ProSIS-FSE

SIL Calculator V1.6 User Guide

Table of Contents

1 OBJECTIVES

SIL Verification is a formal process that utilizes the conceptual design results to perform a reliability evaluation on that conceptual design. The SIL verification will be performed using the online tool to located at ProSIS-FSE >SIL Calculator. The result of the SIL verification is the Achieved Safety Integrity Level (ASIL) for the specific SIF under consideration. As long as the ASIL (Achieved SIL) is greater than or equal to the TSIL (Target SIL), the conceptual design of the SIF is proven sufficient. If the ASIL is lower than the TSIL, the conceptual design will need to be improved.

The Achieved Safety Integrity Level is obtained from two or three separately determined Safety Integrity Levels (PFD, Architecture, and Systematic Capability). Though it is important for engineers to understand that the final ASIL is based on these two (or three) independently determined Safety Integrity Levels, the actual determination of the Safety Integrity Levels is something that is automatically done through the online SIL Calculator Tool.

Safety Integrity Level (SIL) is the internationally accepted term for defining the required performance of a Safety Instrumented Function (SIF) in terms of maximum probability of failure and minimum level of hardware fault tolerance as protection for random failures and for specifying engineering development process requirements as protection against systematic failures. The SIL Calculator tool evaluates all three concepts as defined by current standards.

The purpose of this guide is to provide guidance on using the SIL Calculator Tool. This document is not intended to provide advice on applying the published industry consensus standards on Functional Safety.

2 REFERENCES

2.1 Referenced Publications

(1) IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, 2003, International Electrotechnical Committee, Geneva, Switzerland

(2) ANSI/ISA 84.00.01-2004 (IEC 61511: Mod), Functional Safety: Safety Instrumented Systems for the Process Industry Sector, 2004, The Instrumentation, Systems, and Automation Society, 67 Alexander Drive, Research Triangle Park, North Carolina, 27709

(3) IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, 2000 & 2010, International Electrotechnical Committee, Geneva, Switzerland

3 ACRONYMNS AND DEFINITIONS

Acronymns

Act	Actuator
ASIL	Achieved Safety Integrity Level
Amp	Amplifier
Anlg	Analog
BFV	Butterfly Valve
Lvl	Level
Mtr	Meter
MTTR	Mean Time To Restoration
Multi	Multiplexer
Perf	Performance
PFD_{avg}	Average Probability of Failure on Demand
Pneu	Pneumatic
Press	Pressure
PHA	Process Hazards Analysis
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIL_{pfd}	SIL based on Probability of Failure (pfd) Average
SILarch	SIL based on Architectural Constraints
SIL_{sys}	SIL based on Systematic Capabilities
SILcalc	SIL Calculation Online Tool
SIF	Safety Instrumented System
Smrt	Smart
SOV	Solenoid Valve
SRS	Safety Requirements Specification
Srvc	Service
Sw	Switch
Temp	Temperature
TSIL	Target Safety Integrity Level
Tx	Transmitter

Definitions

Achieved Safety Integrity Level ***(ASIL)***	The SIL achieved given the SIF's conceptual design, it is based on the minimum value for SILpfd, SILarch, and SILsys for low demand applications.
Safety Instrumented Function ***(SIF)***	A function that is implemented by a Safety Instrumented System which is intended to achieve or maintain a safe state for the process with respect to a specific hazardous event. Each SIF should be designed and tested to meet its target SIL.
Safety Integrity Level ***(SIL)***	Discrete level (one out of a possible four) for specifying the probability of a SIS satisfactorily performing the required SIF under all of the stated conditions within a stated period of time.

Safety Instrumented System ***(SIS)***	A system consisting of one or more SIFs. Consists of sensors, logic solver(s), and final elements.
Target Safety Integrity Level ***(TSIL)***	The SIL required of a SIF such that when this SIF is combined with any non-SIS IPLs, the overall risk associated with the hazardous scenario is adequately reduced.

4 SIL VERIFICATION RESPONSIBILITIES

1. Specify SIF design in SILcalc
2. Determine reliability data for components
3. Execute reliability calculations using SILcalc
4. Document results
5. Suggest areas for improvement in case conceptual design does not meet the Target Safety Integrity Level

5 SIS DESIGN Coupled to SIL VERIFICATION PROCESS

The combined SIF Design and SIL verification process shows an iterative process where a Design is created evaluated, and if deemed sufficient finalized. If the design is not sufficient a re-design of the design needs to take place.

The following flowchart documents the combined Design and SIL Verification process.

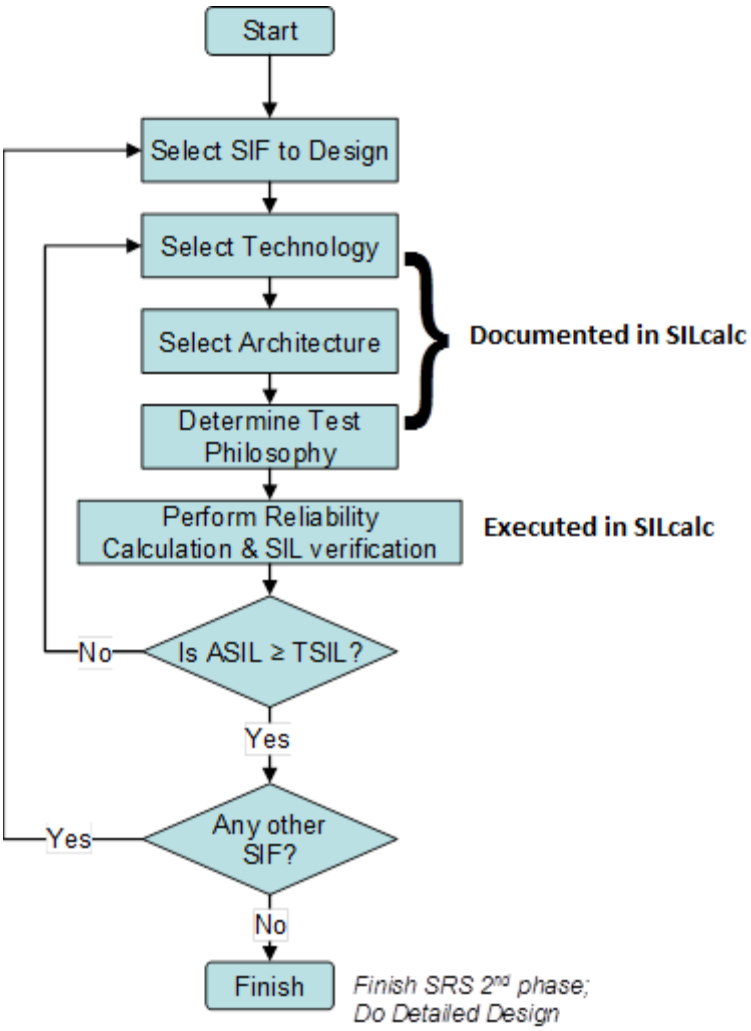

FIGURE 1: SIF DESIGN & SIL VERIFICATION PROCESS

5.1 Overview of SIF Design Tasks

For each Safety Instrumented Function (SIF) identified:

1. Review the Safety Requirements Specification and obtain an understanding of the requirements on the SIF that needs to be designed
2. Select equipment to be used in the SIF
   - o IEC 61508 certified equipment required
   - o Proven equipment, documented justification needs to be generated for each equipment item.
3. Gather and adhere to the Safety Manuals for all equipment items selected
4. Create design
   - o Select Architecture
   - o Specify Test Philosophy
   - o Identify potentially SIF level diagnostics
5. Document Design

5.1.1 Review of SIF Component Selection

Sensors/Logic Solver/Final Element
All SIF components shall be certified per the requirements of IEC 61508 unless documented justification is created to verify sufficient proven in use capability.

5.1.2 Unique Design Requirements Required for SIL Verification

Each SIF shall be designed with the specified equipment to meet the target proof test interval as specified in the SIF SRS. Equipment redundancy in fault tolerant voting configurations (e.g. 1oo2, 2oo3, etc.) may be added as necessary to meet the target SIL and the target proof test interval.
.

Additional diagnostics can be considered whenever practical to reduce redundancy requirements or increase proof test intervals. These may include:

a. Comparison of sensor signals from the same process variable
Deviation alarm credit can be utilized. The assumption is that the deviation alarm is treated as critical and appropriate action taken within the MTTR.

b. Partial valve stroke testing (PVST) on final element

c. Full (full open to full close or vice versa) on-line stroke test of valves.

Based on the SIF component safety manual, proof tests recommended by the manufacturer, proof tests conducted in the field an appropriate Diagnostic (proof) Test Coverage (DTC) must be determined.

5.1.3 Documentation of Design through SIL Verification

The design decisions are documented using the through selections made in the SILcalc SIL verification tool.

As part of the design documentation a SIS Identification (System ID), SIF Name, a SIF Tag (SIF ID), should be specified as a minimum.

For the documentation of the design it is important to have an understanding of the SILcalc structure to ensure correct documentation of the design. The SILcalc structure is shown in Figure 2 for normal configurations.

5.2 SIL Verification Overview

A typical SIS consists of sensors which measure process variables (i.e., level, pressure, flow, temperature, etc.), a logic solver, which is configured to recognize hazardous conditions and initiate Critical Safety Actions, and final elements such as solenoid valves, shutdown valves and motors. These final elements are driven by the logic solver to eliminate the unwanted process condition that, if not corrected, would lead to a hazardous condition. They are the minimum needed to bring the process to the safe state.

Since the design is documented in the SILcalc SIL verification tool, the process of SIL verification is rather trivial, but it will involve the following:

1. Determine all input information
    a. General information, like ISA Architectural Constraints requirements, MTTR, etc.
    b. Failure rate data
2. Compare Achieved Safety Integrity Level with Target Safety Integrity Level
3. Suggest areas for improvement in case conceptual design does not meet the Target Safety Integrity Level
4. Document results

In the Design step, the Safety Instrumented Function is documented in SILcalc, this means that voting arrangements and equipment item selections have already been made. The following provides an overview of required input information.

5.2.1 SIL verification SIF Level Selections

This information applies to the entire Safety Instrumented Function

Input for ISA 84 Architectural Constraints Determination	If any of the SIF components (Sensor, Logic Solver, or Final Element) has ISA selected, the 5 user selections will be available. Otherwise, the user selections will be unavailable.
Consider IEC 61508 Systematic Capability	The Systematic Capability as defined in IEC61508 can be considered. If "**Yes"** is selected, the final Achieved SIL will reflect the overall SIF Systematic Capabilities. The Achieved SIL will be limited up to the Systematic capability of the SIF. If selected as **"Yes"**, the Sys. Cap. "Prior Use" selection is available for the SIF Parts
MTTR	The Mean Time To Restoration (MTTR) indicates the average time it will take to repair a diagnosed fault. **Enter a value between 10 - 100**

5.2.2 SIL Verification SIF Parts Selections

This information applies to selections common to the Logic Solver part, Sensor part and Final Element part. The design will consist of up to four sensor groups and up to four final element groups. The voting between these groups should already have been specified during the design phase. As part of the SIL verification step the common cause / beta factor between the various groups needs to be established.

100% TI	This is also referred to as the Mission Time. The Mission time is the interval at which the SIF components are brought to a like new state. This is also considered the period over which the SIF parts will operate. **Enter a value between 1 – 30 Years**
Architectural Constraints	Architectural constraints can be considered. **IEC 61508:2010** can be utilize for SIL Certified (designed to IEC61508) sensors, Logic Solvers, and Final Elements as this provides the most appropriate evaluation of hardware redundancy. IEC 61511/ISA 84 **(ISA)** can be considered for SIF components not designed to IEC61508 standards or where SIL Certified devices are not used. The standards allow the practitioner to use either one (IEC61508 or ISA).
Beta %	Indicating the percentage of failures of an equipment item that is susceptible to a common cause failure if the equipment item is used in a redundant architecture. The beta-factor is not applicable to non-redundant configurations. **User selections are 0 – 10% in 1% increments**
Proof Test Coverage (DTC) %	Required to account for imperfect testing methods. **Enter a value between 10 and 100 in increments of 1.**
TI (Mo.)	Indicating the frequency in Months that the imperfect test DTC % will take place. This test interval cannot exceed the 100% TI. **Enter a value between 1 – 360 months**

Sys. Cap. "Prior Use"	If Systematic Capabilities is selected as "Yes" (see 5.2.1), then the user can select from the following: • "**N/A",** selected if you do not want to consider Systematic capabilities for this SIF part • **"Certified Device Claim"**, selected if SIL certified devices are used and the certification states the Systematic limit (1, 2, or3) • **"1, 2,or 3",** selected if you are claiming Prior Use, select the highest SIL level you want to use the device in a SIF. • **"1/2",** selected if you are claiming Prior Use, the maximum allowable for a single (simplex) SIF component is SIL1. If the architecture is N+1 (2) or greater the SIL is limited to SIL2. • **"2/3",** selected if you are claiming Prior Use, the maximum allowable for a single (simplex) SIF component is SIL2. If the architecture is N+1 (2) or greater, the SIL is limited to SIL3.
Sensor/FE KooN Voting	Practitioner can input values if KooN is selected on the Solver voting section. • for K enter a value between **1 and 100** • For N enter a value between **1 and 100**
Component Voting (Level 1)	Group voting level 1. Select from the drop down **"1oo1, 1oo2, 2oo2, 1oo3, KooN, etc."**

5.2.3 SIL Verification Sensor Component Selections

This information applies to the sensor selections. The practitioner will select the SIF components and details specific to the SIS application software and alarming. Selections made here can further improve the PFD results

Sensor Alarm	If any of the sensors selected are analog, this will apply if the fail low/high failure rate data is defined. Select **"Over Range"** if the transmitter failure state is set to High. Select **"Under Range"** if the transmitter fail state is set to Low.
PLC Alarm	If any of the sensors selected are analog, select **"Yes"** if the logic solver application software is configured to alarm on the above sensor alarm. Otherwise select **"No".**
Alarm Vote to Trip	If the logic solver application program considers the fault as a trip, set to **"Yes".** Set to **"No"** if the logic solver application program is not configured to detect a transmitter failure. The fail state direction is defined in Sensor Alarm O/U. See above
SIF Trip H/L	If the SIF is protecting against a high process condition, select **"High"**. If the SIF is protecting against a low process condition, select **"Low"**.
Dev Alarm	The standard allows additional diagnostic credit for if there are more than one device measuring the process variable. If there is an alarm that is comparing multiple sensors and an alert is annunciated when the sensor values deviate by some amount, select **"Yes"**. If not select **"No"**.
Deviation Alarm Coverage	If deviation alarm "Yes" is selected, enter a value between**"10 – 100".** The value represents the percent of the Dangerous Undetected failures that are detected by the deviation alarm.

5.2.4 SIL Verification Logic Solver Selections

There are no specific Logic Solver selections other than selecting the type of solver being used.

5.2.5 SIL Verification Final Element Selections

This information applies to the final element selections. The practitioner will select the SIF final element components and details specific to the final element. Selections made here can further improve the PFD results

Component Voting (Level 2)	This is the minimum number of final element components that are required to bring the process to a safe state. Select from **"1oo1, 1oo2, 2oo2".** See the Component Voting (Level 1) under 5.2.2.
Trip Position	Select **"Close"** if the final element trip state is closed Select **"Open"** if the final element trip state is open
Valve - Tight Shutoff	Select **"Yes"** if the hazard will not be mitigated if seat leakage occurs. Select "**No"** if leakage though the valve will not result in a safety event.
Valve - Service	Generally valves are specified to meet the process conditions "**Clean"**. Severe service may be considered if the valve will be operating at an upper or lower design limit that can adversely affect the performance of the valve. If this is the case, select **"Severe"**