

Methodology of SIL Study in Petrochemical Industries Projects (Used for Shiraz 3th Ammonia Plant)

By : Arash Banasaz - Safety and Process Senior Engineer
Petrochemical Industries Design and Engineering Company – PIDECC – Shiraz
BANASAZ.ARASH@PIDECC.COM

Abstract: This Paper defines the methodology to be used for carrying out the Safety Integrity Level-SIL in petrochemical Industries. This paper has been prepared to detail the overall procedure and the organization of the task for Shiraz 3th Ammonia Project. Generally this will be based upon the qualitative method (Risk Graph) described in BS IEC 61508 – Part 5, “Functional safety of electrical / electronic / programmable electronic safety-related systems – Examples of methods for the determination of safety integrity levels.

Key Words: HSE , Petrochemical Industries , SIL Study , Process , Safety , Shiraz Ammonia

1. Introduction

The primary objective will be to check the capability of the identified Safety Instrumented Function (SIF) to reduce the risk to achieve the functional safety for the E/E/PE Safety Instrumented Systems as defined by BS IEC 61508, which have the potential for harm to personnel (through illness and injury or loss of life) or damage to asset or to the environment (temporary or permanent).

During the Design phase, a Hazard and Operability Study should be performed as described in IEC-615882 as one of the methods referred in the BS IEC-61508 part 5 (risk matrix) so in Detailed Engineering phase will revise and update the study to take into account the change carried out in the safety related system.

2. SIL Identification

The SIL assessment will provide a formal review of the safety instrumented function as mentioned in the P&ID (Piping and Instrument Diagram) and the C&E (Cause and Effect) matrix to:

- Identify risks to persons, asset and, environment from potential hazards associated with the process and systems employed on the plant due to SIF failure and
- Define the basic performance requirements of the safety instrumented systems to reduce these risks to As Low As Reasonably Practical (ALARP).

Safety Instrumented Systems will be defined as a system comprising Electrical, Electronic or Programmable Electronic components, which are used to carry out safety functions. This definition specifically includes ESD (Emergency Shut Down) systems and HIPP's (High Integrity Pressure Protection). It may also include Fire and Gas Systems if the system both contains E/E/PE components and initiates an executive action.

A SIL Study report should be issued documenting the review meeting and included a list of all reviewed E/E/PS Safety Instrumented Functions with the required SIL level. The report included, as an attachment, legible copies of the SIL Work Sheets.

During the EPC (Engineering Procurement Construction) phase, after the HAZOP, Contractor shall provide the Electronic/Electrical or Programmable Electronic (E/E/PE) Safety Related systems (including instruments and Actuators) that require assignment of a Safety Integrity Level as required by IEC 61508 and further SIL review shall be performed on these identified systems.

All the new or changed SIF (as per IEC-61508 part 1) shall be identified, analysed and a SIL assessment shall be carried out following the methodology.

If the SIF has not changed from the FEED (Front End Engineering Design), the SIL assessment approved shall not be changed, unless the analysis of the assesment carried out are not still valid due to project or design changes or for other reasons identified by the Team.

3. Classification Process

IEC 61508 / 61511 require a more structured approach to full life-cycle management of a SIS (Safety Instrumented System). Specifically, they require a design methodology that:

- Removes uncertainty regarding the safety integrity, cost effectiveness and availability requirements;
- Provides traceability in the SIF design;
- reduces over-engineering;
- prevents under-engineering and therefore increases integrity;
- provides a basis for maintenance and operating strategies.

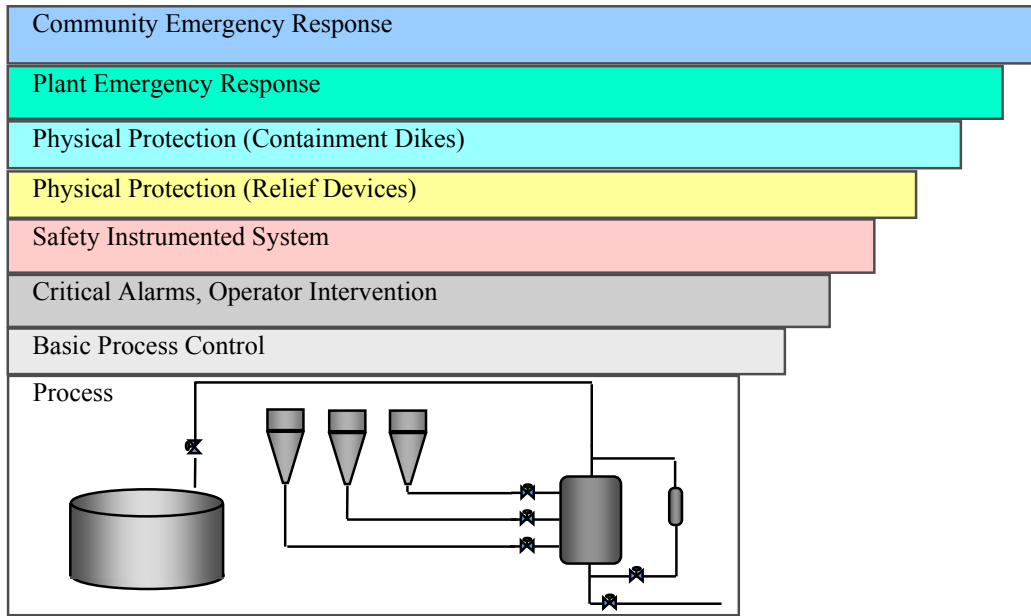
The initial risk associated with operating a process unit or a piece of equipment may be reduced by applying a range of risk reduction measures, including SIS. As shown in Figure, the summed contribution of reductions from all risk reduction measures must bring the remaining or residual risk to a level below the tolerable level.

Reduction can be achieved using a number of means, including mechanical devices (relief valves, bursting discs, etc.) and instrumented devices. In most designs, both types of protection systems are applied, with the mechanical system being the last line of defence wherever possible.

A SIF is required if the summed contributions of all non-SIF risk reduction measures do not reduce risks below the acceptable level.

The allocation of risk reduction to layers of protection (including SIFs) is done via proper design practice verified by Design HSE Review or HAZOP study.

SIF which require manual initiation (i.e. manual alarms and manual push-buttons) shall be excluded from the scope of the reviews.



Risk Reduction by Layers of Protection

3.1 Documentation Required

A well-developed issue of the following documents shall be available to the team performing the classification:

- Process and Instrument Diagram (P&ID);
- C&E (Cause and Effect) matrices
- SIF requirements specification;
- MOS (Maintenance Override Switch) list / POS (Process Override Swith) list
- Control Philosophy / Design Basis Document

3.2 SIL Composition

The team performing the SIL Assessment should be kept small. Competent personnel responsible for the subjects of process technology, process safety, I&C (Instrument & Control System), operations should form the team. Other disciplines shall be consulted when the SIFs of a particular engineering specialty are classified, e.g., rotating equipment specialists shall be consulted for compressor SIFs.

Ideally, the process technology and operations team members should be the same as those who participated in the Design HSE / Hazop review.

An Independent Leader in the use of the SIL assessment methodology will be appointed as facilitator. The task of the facilitator is to guide the team through the classification steps and to ensure that every step is recorded to the satisfaction of all team members before continuing with the next step.

3.3 SIF Identification

A SIF is a function implemented by means of instruments, from field to field, and intended to achieve or maintain a safe state for the process or mitigate consequences, in respect of a specific hazardous event.

A SIF consists of one or more initiators (including all components from the process connection to the logic system input), the logic solver (ESD and in the case of alarms, DCS), and one or more final elements (including all components from the logic system output card to the actuated device) and utilities such as power and instrument air supply required to perform the SIF.

The initiator(s) of a SIF are all the initiators that are required to detect the threat. This may be a single sensor or multiple sensors in a safe and/or dangerous failure robust architecture measuring the same parameter, or in some cases, multiple sensors that measure different parameters and together give an indication of the threat.

An Independent SIF shall be classified individually on the assumption that all other functions are operating properly.

SIL Assessment

The hazards and hazardous events of the EUC (Equipment under control) and the EUC control system shall be determined under all reasonably foreseeable circumstances (including fault conditions and reasonably foreseeable misuse). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC (see clause 7.4.2.3 BS IEC-61508 part 1).

If the SIF (as per IEC-61508 part 1) is not change from the FEED, the SIL assessment shall not be changed, unless the hypothesis and the analysis of the assesment carried out are not still valid due to project or design changes or for other reasons identified by the Team.

The SIL Assessment Team shall record in a clear and understandable way the reason of change in the SIL assessment of the SIF.

Records and Findings

SIL Assesment Team shall complete a Worksheet in order to record the findings and conclusions of the analysis.

All assumptions made shall be documented. Such assumptions typically concern manning levels and the ability of the operators to respond to upsets and alarms, as well as the economic losses caused by spurious trips and equipment damage.

References shall be included to documentation used during the classification, e.g., P&ID complete with revision, QRA report, HAZOP study, etc.

The worksheet shall be reviewed by the Team and approved by the Independent Team Leader.

The SIL Assessment Report shall be issued no later than 5 working days the end of the team activities.

4. SIF Validation and Implementation

The SIL of a function is the target integrity requirement for that function, or in other words the Risk Reduction Factor required for the function.

Based on the SIL, the function has to comply with the requirements for minimum fault tolerance and the probability of failure on demand (PFD) has to be better than the target PFD as given by the SIL (the probabilistic requirement).

The relationship between the SIL of the function, the required PFD is shown in below Table.

Relation between SIL and required PFD

Safety Integrity Level (SIL)	Required PFD
1	10^{-2} to $<10^{-1}$
2	10^{-3} to $<10^{-2}$
3	10^{-4} to $<10^{-3}$
4	10^{-5} to $<10^{-4}$

The required PFD can be achieved in various ways:

- Using equipment with a lower dangerous failure rate will reduce the PFD of the SIF.
- Reduction of the test interval and increase of test coverage will reduce the SIF PFD.
- Using equipment with good self diagnostic capabilities.

The purpose of a PFD calculation is:

- to calculate the required test intervals to fulfil the probabilistic SIL requirements taking into account a number of factors including architecture, dangerous failure rates, test coverage factor, etc;

The PFD of a SIF will be calculated using the following methods:

- IEC 61508 part 6 Annex B

5. Dangerous Failure Classification

- **Demand Rate**

After recording the consequences, the first question to be answered by the classification team is:

how often does the SIF "perceive" a genuine demand, i.e., what is the demand rate?

The first step in determining the demand rate is to determine the cause(s) of the demand on the SIF. The demand could be caused by any of a number of reasons, e.g., control instrument malfunction, operator error, loss of feed, etc. Each should be clearly documented in the SIF classification.

The next step is to determine the probability of the hazardous event taking place without the addition of any safety related system (but having in place external risk reduction facilities) this term W_i is the probability of the unwanted occurrence. Feed analysis the following scale and definition used:

W1: A very slight probability that the scenario will come to pass exists and only a few unwanted occurrences are likely (approximately once every 10-100 years).

W2: A probability that the scenario will come to pass does exist and a few unwanted occurrences are likely (approximately once every 1-10 years).

W3: A relatively high probability that the scenario will come to pass exists and frequent unwanted occurrences are likely (more than once every year).

- **Personnel Health and Safety**

To determine the personnel health and safety consequences, the following three questions shall be answered:

- What is the potential extent of human injury if the SIF fails on demand, i.e., when a hazardous situation occurs?
- What is the duration of presence (‘exposure’) of personnel in the area affected by the hazardous situation? They may be continuously present, for example if the demand occurs during local manual start or when the hazardous situation occurs after personnel have arrived on the scene to investigate a developing abnormal situation.
- What are the possibilities for the person(s) who may be injured to avert the hazardous situation (‘Possibility to remove danger’)? Credit should not be taken for personal protective equipment, unless it is certain that the protective equipment will be worn and will be effective.

During the FEED analysis to help the meaning of the consequence of the hazardous event on the operator was the following:

Ca	A minor reportable injury to 1 or more people
Cb	Serious, permanent injury to 1 or more people or a single death
Cc	Death to more than 1 person, but no more than 10 people
Cd	Death to more than 10 people

Frequency of, and Exposure time in, the hazardous zone (F)

For each safety consequence parameter, the SIL Review Team shall evaluate the frequency of, and the exposure time in, the hazardous zone for the operator with the following two parameters:

Fa: Rare to more often exposure in the hazardous zone.

Fb: Frequent to permanent exposure in the hazardous zone.

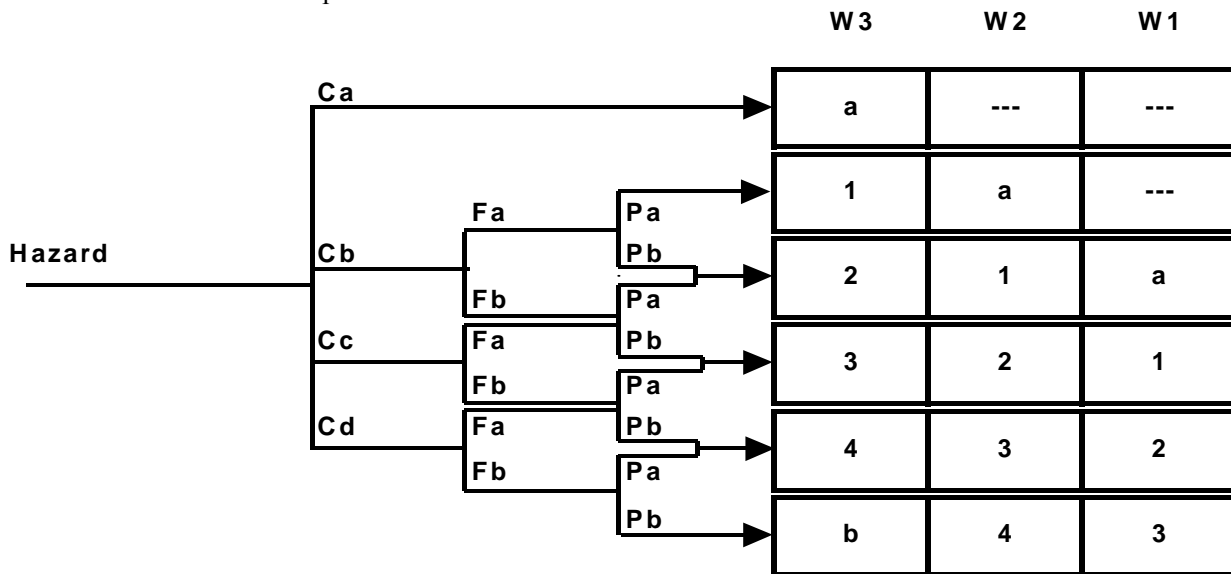
If the presence of persons is a prerequisite for the occurrence of a specific scenario, it should also be classified as Fb. This can be the case, for instance, during local start-up of certain pieces of equipment.

Possibility of failing to avoid the hazardous event (P)

In order to assess the risk from each safety scenario, the following two probability parameters shall be used:

Pa: It is possible under certain conditions to avoid the hazardous event, for instance by escaping.

Pb: It is almost impossible to avoid the hazardous event.



Risk Graph – Safety

- **Environmental**

The methodology determines environmental consequences as one of four categories:

- **Ea** An No perceivable damage to the environment and no adverse PR impact.
- **Eb** minor, but perceivable damage to the environment
- **Ec** Major temporary or minor long term damage to the environment
- **Ed** Major long term damage to the environment.

If flaring is within the allowable environmental limits as set by the local authorities, it shall be considered as having no environmental consequences for classification purposes.

If the result of the classification is Ea, the SIF is not required for environmental protection.

- **Economic**

For the purposes of classification it shall be considered as economic loss, e.g., cost of shutdown, loss of product and fines.

The methodology determines economical consequences as one of four categories:

- La Very minor economic loss.
- Lb Minor economic loss.
- Lc Significant economic loss.
- Ld Catastrophic economic loss.

A common accepted value for the economical loss is shown in the table below:

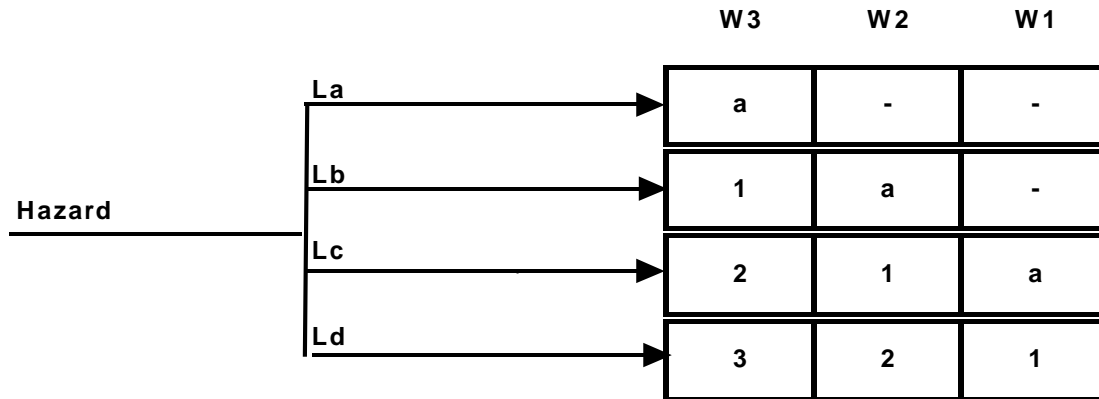
NOTE: THIS FIGURES ARE JUST TENTATIVE VALUES AND THE REAL ONES MUST BE CONCURED AT THE BEGINNING OF SIL STUDY MEETING BY ACCEPTENCE OF ALL TEAM MEMBERS THIS AFFECT THE SIL LEVEL.

Category	Consequence	Description
La	Minor Loss	≤ 10 MMS
Lb	Local Loss	>10 ≤25MMS
Lc	Major Loss	>25 ≤100MMS
Ld	Extensive Loss	>100 MMS

Economic consequences of failure on demand must take into consideration the summed total of all contributors to economic loss. This will include but not be limited to:

- Equipment repair or replacement cost;
- Labour cost required to effect replacement or repair;
- Losses associated with lost production, product give away or product quality shortfall;
- Fines or penalties imposed as a consequence of the failure;
- Clean up costs.
- Loss of inventory.

If the result of the classification is La, the SIF is not required for economic reasons.



Risk Graph – Economic

- **General Classification Rules**

The demand rate is intersected with each of the three consequence categories on the risk matrix to provide three SIL levels. The highest SIL resulting from the three consequences shall be selected for the SIF.

A SIF shall not be removed if the classification result is unclassified (i.e. no consequence of failure on demand), but with the Process Team and on the basis of the HAZOP study will be decide the right solution).

6. Conclusion

The safe failure classification should be performed after it has been decided what SIL is to be implemented, because implementation of the requirements related to the SIL may impact the safe failure rate of initiator or final element configurations.

7. Reference

BS IEC 61508 “Functional Safety of electrical / electronic / programmable electronic safety-related systems”