## *SIL ASSESSMENT STUDY BASIS AND METHODOLOGY*

### *STUDY BASIS*

The study was primarily based on:

- Process HAZOP Study Worksheets;
- Project Cause & Effect Diagram (C&ED) and Emergency Shutdown (ESD) Logic Diagram;
- Project Process & Instrumentation Diagrams (P&IDs); and
- Input from the SIL study team.

Additional supporting information will be derived from Equipment Data Sheets, Material Safety Data Sheets, and other information on a case by case basis.

### *DEFINITIONS*

The following terminology is applied for the SIL Study.

*Definitions of Specific Terms used for SIL Study*

| Terms | Definitions |
|---|---|
| *Safety Instrumented System (SIS)* | Instrumented system used to implement one or more safety instrumented functions (SIF). A SIS is composed of any combination of sensor(s), logic solver(s) and final element(s). The definition is used in IEC61511, and it is equivalent to the IEC61508 "E/E/PE Safety Related System". |
| *Safety Instrumented Function (SIF)* | Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function. A function comprises of one or more initiators, a logic solver and one or more final elements. |
| *Safety Integrity Level (SIL)* | Discrete level (from one to four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity Level 4 has the highest level of safety integrity; Level 1 has the lowest. |
| *Demand* | A process or equipment condition or event that requires the SIF to take action to prevent a Hazardous Situation. |
| *Hazardous event* | A hazardous event is a situation with the potential to cause harm, including ill health and injury, damage to property, products or the environment, production losses or increased liabilities |
| *Consequences of Failure (CoFoD)* | Ultimate consequences arising from a hazardous event if the SIF has failed on demand or the SIF is unavailable. |

| Terms | Definitions |
|---|---|
| *Initiator* | A device or combination of devices that indicates whether a process or equipment item is operating outside the operating envelope. |
| *Logic Solver* | The portion of a SIF, which performs the application logic function of the application logic function. |
| *Final element* | Part of a safety instrumented system, which implements the physical action necessary to achieve a safe state. |
| *Independent Protection Layers (IPL)* | Safeguards available that will reduce demand on a SIF in terms of reducing the frequency of the hazardous event and/or avert/decrease the consequence of the hazardous event. |

The evaluated Safety Integrity Level defines a minimum level of reliability (probability of failure on demand) to be guaranteed as shown in *Table 2.2* [1]:

### *Probability of Failure on Demand of SIL*

| Safety Integrity Level | Probability of Failure on Demand (PFD) |
|---|---|
| - | No safety requirement |
| a | No special safety requirement |
| 1 | $\geq 10^{-2}$ and $< 10^{-1}$ |
| 2 | $\geq 10^{-3}$ and $< 10^{-2}$ |
| 3 | $\geq 10^{-4}$ and $< 10^{-3}$ |
| 4 | $\geq 10^{-5}$ and $< 10^{-4}$ |
| b | A single SIF is not sufficient |

## SIL ASSESSMENT METHODOLOGY

### *Overview*

The SIL assessment workshop is a brainstorming exercise to determine the Safety Integrity Levels (SILs) to be assigned to the Safety Instrumented Functions (SIF) of the Timimoun facilities, based on an assessment of the risk of injury to people, potential damage to the environment or potential damage to the asset if the SIF were to fail on demand.

Each protection loop (i.e. SIF) analysed is considered to include:

- Initiating element(s), e.g. process sensors;
- Logic solver, e.g. ESD/PSS/FGS/PLC; and
- Final element(s), e.g. shutdown valve, machinery, etc.

The Assessment of the unrevealed failures (failures on demand) involved an assessment of the following:

- Potential extent of human injury;

- Potential extent of damage to equipment and equipment loss of production; and
- Potential extent of damage to the environment.

The assessment was performed by applying the risk graph method of IEC 61511-3. The risk graph method is based on the principle that risk is proportional to the consequence and frequency of the hazardous event.

The SIL is defined as a combination of the following 4 parameters:

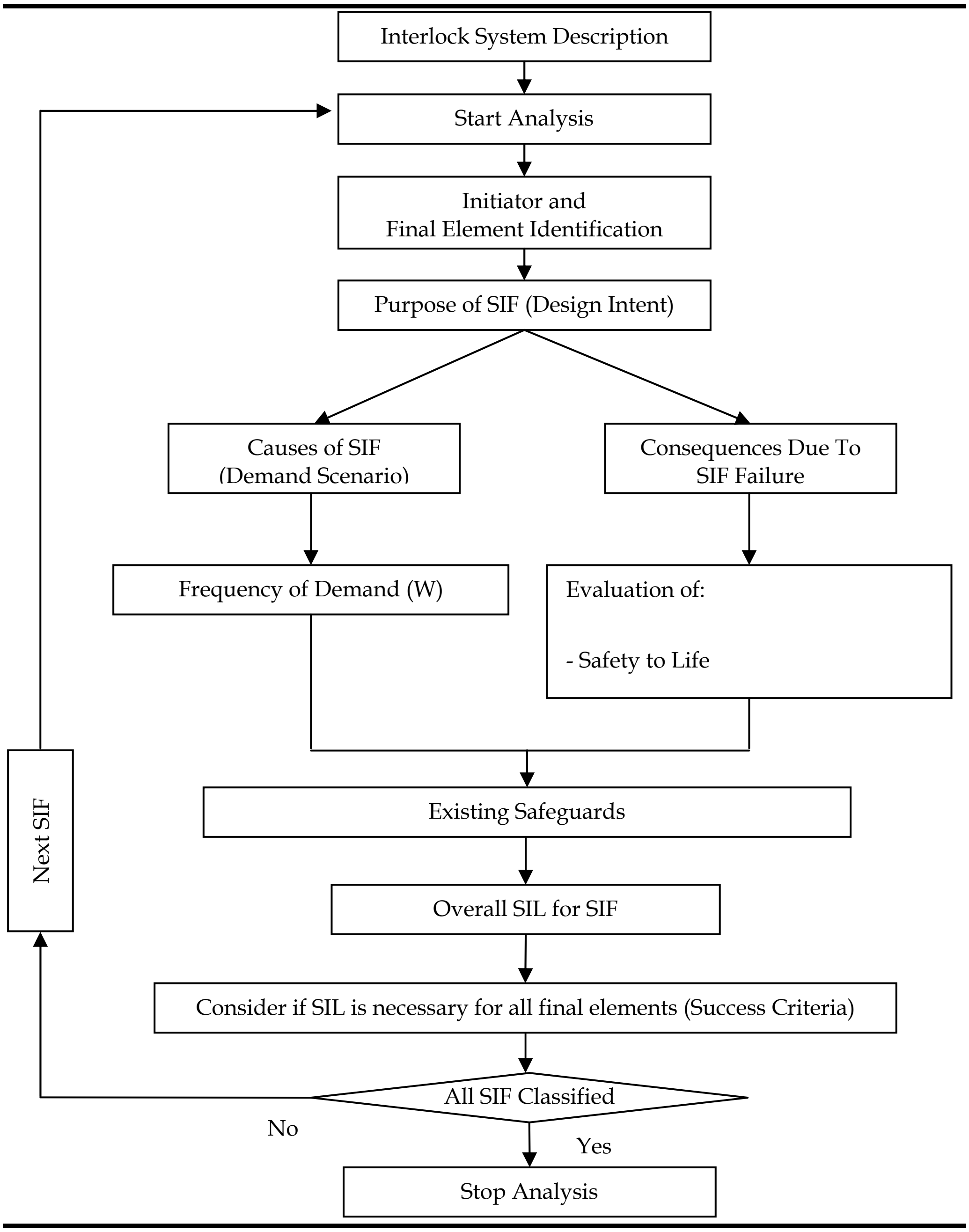
- The consequence of the hazardous event (denoted C for personnel safety, E for environmental, A for asset);
- Frequency of personnel presence in the hazardous zone multiplied by the exposure time (F);
- Possibility of avoiding the consequence of the hazardous event (P); and
- Probability of the unwanted occurrence (W) – without and with consideration of IPLs.

The stages of the study included (as shown in *Figure 2.1*):

- Identification of all typical automatic protection loops identified (SIF) based on Cause and Effects Diagram, P&IDs and ESD logic Diagram;
- Assessment of frequency (W) for protection demand rate;
- Assessment of consequences of failure on demand of the identified loops in an emergency scenario based on a risk matrix as per GS-EP-SAF-041, consequences are specified with respect to personnel safety, equipment damage/plant downtime and environmental impact;
- Identification of Independent Protection Layers (IPLs) and re-assessment of demand frequency (W); and
- Specification of SIL for each protection loop identified.

Different categories of C, E, A, F, P, W and risk graph to be used for SIL assessment are defined in the following context.

### *SIL Assessment Flowchart*




### *Description of SIF*

The ESD Logic Diagrams and SAFE Charts were first reviewed to identify the SIFs that required SIL Assessment. The identified SIFs have also been crosschecked with P&IDs and the HAZOP worksheets.

The following has also been identified during the workshop in order to correctly describe a SIF:

- The purpose (design intent) of the SIF – The design intent of a SIF is always to prevent the hazardous event;

- The causes of the demand on the SIF (demand scenario) (e.g. control valve failure, operator mistake) – the demand scenarios have been extracted from HAZOP study; and
- The consequences of the failure of the SIF (the consequence shall be taken as the difference between "success" and failure on demand) without giving consideration to the available safeguards.

*Multiple Sensors*

Where multiple sensors are provided, a success criterion is defined in terms of their performance in detecting the same hazard. For example, two sensors may be provided to detect high temperature in a vessel, in which case a success criterion of 1 out of 2 (abbreviated to 1oo2) may be assigned (i.e. only one sensor needs to be working in order to detect the hazard). However, if the SIL study team judges that there may be situations where both of the two sensors are required, then a more conservative 2oo2 success criterion may be selected.

*Multiple Final Elements*

For some SIFs, multiple actions are being taken, i.e. several final elements (valves, pumps etc.) are acted upon simultaneously. The success criterion of the SIF is defined in terms of how many elements must operate successfully in order to successfully put the system into a safe state. Thus, for example, for a SIF that closes a valve and stops a pump, if both actions are required to mitigate the scenario, a success criterion of 2oo2 would be assigned. However, for many SIFs, some actions may be secondary in nature, e.g. to prevent collateral hazards or to assist in restarting the unit quickly. These actions need not be considered in evaluating the SIL ranking of the SIF.

*Secondary SIFs*

Secondary SIFs are functions with only final elements and no additional physical sensors which protect against successful or inadvertent acting of one or more final elements. Successful operation of the (primary) SIF often create new hazardous situations and additional actions are required to prevent or mitigate the consequence of the (primary) action. The selected SIL only applies to the primary final elements and logic solver.

***Consequence of Failure on Demand***

*Personnel (C)*

The following table has been used as reference for evaluating consequences related to personnel safety during the workshop:

### *Damage Severity for Physical Injury*

| Consequence Parameter (C) | Severity Level | Definition | Parameter (PLL) * |
|---|---|---|---|
| $C_1$ | Minor | Medical treatment (light injury) | PLL = 0 |
| $C_2$ | Serious | Hospitalisation and damage to health | PLL ≤ 0.01 |
| $C_3$ | Major | Permanent injury eventually leading to one (1) fatality | 0.01 < PLL ≤ 1 |
| $C_4$ | Catastrophic | Multiple fatalities | PLL > 1 |

* PLL = Potential Loss of Life

### *Environment (E)*

The following table has been used as reference for evaluating environmental impact during the workshop:

### *Damage Severity for Environment*

| Consequence Parameter (E) | Severity Level | Definition | Comments |
|---|---|---|---|
| $E_0$ | Moderate | Spill or release of pollutant requiring a notification to plant management, but without environmental consequences. | A moderate leak from a flange or valve |
| $E_1$ | Serious | Serious spill within site limits. | A cloud of obnoxious vapour travelling beyond the unit following flange gasket blow-out or compressor seal failure |
| $E_2$-$E_3$ | Major/ Catastrophic | Significant pollution external to the site. Evacuation of persons. Important pollution with reversible environmental consequences external to the site. Notification to the Authorities. | A vapour or aerosol release with or without liquid fallout that causes temporary damage to plants or fauna |
| $E_4$ | Disastrous | Major and sustained pollution external to the site and/or extensive loss of aquatic life. | A vapour or aerosol release with or without liquid fallout that causes lasting damage to plants or fauna; Solids fallout (dust, catalyst, soot, ash) |

### *Asset (A)*

The following table has been used as reference for evaluating environmental impact during the workshop:

### *Damage Severity for Asset Loss*

| Consequence Parameter (A) | Severity Level | Asset Damage Intensity + Differed production duration |
|---|---|---|
| $A_0$ | Moderate | < €200,000<br>< 1 day delayed production |

| Consequence Parameter (A) | Severity Level | Asset Damage Intensity + Differed production duration |
|---|---|---|
| $A_1$-$A_2$ | Serious/ Major | €200,000 – 10,000,000<br>1 – 10 days of delayed production |
| $A_3$ | Catastrophic | €10,000,000 – 100,000,000<br>10 – 100 days of delayed production |
| $A_4$ | Disastrous | > €100,000,000<br>> 100 days of delayed production |

### *Occupancy*

The probability that the exposed area is occupied at the time of the hazardous event shall be defined. The F parameter is determined by calculating the length of time the area is occupied during a normal working period. This takes into account the possibility of an increased likelihood of people being in the exposed area in order to investigate abnormal situations which may exist during the build-up of the hazardous event. In this case, the parameter C shall be reconsidered.

$F_A$ has been chosen for scenarios that are spontaneous. $F_B$ has been selected for start-up and handling emergencies. F parameter is not applicable for evaluating risk to environment and asset hence $F_B$ is the default selection for environment and asset risk graphs.

The following table is based on IEC61511-3, Table D-2 [3]:

### *Occupancy*

| Occupancy Parameter (F) | Presence Factor |
|---|---|
| $F_A$ | Rare to more often exposure in the hazardous zone.<br>$F < 0.1$ |
| $F_B$ | Frequent to permanent exposure in the hazardous zone.<br>$F \geq 0.1$ |

### *Probability of Avoiding the Hazardous Situation*

The P parameter is defined as the probability that exposed people are able to avoid the hazardous situation if the SIF fails on demand. This depends on there being independent methods of alerting the exposed people to the hazard prior to the hazard occurring and there being methods of escape.

This parameter takes into account:

- Operation of a process (supervised (i.e. operated by skilled or unskilled persons) or unsupervised);
- Rate of development of the hazardous event (for example suddenly, quickly or slowly);
- Ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures);

- Avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions); and
- Actual safety experience.

### *Definition of Probability of Avoiding the Hazardous Situation*

| Probability Parameter (P) | Definition |
|---|---|
| $P_A$ | Possible under certain conditions.<br>$P_A$ should only be selected if **ALL** of the following are true:<br>• Facilities are provided to alert the operator that the protection has failed<br>• Independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area<br>• The time between the operator being alerted and a hazardous event occurring exceeds 1 hour or is definitely sufficient for the necessary actions. |
| $P_B$ | Almost impossible (no reduction in risk).<br>$P_B$ will be the default selection if no operational information is available. |

### *Frequency of Demand*

A demand on a SIF may be caused by instrument malfunction, operator error, etc. The following table, based on IEC 61511-3 Table D.2, describes the frequency of demand in qualitative terms: low, moderate and high.

### *Demand Rate*

| Frequency of Demand (W) | Definition |
|---|---|
| $W_1$ | Low ($W < 0.1$/year) |
| $W_2$ | Moderate ($0.1 \leq W < 1.0$/year) |
| $W_3$ | High ($W \geq 1.0$/year) |

CCPS and OREDA have recommended the following values for estimating the demand frequency. The SIL workshop has used these values as the default choices for respective demand scenarios.

### *Rule Set for Initiating Event Frequency*

| Initiating Event | Failure Rate (per year) | Demand Rate* | Reference | Demand Rate From FEED SIL Assessment |
|---|---|---|---|---|
| Turbine / Diesel Engine Overspeed with Casing Breach | 1.0E-4 | $W_1$ | LOPA-AICHE(CCPS) | - |
| Third Party Intervention (External Impact by Backhoe, Vehicle, etc.) | 1.0E-2 | $W_1$ | LOPA-AICHE(CCPS) | - |
| Crane Load Drop | 1.0E-4 per lift | $W_1$ | LOPA-AICHE(CCPS) | - |
| Lightning Strike | 1.0E-3 | $W_1$ | LOPA-AICHE(CCPS) | - |
| Safety Valve opens spuriously | 1.0E-2 | $W_1$ | LOPA-AICHE(CCPS) | $W_1$ |

| Initiating Event | Failure Rate (per year) | Demand Rate* | Reference | Demand Rate From FEED SIL Assessment |
|---|---|---|---|---|
| Single mechanical pump seal failure | 1.0E-1 | $W_2$ | LOPA-AICHE(CCPS) | - |
| Double mechanical pump seal failure | 1.0E-2 | $W_1$ | LOPA-AICHE(CCPS) | - |
| Tube rupture | - | - | - | $W_2$ |
| Centrifugal pump trip | 7.9E-1 | $W_2$ | OREDA | - |
| Positive Displacement pump trip | 1.1 | $W_3$ | OREDA | - |
| Compressor trip | 2.1 | $W_3$ | OREDA | $W_2$ |
| General utility failure | 1.0E-1 | $W_2$ | LOPA-AICHE(CCPS) | $W_2$ |
| Gasket/Packing Blowout | 1.0E-2 | $W_1$ | LOPA-AICHE(CCPS) | - |
| Isolation Valve Failure (mechanical failure) | 1.0E-2 | $W_1$ | SINTEF PDS Databook 2010 | - |
| BPCS instrument loop failure | 1.0E-1 | $W_2$ | IEC 61508 | $W_2$ |
| Unloading / Loading Hose Failure | 1.0E-1 | $W_2$ | LOPA-AICHE(CCPS) | - |
| Small External Fire (Aggregate Causes) | 1.0E-1 | $W_2$ | LOPA-AICHE(CCPS) | - |
| Large External Fire (Aggregate Causes) | 1.0E-2 | $W_1$ | LOPA-AICHE(CCPS) | $W_1$ |
| Process upset, blocked lines, etc. | | | | $W_2$ |
| LOTO (Lock-Out Tag-Out) Procedure* Failure<br>*Overall Failure of a Multiple-Element Process | 1.0E-3 per opportunity | $W_1$ | LOPA-AICHE(CCPS) | - |
| Operator Failure (if considered):<br>- Under stress, emergency, action performed more than once a quarter.<br>- Unstressed, action performed more than once a quarter.<br>- Under stress, emergency, action performed once/Qtr. or less<br>- Unstressed, action performed once/Qtr. or less | - | <br><br>$W_3$<br><br>$W_2$<br><br>$W_2$<br><br>$W_1$ | LOPA-AICHE(CCPS) | $W_2$ |
| Other Initiating Events | | - | To be determined based on group discussion | - |

* W values are selected based on project requirement shown in *Table 2.8*.

### *Independent Safeguards*

The provision of safeguards for the specific scenario has been reviewed. For each effective safeguard identified, a risk reduction factor has been determined. This risk reduction factor was then applied to the "originally identified frequency of demand". The study takes credit for the Independent Protection Layers (IPLs) that mitigate the likelihood or consequence.

The term 'IPL' refers to a safeguard which is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario.

There is a slight distinction however, in IEC 61511, between the terms 'protection layer' and 'independent protection layer'. Although both need to meet the criteria mentioned above, a safeguard may qualify as a 'Protection layer', if at least a factor of 10 risk reduction can be achieved while to qualify as an 'independent protection layer', a higher degree of reliability is required (i.e. reduces the identified risk by a minimum of 100 fold). The study uses the term 'IPL' for all protection layers, whose corresponding risk reduction factor will be determined based on the rule sets in *Table 2.10*.

Where an IPL is identified, the original event probability (W) was reduced. Also note that where more than one protective measure exists, the highest IPL credit was applied, without taking credit for all, as a conservative measure.

### *Risk Reduction Factors (RRFs)*

| Risk Reduction Measures | RRF | Comment |
|---|---|---|
| Relief Valves | 100 | Prevents system exceeding specified overpressure. |
| Rupture Disk | 100 | Prevents system exceeding specified overpressure. |
| Basic Process Control System (BPCS) | 10 | Can be credited as an IPL if not associated with initiating event being considered |
| Independent SIL1 SIS | 10 | See IEC 61508/ 61511 for life cycle requirements and additional discussion |
| Independent SIL2 SIS | 100 | |
| Independent SIL3 SIS | 1000 | |
| Human Factor | 10 | Process safety time available to take the action must be adequate, for instance:<br>1. Human Action with 10 minutes response time (Simple well-documented action with clear and reliable indications that the action is required)<br>2. Human Response to BPCS indication or alarm with 40 minutes response time (Simple well-documented action with clear and reliable indications that the action is required)<br>3. Human action with 40 minutes response time (Simple well-documented action with clear and reliable indications that action is required) |
| Independent alarm | 10 | Only if the response time is sufficient. |
| Dike | 100 | Will reduce the frequency of large consequences (widespread spill) of a tank overfill/ rupture/ spill, etc. |

| Risk Reduction Measures | RRF | Comment |
|---|---|---|
| Underground Drainage System | 100 | Will reduce the frequency of large consequences (widespread spill) of a tank overfill/ rupture/ spill, etc. |
| Open Vent (no valve) | 100 | Will prevent overpressure |
| Fireproofing | 100 | Will reduce rate of heat input and provide additional time for depressurizing/ firefighting, etc. |
| Blast-wall/ bunker | 1000 | Will reduce the frequency of large consequences of an explosion by confining blast and protecting equipment/ buildings, etc. |
| "Inherently Safe" Design | 100 | If properly implemented can significantly reduce the frequency of consequences associated with a scenario. |
| Double Check Valve | 10 | In accordance with GS EP SAF 361 (2012) |
| Flame/ Detonation Arrestors | 100 | If properly designed, installed and maintained these should eliminate the potential for flash-back through a piping system or into a vessel or tank. |

### *Risk Graph*

The frequency of demand (W) with consideration of IPLs, consequence level (C/E/A), exposure parameter (F) and potential for avoidance (P) have been mapped onto the risk graphs to give a SIL for each hazardous scenario. The most stringent SIL requirement based on the below graphs has been selected as the final SIL value for the SIF of interest. The risk graphs for this project are shown in *Figure 2.2* to *Figure 2.4* [1].

## *Risk Graph for People*

| Hazardous Scenario | | | $W_3$ | $W_2$ | $W_1$ |
|---|---|---|---|---|---|
| $C_1$ | | | a | - | - |
| $C_2$ | $F_A$ | $P_A$ | 1 | a | - |
| $C_2$ | $F_A$ | $P_B$ | 2 | 1 | a |
| $C_2$ | $F_B$ | $P_A$ | 2 | 1 | a |
| $C_2$ | $F_B$ | $P_B$ | 3 | 2 | 1 |
| $C_3$ | $F_A$ | $P_A$ | 2 | 1 | a |
| $C_3$ | $F_A$ | $P_B$ | 3 | 2 | 1 |
| $C_3$ | $F_B$ | $P_A$ | 3 | 2 | 1 |
| $C_3$ | $F_B$ | $P_B$ | 4 | 3 | 2 |
| $C_4$ | $F_A$ | $P_A$ | 3 | 2 | 1 |
| $C_4$ | $F_A$ | $P_B$ | 4 | 3 | 2 |
| $C_4$ | $F_B$ | $P_A$ | 4 | 3 | 2 |
| $C_4$ | $F_B$ | $P_B$ | b | 4 | 3 |

## *Risk Graph for Environment*

| Hazardous Scenarios | | | $W_3$ | $W_2$ | $W_1$ |
|---|---|---|---|---|---|
| $E_0$ | $F_B$ | $P_A$ | 1 | a | - |
| $E_0$ | $F_B$ | $P_B$ | 2 | 1 | a |
| $E_1$ | $F_B$ | $P_A$ | 2 | 1 | a |
| $E_1$ | $F_B$ | $P_B$ | 3 | 2 | 1 |
| $E_2$-$E_3$ | $F_B$ | $P_A$ | 3 | 2 | 1 |
| $E_2$-$E_3$ | $F_B$ | $P_B$ | 4 | 3 | 2 |
| $E_4$ | $F_B$ | $P_A$ | 4 | 3 | 2 |
| $E_4$ | $F_B$ | $P_B$ | b | 4 | 3 |

### *Risk Graph for Asset*

| Hazardous Scenarios | | | $W_3$ | $W_2$ | $W_1$ |
|---|---|---|---|---|---|
| $A_0$ | $F_B$ | $P_A$ | a | - | - |
| | | $P_B$ | 1 | a | - |
| $A_1$-$A_2$ | $F_B$ | $P_A$ | 1 | a | - |
| | | $P_B$ | 2 | 1 | a |
| $A_3$ | $F_B$ | $P_A$ | 2 | 1 | a |
| | | $P_B$ | 3 | 2 | 1 |
| $A_4$ | $F_B$ | $P_A$ | 3 | 2 | 1 |
| | | $P_B$ | 4 | 3 | 2 |

## ADDITIONAL SIL STUDY RULE SETS

In order to ensure consistency in the assessment, a few rule sets were agreed upon by the study team during the workshop:

- Based on manning level in Timimoun field, $F_B$ has been chosen for scenarios associated with operation in MP Compressors and GTG area;
- In case an independent alarm is available for a specific demand scenario and that sufficient time is allowed to avoid the hazardous outcome, $P_A$ is selected and no credit is given to this alarm as IPL;
- For F&G interlocks it should be demonstrated that best available technology has been adopted in case the required SIL should not be achievable; and
- In case of availability of PSV designed to prevent specific consequence of failure on demand, a direct reduction of 2 SIL levels is allowed as per GS EP SAF 361 (2012).

# SIL Study - Risk Graph

Function Name: 1. PSLL11005A/B/C (2oo3) downstream of HCV11003 initiating SD2-XXXXXW to close SSV11009 and ESDV11001.

Initiator(s): PT11005A; PT11005B; PT11005C; 2oo3

DWG No.:

| Design Intent | Demand Scenario | CoFoD | SIL (without IPLs) | | | | | Existing Safeguards / IPL | IPL Credit | Likelihood with IPLs | Target SIL | Recommendation | Resp. | Comment |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | C | F | P | W | SIL w/o IPLs | IPLs | | | | | | |
| Detect leakage in pipeline and isolate inventory. | Leak or rupture in pipeline downstream of wellhead ESDV due to random causes. | 1. Loss of containment of sour hydrocarbons, leading to potential fire/explosion. | $C_4$ | $F_A$ | $P_B$ | $W_1$ | SIL 2 | 1. PAL11004 upstream to PSV11007. (no credit taken on a conservative basis) | 0 | $W_1$ | SIL 2 | | | |
| | | 2. Same as above. | $E_2$ - $E_3$ | $F_B$ | $P_B$ | $W_1$ | SIL 2 | 1. PAL11004 upstream to PSV11007. (no credit taken on a conservative basis) | | $W_1$ | | | | |
| | | 3. Same as above. | $A_0$ | $F_B$ | $P_B$ | $W_1$ | --- | 1. PAL11004 upstream to PSV11007. (no credit taken on a conservative basis) | | $W_1$ | | | | |

Function Name: 2. PSHH1-11005A/B/C (2oo3) (HH1 set point is 52barg while the PSV is set at 57barg) downstream of HCV11003 initiating SD3-XXXXXW to close WV11011.

Initiator(s): PT11005A; PT11005B; PT11005C; 2oo3

DWG No.:

| Design Intent | Demand Scenario | CoFoD | SIL (without IPLs) | | | | | Existing Safeguards / IPL | IPL Credit | Likelihood with IPLs | Target SIL | Recommendation | Resp. | Comment |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | C | F | P | W | SIL w/o IPLs | IPLs | | | | | | |
| Protect piping downstream of choke valve from overpressurization. | Choke valve HCV11003 fails open (mechanical stop provided on HCV11003). | 1. Potential overpressurization of flowline downstream of HCV11001, leading to mechanical damage and loss of containment. However, rupture of piping is not credible because piping is rated for 239barg up to ESDV11003. It is considered that the rupture of piping can occur downstream ESDV11003 as it is rated for 57barg. | $C_4$ | $F_A$ | $P_B$ | $W_2$ | SIL 3 | 1. PSV11007 sized for choke valve failure case, considering the presence of mechanical stop on HCV11007 in accordance with API 521 4.4.8.3 (set pressure of 57barg). | 100 | $W_1$ | SIL 1 | | | The team agrees to allow reduction of 2 SIL levels in case of availability of PSV designed to prevent specific consequence of failure on demand. |
| | Downstream blockage. | | | | | | | 2. Piping is rated for 239barg up to ESDV11003. | | | | | | |
| | | 2. Same as above. | $E_2$ - $E_3$ | $F_B$ | $P_B$ | $W_2$ | SIL 3 | 1. PSV11007 sized for choke valve failure case, considering the presence of mechanical stop on HCV11007 in accordance with API 521 4.4.8.3 (set pressure of 57barg). | | $W_1$ | | | | |
| | | | | | | | | 2. Piping is rated for 239barg up to ESDV11003. | | | | | | |
| | | 3. Same as above. | $A_0$ | $F_B$ | $P_B$ | $W_2$ | a | 1. PSV11007 sized for choke valve failure case, considering the presence of mechanical stop on HCV11007 in accordance with API 521 4.4.8.3 (set pressure of 57barg). | | $W_1$ | | | | |
| | | | | | | | | 2. Piping is rated for 239barg up to ESDV11003. | | | | | | |

| | | | |
|---|---|---|---|
| | | SHEET: | |
| | | DATE: | |
| | **SIL ACTION SHEET** | SIF No. | |

| | | | | | |
|---|---|---|---|---|---|
| SIL Team: | | | | | |
| No.: | 5 | Description: | 28. LSLL32001 on Condensate Storage Tank initiating SD-3-32-03 to trip the loading pump. | | |
| Reference Drawings | | | | Action led by: | |

**Design Intent:**

Prevent loss of level in Condensate Storage Tank.

**Demand Scenarios:**

FIC33002 malfunctions and opens excessively FV33002.; Operator initiating loading operation in case of condensate tank level is low or empty.; Leakage from tank bottom.

**Consequence of Failure on Demand:**

1. Potential low level in Condensate Storage Tank leading to condensate pump running dry and mechanical damage.

**Independent Protection Layer:**

1. LAL32003 on Condensate Storage Tank.; 2. Retention bund provided around the tank. (Effective for environmental impact only)

**Recommendation:**

5. Ensure that the setpoint of low level alarm allows sufficient time between low level conditions and low low level trip (minimum of 10min) for operator action.

**Response:**

**Emptying hours between low level and low low level is 35 minutes as per 01SRF-TIMGEN-1000-CN-CA-000003 CN – VESSELS / TANKS / BASINS(refer to the attachment). . Therefore, enough time for operator action is provided between the high level alarm and high high level trip.**

| Comments: | | |
|---|---|---|
| PRO:<br>Agree. | ☑ Agree<br>☐ Agree with comments<br>☐ Disagree<br>☐ To be followed | Endorsed by:<br>Signed:<br>Date: |