HAZOP AND SIL STUDY PROCEDURE

BUSHEHR PETROCHEMICAL COMPANY MEG PLANT	
Document Review	
Issue Purpose:	AFC
Result Code: AP,AN,CM,RE,NC	AP
Next Status : IFC,IFA,IFI,AFC,AB	-
Responsible Department	MECHANICAL
Commented Date	Jul /17/2022
Approval or review hereunder shall not be construed to relieve Vendor / Subcontractor of his responsibilities and liability under the contract.	

Rev.	Date	Purpose of Issue	Prepared	Checked	Approved	AC Code
01	13/07/2022	Approved for Construction	KP	CL	JR	
00	24/09/2021	For information	KP	PW	LdM	

Class: 1 | Phase: P

TABULATION OF REVISED PAGES

Page	D00	D01	D02	D03	D04
1.	X	X			
2.	X	X			
3.	X	X			
4.	X	X			
5.	X	X			
6.	X	X			
7.	X	X			
8.	X	X			
9.	X	X			
10.	X	X			
11.	X	X			
12.	X	X			
13.	X	X			
14.	X	X			
15.	X	X			
16.	X	X			
17.	X	X			
18.	X	X			
19.	X	X			
20.	X	X			
21.	X	X			
22.	X	X			
23.	X	X			
24.	X	X			
25.	X	X			
26.	X	X			
27.	X	X			
28.	X	X			
29.	X	X			
30.	X	X			

Page	D00	D01	D02	D03	D04

INDEX

1. Scope

This procedure defines the techniques and methodology used for preparing conducting and documenting HAZOP and SIL study.

Once the HAZOP and SIL study are complete a report will be generated to document the findings and conclusions.

The focus for the HAZOP is:

- deviation on pressure conditions (lower or higher than operating)
- deviation on temperature conditions (lower or higher than operating);
- deviation on flow conditions (lower or higher than operating, reverse);
- deviation on liquid level (lower or higher than operating);
- deviation on composition (i.e., change of composition or contaminants);

After HAZOP is performed the SIL allocation study will be performed, Based on the assessment in the HAZOP for the requirement of a SIL allocation (LOPA). After SIL allocation is performed a complete report will be generated with findings and conclusions.

HAZOP and SIL study can only be performed after approval of the following document

- P&ID
- Cause and effect chart
- Control philosophy

2. Team organisation and responsibility

Vendor will arrange the HAZOP and SIL team consisting of the following persons

- TEAM LEADER, (Technical project manager) responsible for the overall execution of the HAZOP and SIL study
- CHAIRMAN (QA / QC Manager or Technical project manager)
    - Deciding the division of the Piping and Instrument Diagram (P&ID) into nodes suitable for reviewing one at a time for HAZOP
    - Leading the team of studies with appropriate guidewords.
    - Ensuring that the procedure is followed and that the notes and results of the study are properly recorded and distributed.
    - Resolving any conflict that may arise during the study.
    - Ensuring that the team works forward a common goal by utilizing expertise of all team members.
    - Ensuring the progress of the study.

- SCRIBE, to record the result of the HAZOP and SIL

The CONTRACTOR / COMPANY is required to provide suitably qualified and experienced personnel who have a detailed knowledge of the way in which the design is intended to work to attend the HAZOP and SIL, with at least the one of each of the following disciplines:

- Process engineer
- Commissioning engineer
- Operations representative

The HAZOP study Team (excluding the Chairman and Secretary) should be limited to the strict necessary wherever possible (max 8 people).

3. Overview HAZOP technique

Hazard and Operability (HAZOP) study is performed to identify all the process deviations, from the design intent, and to identify and estimate the correspondent consequences on people, assets, and environment.

The HAZOP technique is qualitative. It is not intended, nor is it necessary, to apply quantitative probability numbers to the hazards that are identified.

The technique is a highly disciplined procedure and is concerned only with the adequacy of a proposed design and not with the merits of alternative designs.

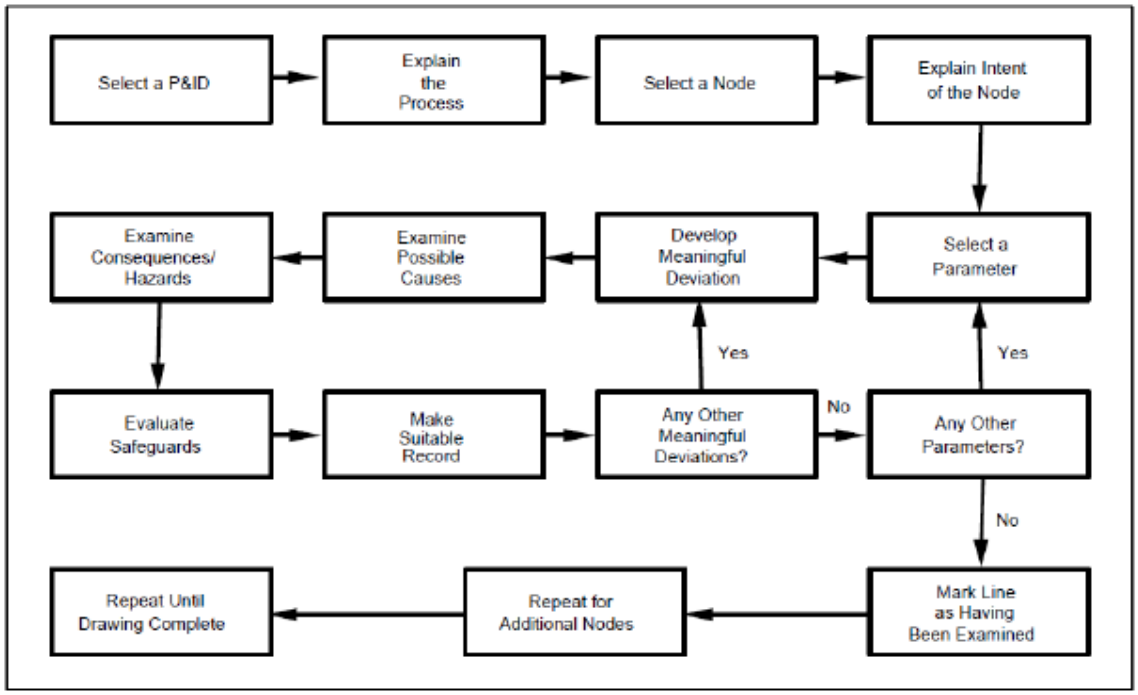
Therefore, the emphasis in the HAZOP study is on identifying potential problems, not necessarily solving them. However, if obvious solutions are apparent, the team can propose these.

The HAZOP technique is a guideword approach. The guidewords are used to provide structure to the technique.

1.1 HAZOP Review session

The HAZOP study is performed through a review session. The study session is the most essential step in the HAZOP Technique as this is where the group reviews and discussions are held.

Before starting the HAZOP session, an short briefing led by the HAZOP chairman shall be done. This preliminary briefing serves to highlight the battery limit, the nodes, possible scenarios and golden rules to be applied during the HAZOP session study itself. Chairman will briefly remind the scope and technique of HAZOP to all participants. The routine of the study sessions is shown below.



1.2 Select and Describe Node to be reviewed

A node is a section of a process unit generally consisting of piping and vessels that allows the study team to assess equipment in an organized fashion. The Technical project manager shall describe the purpose and design of the particular node. At this point important criteria for the node shall be specified. From the description of the node purpose or intention, the relevant parameters to be reviewed for this node shall be determined.

1.3 Select Parameters

The team then chose a parameter for the selected node. Several relevant parameters may be chosen by the team to be explored for one node. However, only one parameter can be applied at one time for one deviation. The following Process parameters describe the process intention of vessels, piping or other equipment in specific terms:

- FLOW
- PRESSURE
- TEMPERATURE
- LEVEL
- COMPOSITION
- OTHERS

1.4 Apply guidewords

One guide word shall be applied to a relevant parameter to develop meaningful deviations. For one node and parameter, more than one guide word may be available to determine more than one deviation. However, only one guide word can be applied to one node's parameter to generate one deviation. Therefore, many deviations may stem from one parameter of a node, and each node can have several parameters.

The guide words are the tools that are used to systematically direct the HAZOP review session of the integrated study. They are words or phrases that, when considered together with a parameter, form a hypothetical deviation for the team to consider. The basic guide words and phrases are represented in the following Table 1:

Guide Word	Meaning
NO	Negation of the design intent (e.g., no flow when there should be; no pressure when there should be
LESS	Less of a physical property than there should be —quantitative decrease (e.g., lower flow rate than there should be)
MORE	More of a physical property than there should be —quantitative increase
PART OF	Composition of the system (stream) is different than it should be —qualitative decrease (e.g., less of one component)
AS WELL AS	More components present than there should be—qualitative increase (e.g., extra phase or impurities present)
REVERSE	Logical opposite of the design intent (e.g., reverse flow)
OTHER THAN	Complete substitution (e.g., transfer of a material other than the material intended; transfer of a material to a location other than intended)

Table 1: Guidewords for HAZOP

1.5 Determine Deviations

Deviations are departures from the design intention which are discovered by systematically applying the guide word/parameter combinations to study the process.

At this stage of the HAZOP review session the team determines if the deviation is credible (i.e. there is a cause), and proceed to review the consequences. Causes are the reasons why deviations might occur. Once a deviation has been shown to have a conceivable or realistic cause, it can be treated as meaningful.

Table 2 combines a sample of the guidewords and process or design parameters into a matrix of common deviations that will be considered during the HAZOP review session of the integrated study. As can be seen from the chart, some guide word/parameter deviations are not meaningful, such as "reverse temperature" or "as well as pressure." The Team shall document which deviations were used and dismiss those which were considered

	More Of	Less Of	None Of	Reverse	Part Of	As well as	Other than
Flow	High Flow	Low Flow	No Flow	Back Flow	Wrong Concentration	Contaminants	Wrong Material
Temperature	High Temperature	Low Temperature					
Pressure	High Pressure	Low Pressure					
Level	High Level	Low Level	No Level				

Table 2: Deviation Matrix

1.6 Examine consequences

Consequences are the results of the deviations should they occur. The potential consequences of each deviation will be discussed and assessed within the limits of the information available and the expertise of the team. The potential consequence threats will be assessed without considering operator or instrument intervention or any mitigation or safeguards. Consequences will focus on possible major effects in terms of personal safety, environment and production/equipment loss.

A risk ranking will be assigned by the HAZOP Team considering the safeguards identified for each selected scenario, according to the likelihood of the initiating cause and the severity of the consequences, in order to prioritize the recommendation for implementation.

Consequence Categories & Indices			Consequence Indices				
			C_0	C_A	C_B	C_C	C_D
			Insignificant	Low	Medium	High	Very High
	Consequence Descriptions	Safety (S)	Minor Injury or Damage to Health	Mild to Moderate Injury with Some Treatment but Medically Manageable	Serious Illness or Chronic Exposure Resulting in an Employee Fatality or Significant Life Shortening Effects	Employee Fatalities and Mild Health Impact on Third Parties.	Multiple Employee and Third Party Fatalities
		Environment (E)	No Impact	Localized Short-Term Effect on the Environment, Habitats and Species	Localized Long-Term Effect on the Environment, Habitats and Species	Severe Damage to the Local Environment, Habitat, Species	Contamination Over Large Public Areas with Loss of Significant Ecosystems Effecting Inhabitants, Habitats or Species.
		Economic (L)	Operational Upset. Loss Less than $1 million	Minor Damage to Equipment and Downtime. Loss up to $10 million	Serious Asset Loss, Damage to Facility and Downtime Requiring Partial Shutdown. Loss up to $100 million	Severe Asset Loss or Damage to the Facility with Appreciable Operation Loss. Loss up to $500 million	Significant or Total Destruction of the Facility. Asset Loss above $500 million

Table 3: Consequence Categories

Safety (S)
Includes Personal Safety - injury or fatality and Health - short term and long-term illness as a result of personal exposure to the event including exposure to land, air or water of harmful materials.

Environment (E)
Includes Fines, rehabilitation and clean-up costs both short and long term for affected plants and animals exposure to land, air and water.

Economic (L)
includes:

- Equipment repair & replacement costs, Labour costs for design, procurement, installation
- Lost production, product giveaway, product quality loss associated with asset damage
- Fines and penalties because of the failure

- Clean up costs

- Loss of inventory
- Loss of contracts, purchase orders, business relationships
- Loss of goodwill

Risk ranking will be done according to the following Table 4.

Likelihood Descriptions			Consequence Indices				
			C_0	C_A	C_B	C_C	C_D
Scenario Descriptions	Likelihood Indices		Insignificant	Low	Medium	High	Very High
Expected to occur in the life of this facility	1	Likely	alarp	alarp	alarp	HIGH	HIGH
May occur in the life of this facility	2	Occasional	LOW	alarp	alarp	alarp	HIGH
An event has occurred in Saudi Aramco but not likely in this facility	3	Seldom	LOW	LOW	alarp	alarp	alarp
Some events have occurred in the industry but not likely in this facility	4	Unlikely	LOW	LOW	LOW	alarp	alarp
Rare or never heard of in industry.	5	Remote	LOW	LOW	LOW	LOW	alarp

Risk level	**Tolerability**
LOW	Implement measures to maintain risks at this level; improve through administrative measures
As Low As Reasonably Practicable, ALARP	Risk must be reduced based on cost benefit
HIGH	Risk must be reduced at any cost by applying engineering controls

1.7 Discuss Safeguards

Safeguards are layers of protection / barriers that will prevent the failure scenario from occurring or mitigate the consequences if it occurs. The team will identify safeguards that are effective in preventing or controlling the hazards.

The safeguards can be classified as Independent Protection Layers (IPLs) and non-IPLs. An IPL is a device, system or action that 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. An IPL may also include a Safety Instrumented Function (SIF). Safeguards are identified in order to reduce the severity of the consequences, or in order to reduce the likelihood of the initiating cause of the scenario. The former are MITIGATIVE safeguards, the latter are PREVENTIVE safeguards. In the HAZOP study all safeguards shall be listed down without consideration to their IPL value. IPL calculations and filtration of safeguards shall be carried out in the LOPA analysis.

1.8 Recommendations

Recommendations shall be given in HAZOP analysis as needed, in order to improve safety and / or Operability of the plant. Recommendations to be direct, clear, and based on reel need and added value.

Recommendations can be divided in two categories:

- "Provide an additional trip for Low Low Level…." or "PSV-xxx shall be sized for blocked outlet also…" are mandatory for the owner.
- "Consider adding an independent Transmitter…." or "Evaluate to remove the demister…." are subject to further analysis by Discipline Leaders and may lead to a different solution from what has been recommended, as well as the implementation or non-implementation of the recommendation.

It is not the HAZOP Team objective to find technical solutions to risk scenarios, but instead the focus shall be on recognize and circumstance the risk scenarios. If the recommendation points are an easy and shared solution, then it can be detailed in the analysis. Alternatively, the recommendations should be more open in order to let the Discipline Leaders follow up with the best solution.

1.9 Assumptions

The following HAZOP premises will be applied by all teams in order to ensure a consistent approach:

- Mechanical protection devices (PSVs, rupture discs) are expected to work as intended.
- No quantitative analysis will be performed during HAZOP meeting.
- If there is more than one train (identical) or pass, only one will be reviewed, considering they are identical.
- Check Valves will be accounted to with the same approach of ISO 23251, point 4.3.4.4.: "Experience has shown that when inspected and maintained to ensure reliability and capability to limit reverse flow, two back-flow-prevention devices in series are sufficient to eliminate Significant reverse flow. Check valves will be therefore considered as HAZOP safeguards as determined appropriate by the Team
- No design work will be done. If a design violation is clear then it should be noted for the correction in the separate design activities.
- Car sealed open / closed valves won't be evaluated for being inadvertently closed / opened, because they are managed by administrative controls (ISO 23251, 4.2.1). Car sealed open valve for RV's are assumed to be controlled according to COMPANY standard operational procedure.
- The following items will not be considered:
    - Simultaneous occurrence of two unrelated incidents (ISO 23251, 4.2.1)
    - Natural calamity (e.g. flood, earthquake)
    - Dropped objects on live line
    - Sabotage
    - Wrong design calculation (structures, equipment etc..) or disattended
- The facility will be subject to overall fire/gas leak scenario (e.g. emergency isolation) but any catastrophic rupture of equipment will be generally not considered as a cause except for tube rupture/seal leak, as determined appropriate by the Team;
- Company Operator shall be always considered well/deam trained;
- Equipment, piping and valves will be designed and installed as per installation code requirements;
- Incorrect position (open/close) of manual valves:
    - Unit BL valves will be assumed open;
    - Manual valves normally will be assumed normally not operated; therefore no investigation will be performed;
    - Manual valves, manual drains and vents: if provided for maintenance only, no investigation will be performed. In case of functional (operational) purpose (i.e. requiring periodical operation or running unit) items will be analysed.
- Utilities failure will be analysed localized on each node (e.g. non cooling water to heat exchanger). No
  general utilities (power, etc..) will be considered. This is included in the plant design;
- Loss of production means gas to flare.

2 HAZOP FOLLOW-UP AND CLOSE-OUT

All HAZOP recommendations that are recorded on the HAZOP worksheet will be shared with all involved parties in the form of a HAZOP register

	Recommendations (HAZOP)	P&ID	Place(s) Used	Responsibility	Implemented (Yes/No)	Closed/ Open	Process Status 09/10/19	Short Status
1								
2								

in this register all outstanding HAZOP points are tracked in case of closure of the points COMPANY / CONTRACTOR need to provide VENDOR with signed version to add in the Databook for record.

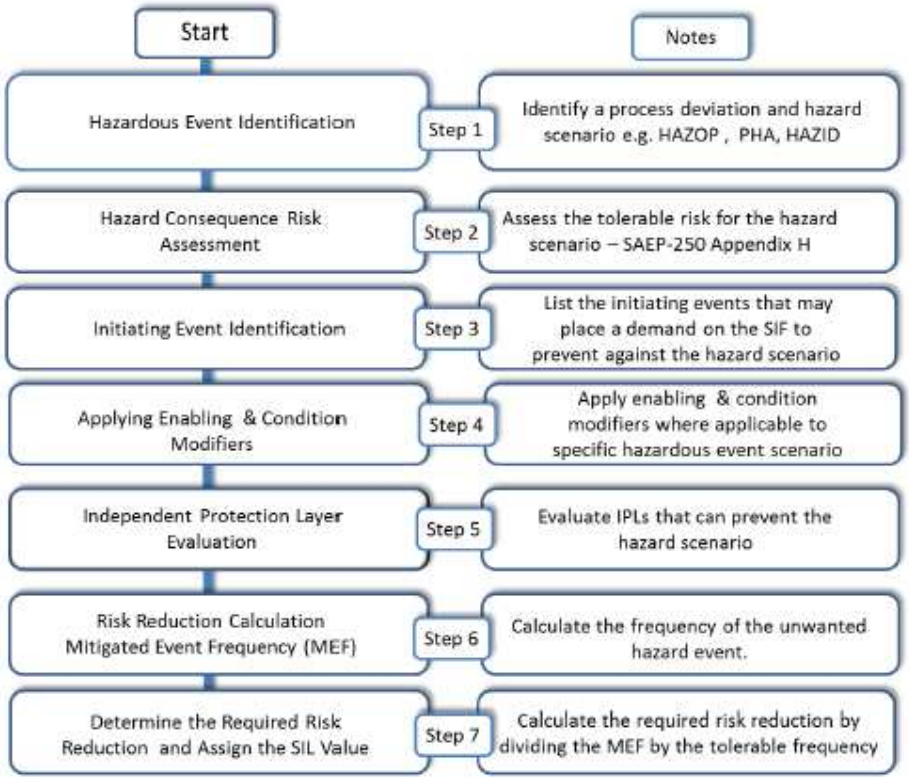
The following statuses are avaiable

OPEN: The Recommendation have not yet received an answer; (action to VENDOR)
ISSUED: The Recommendation has been answered, and the answer has been issued to COMPANY / CONTRACTOR for review and approval. (Action to COMPANY / CONTRACTOR)
CLOSED WITH ACTION: the Recommendation has been submitted to COMPANY with marked up documents providing evidence of early implementation. The answer is considered satisfactory by COMPANY. An action is pending to verify actual implementation of the recommendation once the official issue of the marked up document has been verified by CONTRACTOR.
CLOSED: the Recommendation has been submitted to COMPANY and the answer is considered satisfactory. In this case, No action is pending because implementation of the recommendation is either not needed or verified with officially issued documents.
REJECTED: the Recommendation have received an answer but said answer has not been considered completely satisfactory by COMPANY / CONTRACTPR (action to VENDOR).

3 Explanation of SIL methodology

LOPA is the engineering method used to assess the process risk of a specific safety function on a process and process equipment taking into consideration IPLs and other conditions which may reduce the frequency of the hazardous event. The objectives of this analysis are to assess protective functions and IPLs that will be relied on to prevent or mitigate the loss of containment and reduce the risk to an acceptable level.

Figure below shows the general steps the team should to complete a LOPA study



3.1 Hazard event identification

The first step for LOPA consists of identifying hazardous scenarios that may lead to loss of containment of combustible, flammable or toxic materials. The hazardous scenarios identified during the HAZOP session will be considered for conducting LOPA.

LOPA study will evaluate the scenario consequence to produce protection for all cases and to determine whether a SIF is required.

If the safeguards identified by the HAZOP team to mitigate the hazardous event will be estimated inadequate by the LOPA team, recommendations will also be made to further reduce the risk by applying additional independent protection layers including a safety instrumented function.

3.2 Hazard consequence risk analysis

The Risk Target Frequency for each of the severity levels of concern is provided in Table 1 Once the potential severity of the hazard scenario is defined, a Risk Target Frequency for the scenario shall be assigned. The Target Frequency shall be assigned to each scenario as applicable for safety, environmental and commercial severity levels.

Risk ranking performed during HAZOP session could be reviewed if deemed inadequate by the LOPA Team

Risk Target Frequency (yr^{-1})	Risk Indices	Category	Consequence Description
1×10^{-6}	C_D	Safety (S)	Multiple Workforce Fatalities (5-50) or Public Fatalities (1-10)
		Environment (E)	Contamination Over Large Public Areas with Loss of Significant Ecosystems Effecting Inhabitants, Habitats or Species.
		Economic (L)	Significant or Total Destruction of the Facility. Asset Loss above $500 million.
1×10^{-5}	C_C	Safety (S)	Multiple Workforce Fatalities (2-4) and Mild Health Impact on Public.
		Environment (E)	Severe Damage to the Local Environment, Habitat, Species.
		Economic (L)	Severe Asset Loss or Damage to the Facility with Appreciable Operation Loss. Loss (Asset and Operational) up to $500 million.
1×10^{-4}	C_B	Safety (S)	Serious Illness or Chronic Exposure Resulting in a Workforce Fatality or Significant Life Shortening Effects.
		Environment (E)	Localized Long-Term Effect on the Environment, Habitats and Species.
		Economic (L)	Serious Asset Loss, Damage to Facility and Downtime Requiring Partial Shutdown. Loss up to $100 million.
1×10^{-3}	C_A	Safety (S)	Mild to Moderate Injury with Some Treatment but Medically Manageable.
		Environment (E)	Localized Short-Term Effect on the Environment, Habitats and Species
		Economic (L)	Minor Damage to Equipment and Downtime. Loss up to $10 million.
1×10^{-2}	C_0	Safety (S)	No Injury or Damage to Health.
		Environment (E)	No Impact.
		Economic (L)	Operational Upset. Loss $100k - $1 million.

3.3 Initiating event identification

The initiating event causes that could lead to hazardous event scenarios are identified in the HAZOP Study. The LOPA Team will quantify the Initiating Event Frequency (IEF), in failures per year, for each initiating event cause. Table 2 provides default values for the IEF of common industry initiating causes.

Other values based on operating history can be considered based on LOPA Team discretion.

However, the rational for any deviation from the values in Table 2 (e.g. use of operating history) shall be documented in the LOPA study Report.

Initiating Causes	Conditions	IEF [Years]
Sensors		
Transmitter Spurious Failure – Level, Pressure, Temperature, Flow	Electronic level, pressure, temperature and flow transmitters may use the generic MTBF[a] values provided by Exida or as stated here, whichever is the more conservative value.	200
Switch Spurious Failure - Level, Pressure, Temperature, Flow	Electronic Level, pressure temperature and flow switches may use the generic MTBF[a] values provided by Exida or as stated here, whichever is the more conservative value.	48
Mechanical or Float Level Devices Spurious Failure	Caution: Mechanical or float type level transmitters and switches should be used with care in ESD service.	15
Electronic Servo Level Gauges	Electronic servo gauges may use the generic MTBFs values provided by Exida or as stated here, whichever is the more conservative value.	20
Sensors - Other	See Exida for generic MTBFs values for other sensors.	EXIDA
Control Function		
Control Loop Failure	BPCS failure causing a demand on the SIS for the given scenario.	10
Failure of Inline Pressure Regulator (PRV)	Local pressure regulator or pressure reducing valve in under periodic maintenance in clean service.	10
Field Mounted Pressure Controller and Valve (PCV)	Local pressure regulator controller under maintenance in clean service.	10
Final Control Elements		
Spurious Closure of a Fail-Safe Spring Return ZV	All failures that could potentially cause a spurious closure of a spring return ZV. Can be hydraulically operated, motor operated or pneumatic operated.	50
Spurious Closure of a Fail-Safe Double Acting ZV	Pneumatic actuator with air storage backup for 3 strokes.	60
Spurious Closure of a Gas Operated Valve	With either N2 backup or inline gas filters that have regular maintenance and alarm on low condition	30
Spurious Closure of a Motor Operated Valve		80

Initiating Causes	Conditions	IEF [Years]
(MOV).		
Spurious Failure of a Solenoid Valve		50
PZV Relief Valve Opens Early	Opening a PZV early that may result in an loss of containment scenario	100
Final Control Elements - Other	See Exida for generic MTBFs values for other final control elements.	EXIDA
Mechanical & Rotating Equipment		
Single Mechanical Pump Seal Failure	Partial or total failure that may result in sufficient loss of containment that potentially leads to a hazardous scenario.	10
Double Mechanical Pump Seal Failure	Total failure that may result in sufficient loss of containment to result in a hazardous scenario.	100
Magnetic Drive Pump Seal and Seal-Less Pumps	Total failure that may result in sufficient loss of containment to result in a hazardous scenario.	100
Gasket Packing Blowout	Total failure that may result in sufficient loss of containment to result in a hazardous scenario.	100
Centrifugal Compressor Trip	Spared equipment with one in standby with auto-start. Both compressors must fail and prevent adequate supply to downstream process, directly resulting in the potential hazard scenario.	10
	Single compressor or no auto-start on standby.	1
Reciprocating Compressor Trip	Spared equipment with one in standby with auto-start. Both compressors must fail and prevent adequate supply to downstream process, directly resulting in the potential hazard scenario.	10
	Single compressor or no auto-start on standby.	0.5
Pump Failure	Spared equipment with one in standby with auto-start. Both pumps must fail and prevent adequate supply to downstream process, directly resulting in the potential hazard scenario.	10
	Single equipment whose failure prevents adequate supply to downstream process, directly resulting in the potential hazard scenario.	1.6

Initiating Causes	Conditions	IEF [Years]
Other Mechanical & Rotating Equipment Failures	Consider the components used, and operating experience on the specific components.	-
Electrical Equipment		
Spurious Failure of an MCC Shutdown Relay		20
Loss of Single UPS power		10
Loss of Redundant UPS power	A redundant UPS shall have no single point of power loss in the circuits.	100
Loss of Electrical Power	Use operational values if they are available for the specific facilities otherwise 10 years. E.g. Total plant shutdown, Unit shutdown	10
Human Error		
Human Error	Error during normal operation where the person is trained on the required task and has procedures available and the individual performs the task more than once per week.	1
	Error during normal operation where the person is trained on the required task and has procedures available and the individual performs the task more than once per year and the task is independently checked for correctness. The task is performed less than once per month.	10
	Error during normal operation where the person is trained on the required task and has procedures available and the individual performs the task more than once per year and the task is independently checked for correctness. The task is performed less than once per year.	100
Other Process Equipment		
Parallel Cooling Pump Failure resulting in Loss of Flow	Spared equipment with one in standby with auto-start. Both pumps must fail and prevent adequate supply to downstream process, directly resulting in the potential hazard scenario.	10
	Single equipment with one in standby and no auto-start. Both pumps must fail and prevent adequate supply to downstream process, directly resulting in the potential hazard scenario.	1.6
Redundant Utility Failure (Steam, Instrument Air,	Redundant utilities must be capable to take up the full process load in the event of the failure of the primary.	50

Initiating Causes	Conditions	IEF [Years]
Cooling Water)		
Heat Exchanger Leakage	No moving parts, no vibration and non-corrosive service.	100
	Medium to high vibration.	10
Loading or Unloading Hose Failure	No moving parts and no vibration.	100
	Medium to high vibration.	10

3.4 Independent protection layers (IPL) evaluation

An assessment of each safeguard identified during the HAZOP will be undertaken by the LOPA Team to determine the amount of risk reduction provided by each safeguard, its dependability and its independence from other safeguards. Those identified as IPLs shall be then quantified during the LOPA. Risk reduction factors are
shown in Table 7 below

Only those protection systems that meet the following criteria shall be classified as independent protection layers, and therefore used in SIL studies. These criteria are:

- Specificity: the IPLs must be able to prevent or mitigate the consequences of the hazardous event;
- Independence: the IPLs must be independent of all the other protection layers such that the performance of the IPL is not affected by another protection layer or the conditions that could potentially cause another protection layer to fail.
- Dependability: the protection provided by the IPL must dependably reduce the identified risk by a known and specific amount.
- Auditable: the IPL must be such that it can be inspected, maintained and tested at regular intervals.

Independent Protection Layer (IPL)	Guidelines	Risk Reduction Factor (RRF)
BPCS Control Loop	Credit for a BPCS control loop/interlock in the same controller can credited once only with a risk reduction factor of 10 when meeting the following conditions: 1) The BPCS Control loop action must prevent the scenario by bringing the PV to the set point under control. 2) The BPCS Control loop components (sensor and final control element) shall be independent from other protective layers such as ESD. 3) The BPCS shall not be a cause of a dangerous failure on the SIF. 4) Failure of the BPCS Control loop shall not be initiating event cause. 5) The PCS must run in automatic mode during all operational phases where the hazard scenario exists. 6) Testing of the PCS instruments and final control elements must be part of the regular PM. 7) For a control loop controlling a pressure relief, the control valve must be sized to prevent the overpressure scenario. 8) The BPCS controller is redundant.	10
	A field local control loop with independent sensor and final control elements can also be credited with a risk reduction factor of 10 if the field control loop action mitigates the scenario by bringing the PV to the set point under control. The service shall be relatively clean with no or minimal history of instrumentation or control issues.	10

Independent Protection Layer (IPL)	Guidelines			Risk Reduction Factor (RRF)
Operator Response & Alarms	The criteria for qualifying an operator response to alarms as an IPL are : 1) There is sufficient process safety time (PST) to allow the operator to take action. As defined in this table. 2) The operator has capability according to the criteria listed below. 3) The alarm signal is from an instrument other than BPCS Control/Interlock loop 4) The final control element (valve, pump, compressor etc.) used to control the process is not the same used in the BPCS Control/Interlock loop. Note: 1) Alarm with operator response shall not be considered as an IPL when a BPCS control loop/interlock within the same controller has been already been determined as an IPL in the LOPA unless there is a separate independent annunciator panel. 2) A maximum credit RRF for operator actions whether in the field or in the control room is 10.			
	Control Room or Field Response	**Process Safety Time (min)**	**Description**	
	Control Room	<15	Operator has less than 15 minutes to respond to a pre-alarm.	1

Independent Protection Layer (IPL)	Guidelines			Risk Reduction Factor (RRF)
	Control Room	>15	Operator has more than 15 minutes to respond to a pre-alarm and the following conditions are met then a maximum credit RRF of 10 may be applied: a. Operator has been trained on the response procedure and a regular drilled exercise is conducted to ensure the operator's readiness. b. The Operator has an adequate alarm system where the alarm rate is monitored and controlled for e.g. less than 280 alarms per day per console or there is a separate alarm annunciator panel. c. Alarm signal is independent of the initiator's for automatic controls or a SIF. d. The alarm action is well defined, documented and the response straight-forward. e. Operator is present and capable of doing the action under all conditions. f. There is adequate means of communications available. g. The pre-alarm value is provided on the BPCS HMI console and is prioritized e.g. as low, medium or high priority.	10
	Field	<30	Operator has less than 30 minutes to respond to a pre-alarm.	1

Independent Protection Layer (IPL)	Guidelines			Risk Reduction Factor (RRF)
	Field	>30	Operator has more than 30 minutes to respond to a pre-alarm and the following conditions are met then a maximum credit RRF of 10 may be applied: a. Operator has been trained on the response procedure and a regular drilled exercise is conducted to ensure the operator's readiness. b. The Console Operator has an adequate alarm system where the alarm rate is monitored and controlled for e.g. to less than 280 alarms per day per console or there is a separate alarm annunciator panel c. Alarm signal is independent of the initiator's for automatic controls or a SIF. d. The alarm action is well defined, documented and the response straight-forward. e. Field operator is present and capable of doing the action under all conditions. f. There is adequate means of communications available g. The pre-alarm value is provided on the BPCS HMI console and is prioritized e.g. as low, medium or high priority.	10

Independent Protection Layer (IPL)	Guidelines	Risk Reduction Factor (RRF)
BPCS Interlock	A BPCS interlock is a process interlock that protects against the same scenario providing that the sensors and final control elements are not shared with the ESD. A risk reduction of 10 is allowed for either a BPCS control interlock or BPCS control loop, but not both.	10
Pressure Relief Valve (PZV)	Clean Service. PZV must be sized to completely mitigate the scenario and sized per Saudi Aramco (SA) Standards. The PZV must be tested and maintained per the Saudi Aramco Preventative Maintenance requirements.	100
	Clean Service. When more than one PZV is available to mitigate overpressure scenario and each PZV must be capable of independently relieving the vessel load without affecting the other. This does not include PZVs that are staged at different pressures. **Caution: The PZV can be the source of chattering and the capacity of the entire relieving system (piping, knock-out drums, and flare) must be evaluated. The above is not applicable where a parallel PZV has been installed for maintenance purposes and is normally isolated.**	1000
	Clean Service. More than one PZV is available, but more than one is required to mitigate the full load such as staged PZVs. To achieve a risk reduction factor of 100, the PZV calculations must determine for the specific scenario whether the load can be successfully handled by one PZV.	10-100
	Plugging Service. Those processes prone to plugging as a result of deposition, polymerization, or have a history of failure to operate properly when tested. To achieve a risk reduction factor of 10 the PZV must be installed with an integrated rupture disk and pressure gauge installed to measure pressure between rupture disk and PZV to detect disk leakage.	1-10
Vessel Rupture Disk	Clean service. The rupture disk must be designed to militate against the flow scenario and evaluated for any potential risk.	100
	Plugging Service. The rupture disk must be designed to militate against the flow scenario and evaluated for any potential risk.	10
Fire Detection with Water Deluge System	Operator initiated response. A risk reduction factor of 10 when the operator alarm response criteria are satisfied and the case is applicable to consequences relating to fire.	10
	Fire detection with automatic deluge such as foam, water curtain or water sprays. The risk reduction factor of 10 when the case is applicable to consequences relating to fire. Fire detection with emergency evacuation. A risk reduction factor of 10 is applicable to emergency evacuation when the operator alarm response criteria are satisfied and when documented in emergency response plans, Operator Instructions Manuals and applied in training drills.	10

Independent Protection Layer (IPL)	Guidelines	Risk Reduction Factor (RRF)
	Operator initiated response. A risk reduction factor of 10 when the operator alarm response criteria are satisfied and the case is applicable to consequences relating to gas.	10
Gas Monitors with Automated Deluge	Gas monitoring with automatic deluge such as water cannons, water sprays, or emergency evacuation. The risk reduction factor of 10 when the case is applicable to consequences relating to fire or gas release. Gas detection with emergency evacuation. A risk reduction factor of 10 is applicable to emergency evacuation when the operator alarm response criteria are satisfied and when documented in emergency response plans, Operator Instructions and applied in training drills.	10
SIS (Safety Instrumented System)	SIL 1 ESD SIF – Must comply with the requirements of SAES-J-601, SAEP-250 and achieve SIL 1 risk reduction. The verified risk reduction may be used if documented; otherwise a risk reduction factor of 10 shall be used. **Cautionary Note: Applying multiple safety instrumented functions to protect against the same scenario is not recommended as it will potentially lead to higher spurious trip rates (STR).**	10
	SIL 2 ESD SIF – Designed to comply with the requirements of SAES-J-601, SAEP-250 to achieve a SIL 2 risk reduction. The verified risk reduction may be used if documented, otherwise a risk reduction factor of 100 shall be used. **Cautionary Note: When applying multiple functions to protect against the same scenario will lead to higher spurious trip rates (STR).**	100
	SIL 3 ESD SIF – Designed to comply with the requirements of SAES-J-601 and SAEP-250 to achieve a SIL 3 risk reduction. The verified risk reduction may be used if documented; otherwise a risk reduction factor of 1000 shall be used. If the SIF is a HIPS then it shall comply to the requirements of SAEP-354 and be provided with a second safety layer of protection such as ESD SIF as a backup irrespective of the outcome of the LOPA. A risk reduction factor of 1000 may be used for HIPS unless the calculated RRF is provided. **Cautionary Note: The minimum requirement for HIPS is two safety layers of protection (e.g. an independent HIPS SIF and ESD SIF or flare).**	1000

Independent Protection Layer (IPL)	Guidelines	Risk Reduction Factor (RRF)
Independent Mechanical Protection	Mechanical safeguards that are independent of the ESD or BPCS such as: 1) Mechanically disconnected power source to an equipment use a RRF = 10. 2) Car sealing use a RRF = 10. 3) Variable speed drive circuits use a RRF = 10. 4) Mechanical keying LOTO use a RRF =100. 5) Mechanical over speed trip use RRF = 10. 6) Mechanical stop use RRF = 100.	10-100
Independent Electrical Safety Trips	Electrical safety trips that are hard-wired and independent of the ESD and BPCS such as: 1) Motor protection trip such as over-current and winding temperatures when protecting against the scenario. 2) Electrical over speed trip use RRF = 10. 3) Vibration Monitoring System (VMS) hardwired directly to the MCC. 4) Vibration Monitoring System (VMS) wired to the ESD with `separate shutdown relay.	10
Vacuum Breaker	Must be designed to mitigate the scenario. Vacuum breaker must be part of the facility's preventive maintenance program. The vent is in clean service, materials corrosion resistant. Installations without a block valve upstream or downstream use RRF =100 otherwise use RRF = 10.	10-100
Restrictive Orifice	Clean Service only and must be designed to mitigate the scenario. **Caution: restrictive orifices must be carefully designed and consider the effect of pressure losses and holdup in the process. The restrictive orifices must not be used in plugging or fouling services. The restricted flow quantity shall be validated for each operational mode or a change in the operations. The RO flow rate shall not create a potential hazard.**	10
Flame Arrester	Must be designed to mitigate the scenario. Flame arrestor must be part of the facility's preventive maintenance program.	10
Check Valve	Single check valve.	1
	Dual check valves in series. The check valves must be able to be removed and inspected as part of the facility's preventive maintenance program on a regular basis not greater than the T&I or 5 years.	10

Independent Protection Layer (IPL)	Guidelines	Risk Reduction Factor (RRF)
Dikes	Dikes which are capable of mitigating the hazardous event and has: a. Periodic inspection to ensure integrity of the structure. b. Adequate design basis for volume and strength. c. Sufficient distance from a source of ignition. d. Sufficient distance from other flammable or toxic storage tanks. e. Adequate firefighting equipment and procedures. Use a risk reduction factor 100 when the dike is sized for the largest tank within the dike otherwise use RRF =10. Caution: For compressed or liquefied gases where the product is stored above the atmospheric boiling point use a risk reduction factor of 1.	10-100
Fire Proofing	Fire Proofing shall be as per Saudi Aramco standards e.g. SAES-B-006. If a hazard is due to collapse of a supporting structure such as pipe racks that could cause breakage of pipes, collapse of vessels underneath the support structure. Or fire-proofing walls that could delay spread, propagation of fire to adjacent areas.	10
Blast Proofing	Blast-proofing of control rooms adjacent to process areas where an explosion is likely to occur and the control rooms/PIBs are designed to withstand the expected blast pressure.	100

3.5 Risk reduction calculation

Once all IPLs have been identified, the Mitigated Event Frequency (MEF) for the identified hazardous event shall be quantified by multiplying the IEF, the product of all enabling and conditional modifiers and the product of the
PFD of all IPLs identified.

The required Risk Reduction Factor (RRF) shall be calculated by dividing the MEF by the TEF previously identified.

3.6 SIL allocation

A SIL shall be assigned to each Safety Instrumented Function (SIF) under investigation based on SIL categories, in terms of RRF, Average Probability of Failure on Demand (PFDavg), as shown in the following

SIL	RRF (Risk Reduction Factor)	PFD_{avg} (Probability of Failure on Demand) (1/RRF)	Safety Availability (1-PFD_{avg})
0/a	Process Control		
1	10 to 100	1/10 to 1/100	90 - 99%
2	100 to 1,000	1/100 to 1/1,000	99 - 99.9%
3	1,000 – 10,000	1/1,000 to 1/10,000	99.9 - 99.99%

3.7 Assumptions

All the assumptions listed in the HAZOP Procedure (Ref. [17]) and those discussed and agreed by the HAZOP team during the session, must be considered applicable to SIL Allocation study.

The following SIL Allocation premises will be applied by all teams in order to ensure a consistent approach:

- OPA shall be performed only if trip action is provided in the relevant HAZOP worksheet;
- relief valves can be considered as IPLs if the relief system has been sized for all reasonably foreseeable failures of the process and process controls and completely mitigates the hazard scenario under consideration
- when two independent (diverse) relief devices are present, each 100% sized for the hazard scenario, then credit should be taken for an additional layer of protection;
- failure mode of the final element is to the safe state;
- the following conditions must be met before operator response to alarm will be claimed as an IPL:
    - alarm is independent of the cause and any BPCS control loop claimed as a protection layer;
    - operator is always present and available at the alarm point (e.g., control room is continuously manned);

- alarm gives clear indication of the hazard and will be given high priority on control room console;
- operator has a minimum of 20 minutes of time to diagnose and take appropriate corrective action;
- operator is trained in the response associated with the alarm state and the response steps are identified in the Safe Operating Limits of the operating manual;
- Risk reduction for "operator response to alarms" was only counted as a single protection layer accounting for a factor of 10;

- human error shall be considered once only for routine operations (no multiple errors shall be considered).

Any other assumption that should be discussed and agreed by the LOPA Team during the session, shall be explicitly documented and recorded in the SIL Allocation Report.

3.8 Reporting

The LOPA Worksheets shall be prepared daily for recording the study proceedings in accordance with the chairman's instructions.

The LOPA worksheets shall be agreed by the SIL Allocation Team as the worksheets are completed during the session.

A copy of the LOPA worksheets shall be included in the SIL Allocation Report as attachment.