by detailed analysis and sometimes by estimation. With the emergence of new techniques such as Layer of Protection Analysis; however, the trend is clearly toward more analysis.

The consequence severity and the likelihood frequencies determine risk. In some cases, the risk of a hazard is within tolerable levels, and no risk reduction is needed. For these cases, no SIS is required. In other cases, risk reduction is required, and the quantity of risk reduction is specified by an order-of-magnitude level called the safety integrity level (SIL).

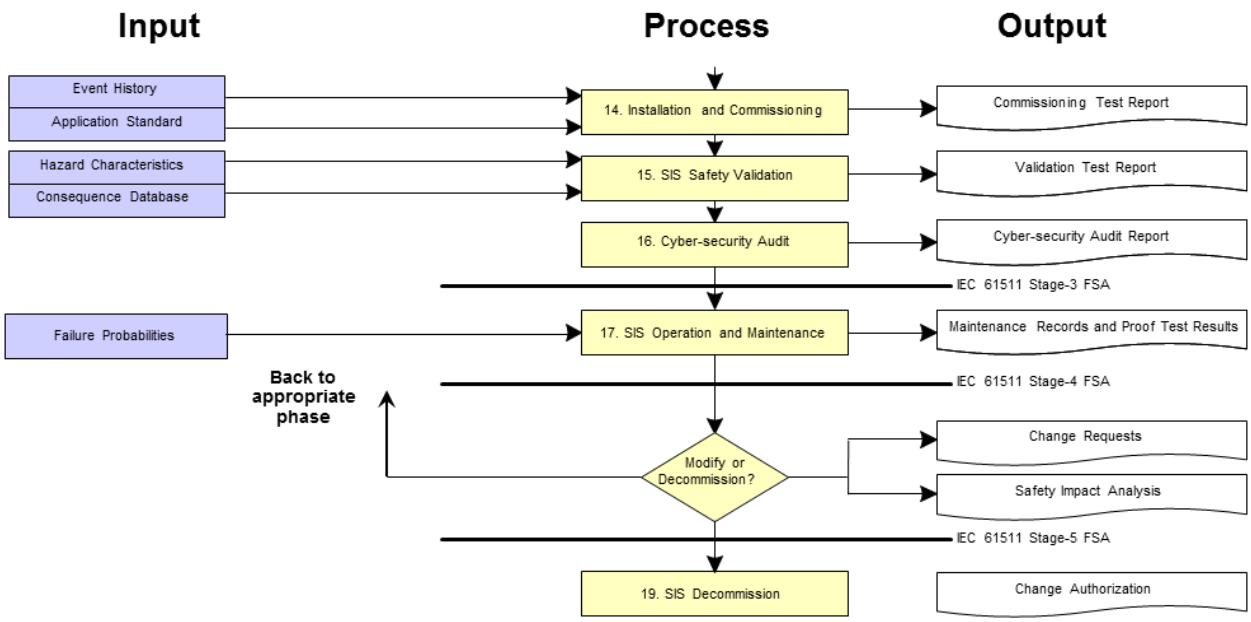
## 2. Safety Lifecycle – Realization Phase




When all safety instrumented functions are identified and documented, the design work can begin. A conceptual design is performed by choosing the desired technology for the sensor, the logic solver, and the final element.

Redundancy may be included so as to achieve high levels of safety integrity, to minimize false trips, or for both reasons. Once the technology and architecture have been chosen, the designers review the periodic test philosophy constraints provided in the SRS. Given that safety instrumented systems will, hopefully, not be called on to activate, they must be completely inspected and tested at specified time

## 3. Safety Lifecycle – Operation Phase




The operation phase of the safety lifecycle begins with a pre-startup safety review (PSSR) of the SIS design. During the PSSR, the engineers must answer a number of questions such as:

- Does the system meet all the requirements stated in the safety requirements specification?
- Have all safety instrumented functions met SIL targets and Mean Time To Trip Spuriously (MTTFS) targets?
- Have all the necessary design steps of the safety lifecycle been carried out successfully?
- Has the manufacturer's safety manual been followed for all equipment?
- Is there a periodic inspection and test plan for each safety instrumented function?
- Have the maintenance procedures been created and verified?
- Is there a management-of-change procedure in place?
- Are operators and maintenance personnel qualified and trained?

If the answers to these questions are acceptable, the process can proceed with startup and operation.

While in operation, proper operating procedures and all maintenance activities including periodic function testing and mean time to repair targets have to be followed. Periodic functional testing must be done as per the time schedule established during the conceptual design verification calculations and must be done per the plan established to ensure that all potentially hidden dangerous failures are detected. All periodic inspection and test activities must be documented. It is very important that each safety instrumented function is restored to full operation after each test. Bypass valves and force functions must be removed and these restorations must be documented.

The safety lifecycle includes management of all modifications made to the system during its useful life. For each, the engineer making the change must analyze the impact of the change and go back

to the appropriate step in the safety lifecycle. If new technology is chosen, the SIL verification must be repeated. The new SIL level must meet or exceed the original. Decommissioning is considered as well. The engineer must analyze the effect of decommissioning the system. Are all safety instrumented functions no longer needed? If some are still needed, they must be relocated or decommissioning must not proceed

## B. SERVICES

### 1. SIS Gap Assessment

The SIS gap assessment is carried out to identify any critical and potential gaps between the SIS best practices and the requirements of ANSI/ISA 84.00.01-2004 (IEC 61511) with the design and the implementation, the operation as well as the maintenance of the existing SIS. The findings will be categorized based on their impacts to the safety, business as well as environment and will be used as a basis for SIS opportunity improvement. All findings and recommendations that have significant safety, business and environmental impact shall be documented, followed-up, tracked and closed out

Following figure shows the example of assessment result of SIS Gap Assessment

| Area | R (# items) (%) | Y (# items) (%) | G (# items) (%) | B (# items) (%) | Total # Items |
|---|---|---|---|---|---|
| 1. Prelim Engineering and Design | 4<br>7.7% | 0<br>0.0% | 16<br>30.8% | 32<br>61.5% | 52 |
| 2. Detailed Eng/Design/SIS Build | 4<br>16.7% | 6<br>25.0% | 13<br>54.2% | 1<br>4.2% | 24 |
| 3. Construction and Startup | 4<br>7.8% | 2<br>3.9% | 44<br>86.3% | 1<br>2.0% | 51 |
| 4. Operate and Maintain | 8<br>25.0% | 2<br>6.3% | 15<br>46.9% | 7<br>21.9% | 32 |
| 5. SIS Modification | 1<br>8.3% | 0<br>0.0% | 10<br>83.3% | 1<br>8.3% | 12 |
| 6. Overall Safety Lifecycle Management | 6<br>10.9% | 24<br>43.6% | 15<br>27.3% | 10<br>18.2% | 55 |
| Total Conformance Items | 27 | 34 | 113 | 52 | 226 |
| Total % | 11.9% | 15.0% | 50.0% | 23.0% | |

Note:

–non conformance with ISA 84 or IEC 61511 could have significant safety, business or environmental impact

–non conformance with ISA 84 or IEC 61511 , probably no significant near term safety, business or environmental impact

–in conformance with ISA 84 & IEC 61511

–non conformance with checklist/good engineering practice, probably no near term significant safety, business or environmental impact

### 2. SIL Verification

The purpose of SIL Verification is to determine if each SIF that hasn't been verified would meet the target Safety Integrity Level (SIL) specified during the SIL classification performed during design.

For each SIF the average probability of failure on demand (PFDavg) will be calculated using SIL software package (such as SIL Solver, ExSILentia) and the results compared with the PFDavg range for the target SIL. A standard test interval will be defined for all calculations. Reliability data is generally obtained from the industry database such as OREDA, EXIDA SERH (Safety Equipment Reliability Handbook). Compliance with the architectural constraints specified in IEC61508.2 is also verified as well as SIL Capability.

**Scope of Work**

Following typical process will be included.

- Data Collection
  - Determine SIFs
  - Collect P&ID and Loop Drawing Diagram
  - Collect Datasheet of instruments (Sensor, Logic Solver and Final Element)
  - Collect other required information

- SIL Verification
  - Determine SIF Definition using Exsilentia
  - Determine SIF Target Selection using Exsilentia
  - Conduct SIF Verification

- Compliance Report
  - IEC 61511 Compliance Report

Following figure shows the snapshot of SIL Verification

Integrity Level verification, the following assumptions have been made.

Mission Time: 15 years

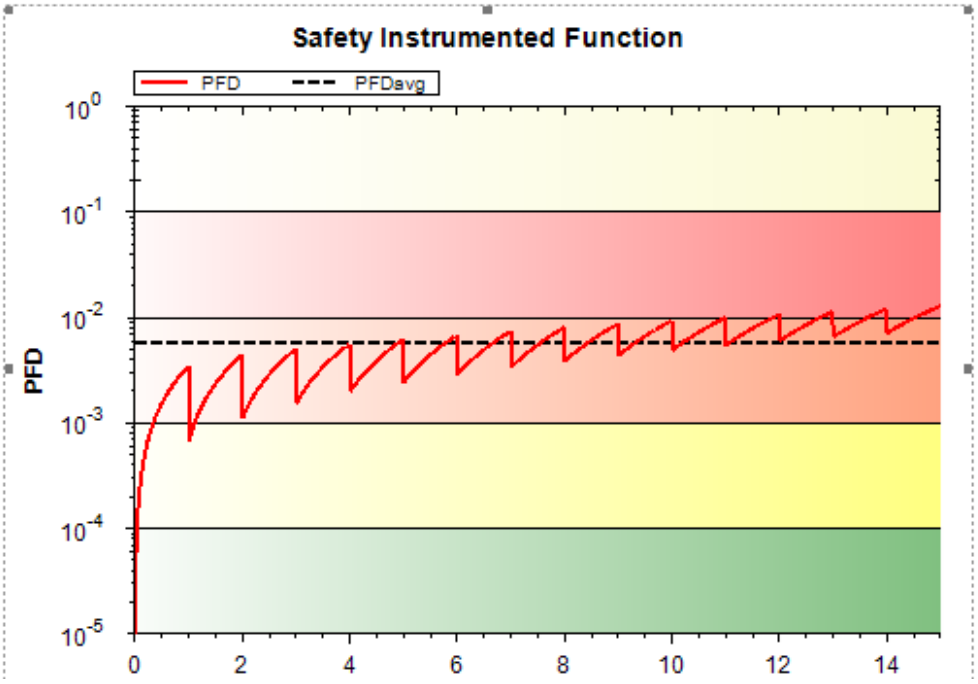
Startup time: 12 hours

The SIF operates in Low demand mode.

The SIL verification has been performed by , on 12 Dec 2012.

The systematic capability of the various components in the LAHH0001A/B/C Safety Instrumented Function was considered.

Comments: Service: Flare Liquids



Given the reliability data and calculation details described in the subsequent subsections in this report the LAHH0001A/B/C Safety Instrumented Function achieves the functional safety performance as displayed in Table 4.

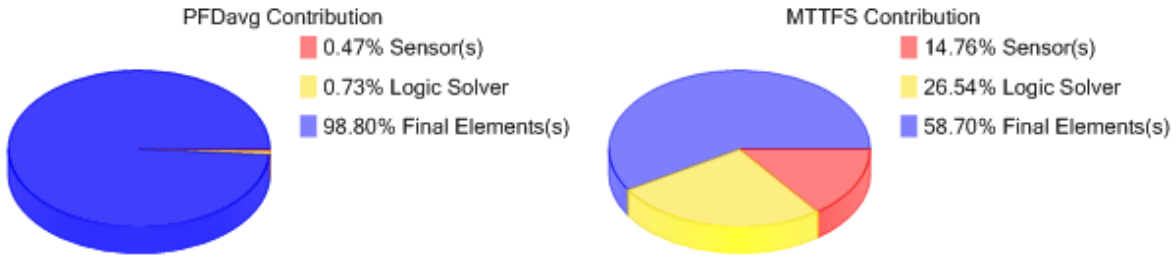
**Table 4 Functional Safety Performance**

| PFDavg | RRF | SIL (PFDavg) | SIL (Architectural Constraints IEC 61508:2000) | SIL (Systematic Capability) |
|---|---|---|---|---|
| 5.67E-03 | 176 | 2 | 2 | 2 |

The LAHH0001A/B/C Safety Instrumented Function was also evaluated on spurious trip behavior. The results expressed in the MTTFS are displayed in Table 5.

**Table 5 Spurious Trips**

| MTTFS (years) |
|---|
| 40.96 |




**3. SIS Training**

We provide standard and custom training of Safety Instrumented System. The detail can be seen in Training section in this website.