LAYER OF PROTECTION ANALYSIS (LOPA) GUIDELINE

EGPC-PSM-GL-015

PSM GUIDELINES

The Egyptian Process Safety Management Steering Committee (PSMSC Egypt)
PSM TECHNICAL SUBCOMMITTEE (PSMTC)

Acknowledgments

This publication has been produced as a result of the comprehensive efforts carried out by the PSM Technical Subcommittee on behalf of the Egypt PSM Steering Committee, formed per the Memorandum of Understanding signed between the Ministry of Petroleum and Mineral Resources and Methanex Egypt in February 2020 overseeing the design and implementation of a detailed PSM program to promote and enhance PSM culture for Ministry of Petroleum and Mineral Resources (MOP) and its affiliated COMPANIES following industry best practice, international codes and standards. The Egyptian Process Safety Management Steering Committee comprises MOP, EGPC, ECHEM, EGAS, GANOPE, and Methanex Egypt representatives.

PSM Technical Subcommittee team members during the project comprised:

Amr Moawad Hassan	**PSM Senior Consultant – Methanex Egypt**	**Team Leader**
Mohamed Mesbah	Operations Department Head - KPC	Member
Ahmed Mostafa	Operations Section Head - ELAB	Member
Ahmed Roustom	Risk Management and Loss Prevention Studies Assistant General Manager – GASCO	Member
Hany Tawfik	OHS & PS General Manager – ETHYDCO	Member
Mohamed Ashraf Aboul-Dahb	Safety Section Head for Upstream – EGPC	Member
Mohamed Hamouda	HSE Department Head – Pharaonic Pet. Co.	Member
Mohammed Sabry	Risk Management and Loss Prevention Studies Executive General Manager – GASCO	Member
Sayed Eid	HSE A. General Manager – Agiba Pet. Co.	Member
Tamer Abdel Fatah	QHSE Senior – UGDC	Member

All PSM technical subcommittee documents are subjected to a thorough technical peer-review process during development and prior approval. The PSM technical subcommittee gratefully appreciates the thoughtful comments and suggestions of the peer reviewers. Their contributions enhanced the accuracy and clarity of the documents. The PSM Technical Subcommittee acknowledges the following reviewers from major Process Safety consultants as well as major operators & EPC contractors who provided valuable comments during the technical peer reviews that resulted in an outstanding product structure and quality:

Process Safety Consultants (in alphabetical order):

- Exida - By: Greg Chantler, Principal Consultant.
- Risktec Solutions - TÜV Rheinland.

Major IOCs & EPCs (in alphabetical order):

- ENPPI - By: Ramadan Ismail- Process Technology | GM Assistant, Safety & Loss Prevention Engineering.

It should be noted that the above have not all been directly involved in developing this document, nor do they necessarily fully endorse its content.

Egypt PSM Steering Committee team members during the project comprised:

Gamal Fathy	EGPC CEO Consultant for HSE – EGPC	Member
Mohamed Mahmoud Zaki	Executive Vice President – ECHEM	Member
Salah El Din Riad	Q&HSE Chairman Assistance – ECHEM	Member
Dr. Ashraf Ramadan	Assistant Chairman for HSE – EGAS	Member
Emad Kilany	OHS & Fire Fighting Technical Studies GM - EGAS	Member
Mohamed Sayed Suliman	HSE General Manager – GANOPE	Member
Mohamed Mostafa	Inspection & External Audit GM – ECHEM	Member
Mohamed Shindy	Managing Director – Methanex Egypt	Member
Manal El Jesri	Public Affairs Manager – Methanex Egypt	Member
Mohamed Hanno	RC Manager – Methanex Egypt	Member
Amr Moawad Hassan	PSM Senior Consultant – Methanex Egypt	Member
Mourad Hassan	PSM Consultant – Methanex Egypt	Member

DOCUMENT NO.	TITLE	ISSUE DATE
EGPC-PSM-GL-015	LAYER OF PROTECTION ANALYSIS (LOPA) GUIDELINE	Nov. 2022

Approval

NAME	TITLE	DATE	SIGNATURE
Amr Moawad Hassan	PSM Senior Consultant - Methanex Egypt PSM Technical Subcommittee TL	Nov. 2022	
Gamal Fathy	EGPC CEO Consultant for HSE	Nov. 2022	

Endorsement

NAME	TITLE	DATE	SIGNATURE
Alaa El Batal	CEO - Egyptian General Petroleum Corporation (EGPC)	Nov. 2022	

Copyright

Disclaimer

Controlled Intranet Copy

The intranet copy of this document is the only controlled document. Copies or extracts of this document, downloaded from the intranet, are uncontrolled copies and cannot be guaranteed to be the latest version. All printed paper copies should be treated as uncontrolled copies of this document.

All administrative queries must be directed to the Egyptian Process Safety Technical Subcommittee.

Table of Contents

1. Introduction 6
2. Purpose 6
3. Scope 7
4. Definitions 7
5. Abbreviations 9
6. LOPA Overview 9
6.1 What is LOPA? 9
6.2 Advantages 10
6.3 Limitations 11
7. LOPA Methodology 11
7.1 General 11
7.2 Screen Hazardous Events Scenarios 12
7.3 Target Mitigated Event Likelihood (TMEL) 12
7.4 Initiating Events 14
7.5 Independent Protection Layers Identification 15
7.6 Enabling Conditions 17
7.7 Conditional Modifier 18
7.8 Intermediate Event Likelihood (IEL) 18
7.9 Evaluation of SIS Integrity Level 19
8. LOPA Timing 20
9. LOPA Team Roles and Responsibilities 20
9.1 LOPA Study Coordinator 20
9.2 LOPA Study Leader 20
9.3 Scribe 21
9.4 Other Team Members 21
10. LOPA Documentation 22
10.1 LOPA Terms of Reference (TOR) 22
10.2 Documents Required for LOPA 22
10.3 LOPA Report 23
10.4 Follow-up 24
11. References 25
12. List of Annexes 25
Annex A - Initiating Events Frequencies 26

Annex B - Independent Protection Layers PFD Data 28
B.1. PFD for Passive IPLs 28
B.2. PFD for Active IPLs 34
Annex C - Enabling Conditions and Conditional Modifiers 49
C.1. Time at Risk 49
C.2. Probability of Ignition and Explosion 49
C.3. Vulnerability (Probability of Injury/Fatality). 49
Annex D - LOPA Worksheet Example 50

1. Introduction

The layer of protection analysis (LOPA) is a semi-quantitative tool for analyzing and assessing risk. LOPA typically uses the order of magnitude categories for initiating event frequency, consequence severity, and the likelihood of failure of independent protection layers (IPLs) to approximate the risk of a scenario. It is an analysis tool that typically builds on the information developed during a qualitative process hazard analysis, such as Hazards and Operability studies (HAZOP).

Like many other hazard analysis methods, the primary purpose of LOPA is to determine if there are sufficient layers of protection against an accident scenario (can the risk be tolerated?). A scenario may require one or many protection layers depending on the process complexity and potential severity of a consequence. Only one layer must work successfully for a given scenario to prevent the consequence. However, since no layer is perfectly effective, sufficient protection layers must be provided to render the risk of the accident tolerable.

LOPA provides a consistent basis for judging whether there are sufficient independent protection layers (IPLs) to control the risk of an accident in a given scenario. If the estimated risk of a scenario is not acceptable, additional IPLs may be added. Alternatives encompassing inherently safer design can be evaluated as well. LOPA does not suggest which IPLs to add or which design to choose, but it assists in judging alternatives for risk mitigation. LOPA is not a fully quantitative risk assessment approach but a simplified method for assessing the value of protection layers for a well-defined accident scenario.

This guideline generally describes the requirements for LOPA implementation, including LOPA timing, advantages and limitations, and roles and responsibilities. Besides, the required documentation to apply effective LOPA and develop a comprehensive report and follow-up procedures were addressed. Also, a detailed LOPA examination methodology is explained, starting with selecting the hazardous event scenario developed in HAZOP until the LOPA study's final recommendations are reached. The appendices contain useful data to estimate the initial event frequency and the independent protection layers' probability of failure on demand (PFD).

2. Purpose

This guideline defines the basis, scope, and methodology for completing layer of protection analysis (LOPA) studies for new and existing facilities within the Egyptian oil, gas, and petrochemicals industry.

3. Scope

This document provides a guideline for conducting layer of protection analysis (LOPA) studies within the Egyptian General Petroleum Corporation (EGPC) and Oil and Gas Holding Companies, including the Egyptian Natural Gas Holding Company (EGAS), the Egyptian Petrochemicals Holding Company (ECHEM), and the South Valley Petroleum Holding Company (GANOPE) covering all their operational subsidiaries, state-owned companies, affiliates, and joint ventures.

ENTITIES and their COMPANIES and contractors should ensure that all requirements listed herein are fully understood, implemented, complied with, and always monitored, including current operations and future projects during the whole project's life cycle from feasibility to decommissioning.

4. Definitions

BASIC PROCESS CONTROL SYSTEM (BPCS): A system that responds to input signals from the process, its associated equipment, other programmable systems, or operator and generates output signals causing the process and its associated equipment to operate in the desired manner but that does not perform any safety instrumented functions with a claimed SIL > 1.

COMMON CAUSE FAILURE: Failure of more than one device, function, or system due to the same cause.

COMPANY: Refers to any operating company, subsidiary, affiliated, or joint venture company that belongs to an ENTITY.

CONDITIONAL MODIFIER: One of several possible probabilities is included in scenario risk calculations, generally when the risk criteria are expressed in impact terms (e.g., fatalities) instead of loss event terms (e.g., release, loss-of containment, vessel rupture).

CONSEQUENCE: Adverse effects or harm which causes the quality of human health or the environment to be impaired. It is the loss that can be inflicted if any hazardous event occurs.

DEMAND MODE: Dormant or standby operation where the IPL acts only when a process demand occurs and is otherwise inactive. Low demand mode occurs when the process demand frequency is less than once yearly. High demand mode occurs when the process demands happen more than once yearly.

ENABLING CONDITION: Operating conditions are necessary for an initiating cause to propagate into a hazardous event. Enabling conditions do not independently cause the incident but must be present or active for it to proceed.

ENTITIES: Refers to the Egyptian General Petroleum Corporation (EGPC) and Oil and Gas Holding Companies, including the Egyptian Natural Gas Holding Company (EGAS), the

Egyptian Petrochemicals Holding Company (ECHEM), and the South Valley Petroleum Holding Company (GANOPE).

ENVIRONMENTAL INTEGRITY LEVEL (EIL): Level for specifying environmental integrity requirements of environmental function allocated to SIS.

FREQUENCY: The number of times an event is estimated to occur over a specified period.

FINANCIAL INTEGRITY LEVEL (FIL): Level for specifying financial integrity requirements of financial function allocated to safety instrumented systems (SIS).

INDEPENDENT PROTECTION LAYER (IPL): Device, system, or action that can prevent a postulated accident sequence from proceeding to a defined, undesirable endpoint. An IPL is (1) independent of the event that initiated the accident sequence and (2) independent of any other IPLs. IPLs are normally identified during the layer of protection analyses.

INCIDENT SCENARIO: A hypothetical sequence of events that includes an initiating event and failure of any safeguards resulting from concern.

INITIATING EVENT (IE): A device failure, system failure, external event, or wrong action (or inaction) begins a sequence of events leading to a consequence of concern.

INITIATING EVENT FREQUENCY (IEF): How often is the initiating event expected to occur; in LOPA, the IEF is typically expressed in yearly occurrences.

PROBABILITY OF FAILURE ON DEMAND (PFD): The likelihood that a system will fail to perform a specified function when needed.

SAFEGUARD: Engineered systems or administrative controls designed to prevent the cause, protect against the deviation progressing to a loss event or mitigate the immediate loss event consequences (e.g., process alarms, shutdowns, automatic isolation). Not all safeguards will meet the requirements of an IPL.

SAFETY INSTRUMENTED FUNCTION (SIF): A safety function allocated to a Safety Instrumented System (SIS) with a Safety Integrity Level (SIL) is necessary to achieve the required risk reduction for the identified scenario of concern.

SAFETY INTEGRITY LEVEL (SIL): One of four discrete ranges is used to benchmark the integrity of each SIF, and the SIS, where SIL 4 is the highest and SIL 1 is the lowest.

SAFETY INSTRUMENTED SYSTEM (SIS): A separate and independent combination of sensors, logic solvers, final elements, and support systems is designed and managed to achieve a specified Safety Integrity Level (SIL). The SIS may implement one or more Safety Instrumented Functions (SIFs).

SEVERITY: A measure of the degree of impact of a particular consequence.

5. Abbreviations

ALARP	As Low As Reasonably Practicable
BPCS	Basic Process Control System
EIL	Environmental Integrity Level
FIL	Financial Integrity Level
FMEA	Failure Mode and Effects Analysis
HAZOP	Hazard and Operability
IEL	Intermediate Event Likelihood
IEF	Initiating Event Frequency
IPL	Independent Protection Layer
ISD	Inherently Safer Design
LOPA	Layer of Protection Analysis
OREDA	Offshore Reliability Data
PFD	Probability of Failure on Demand
PRV	Pressure Relief Valve
RRF	Risk Reduction Factor
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TMEL	Target Mitigated Event Likelihood

For other definitions and abbreviations, refer to the PSM Glossary of Definitions and Abbreviations Guideline (EGPC-PSM-GL-011).

6. LOPA Overview

6.1 What is LOPA?

LOPA is a method for evaluating the effectiveness of protection layers in reducing the frequency and consequence severity of hazardous events. LOPA provides specific criteria and restrictions for evaluating IPLs, reducing the subjectivity of qualitative methods. LOPA can be used to determine the target SIL for a SIF, but that is just one outcome of LOPA. LOPA also evaluates whether a protection layer can be considered independent and can determine the performance required for non-SIS independent layers of protection.

6.2 Advantages

The advantages of conducting LOPA study for new and existing facilities include the following:

- LOPA requires less time than quantitative risk analysis. This benefit applies particularly to scenarios that are too complex for qualitative risk assessment.
- LOPA is effective in resolving disagreements related to risk.
- LOPA facilitates the determination of more precise cause–consequence pairs and improves scenario identification.
- LOPA determines whether SIS or alternative means of protection are required and associated SIL if SIS is chosen.
- LOPA conforms to industry standards, i.e., ISA S84.01, IEC 61508, and IEC 61511.
- LOPA facilitates the analysis of protective layers addressing health and safety and environment and may also be applied to risks due to equipment damage and business value lost.
- If the same approach is used throughout the company, LOPA compares risk from unit to unit or plant to plant.
- LOPA provides more defensible comparative risk judgments than qualitative methods due to the more rigorous documentation and the specific values assigned to the frequency and consequence aspects of the scenario.
- LOPA can help an organization decide if the risk is" As Low As Reasonably Practicable" (ALARP), which may also meet specific regulatory requirements.
- LOPA helps identify operations and practices previously thought to have sufficient safeguards. Still, on more detailed analysis (facilitated by LOPA), the safeguards do not mitigate the risk to a tolerable level.
- Information from LOPA helps an organization decide which safeguards to focus on during operation, maintenance, and related training. For instance, many companies focus their inspection, test, and preventive maintenance activities on the IPLs identified during LOPA; these companies often decide to run the remaining safeguards (those not identified as IPLs) to failure or subject them to less rigorous test and maintenance schedules. Therefore, LOPA is a tool for implementing a wise PSM mechanical integrity or risk-based maintenance system, and it aids in identifying "safety critical" elements and tasks.

6.3 Limitations

LOPA limitations could be summarized as follow:

- LOPA is not a method for identifying hazards.
- LOPA is a simplified approach and should not be applied to all scenarios. The effort required to implement LOPA may be excessive for some risk-based decisions and overly simplistic for other decisions.
- LOPA is not a method to analyze escalation events.
- LOPA requires more time to reach a risk-based decision than qualitative methods such as HAZOP and What-if. The improved risk decision offsets this extra time compared to using only qualitative methods for moderately complex scenarios. For simple decisions, the value of LOPA is minimal. For more complex scenarios and decisions, LOPA may save time compared to using only qualitative methods because LOPA brings focus to the decision-making.
- LOPA allows the analyst to take a predefined scenario and estimate the risk of the scenario in a consistent and simplified manner.
- Despite using numbers, the LOPA results do NOT express the scenario's specific risk. Like other techniques, LOPA gives approximations of risk that are useful in making comparisons (which help to allocate limited resources for risk control). For many purposes, LOPA analyses have sufficient precision to quantify a particular process scenario's risk adequately.
- A full assessment must justify the quantification of the integrity of the IPLs.

7. LOPA Methodology

7.1 General

LOPA methodology could be summarized as follow (see Figure 1):

1. List the hazardous events and consequences of each scenario identified in the HAZOP or from any reliable source. Identify and evaluate the consequences of each scenario.
2. Determine the Target Mitigated Event Likelihood (TMEL) for each category of consequences (i.e., health & safety, environment, and business).
3. Identify the initiating events for each scenario and the frequency of each event.
4. Identify the IPLs and probability of failure on demand (PFD) for each scenario.
5. Identify the enabling conditions and conditional modifiers probabilities for each scenario.

6. Determine the Intermediate Event Likelihood (IEL).
7. Determine if other IPLs are required by evaluating the IEL against the TMEL for each category.
8. If IEL is higher than the TMEL, an additional independent protection layer shall be added, where PFD (for the additional IPL) = TMEL / IEL.

7.2 Screen Hazardous Events Scenarios

Usually, the scenarios developed in the HAZOP with the highest consequences on health & safety, environment, and business are selected for LOPA. In addition to the scenarios developed in the HAZOP, the event scenarios could also be obtained from other sources, such as:

- Risk studies include what-if analysis and failure mode and effect analysis (FMEA).
- Plant operational experience.
- Plant and industry incident and near-miss data.
- Management of change reviews

7.3 Target Mitigated Event Likelihood (TMEL)

Target Mitigated Event Likelihood (TMEL) is the maximum allowable frequency for a specified severity of consequence, as illustrated in Table 1. The TMEL is derived from the risk matrix, which explains each severity level. The TMEL should be determined for each category of consequences according to its severity. Therefore, there should be TMEL (safety), TMEL (environment), and TMEL (financial). Severity levels are clearly illustrated in the corporate risk matrix included in the Risk Management Standard (EGPC-PSM-ST-001). For extensive events that could lead to a huge impact, e.g., 100 fatalities or more, the TMEL should be lowered, and the scenario should be studied in more detail in a fully quantitative risk assessment study.

Table 1. *Typical TMEL values.*

Severity Level	TMEL (yr^{-1})
Disastrous	1.00E-06
Catastrophic	1.00E-05
Major	1.00E-04
Serious	1.00E-03
Minor	1.00E-02
Notable	1.00E-01

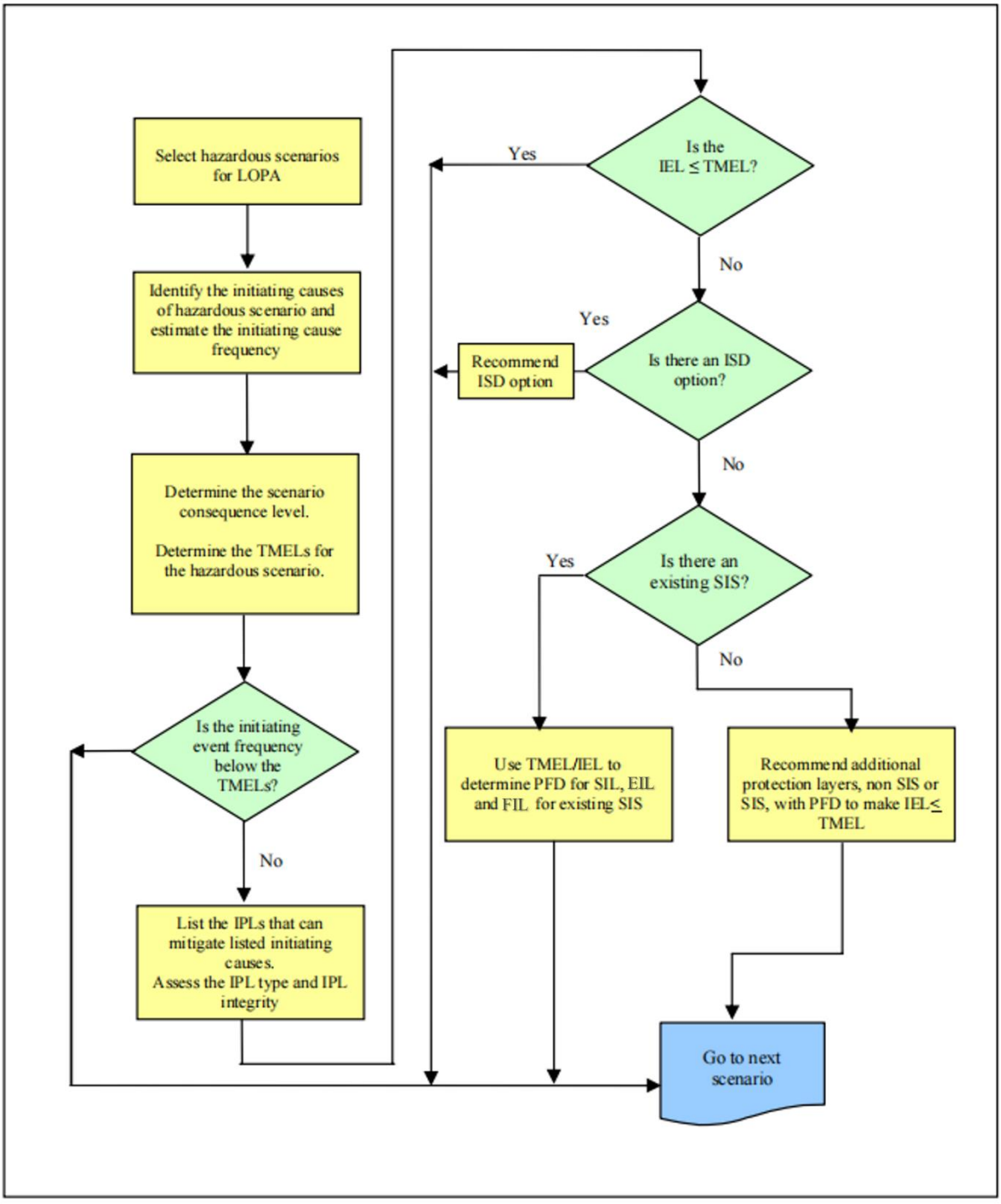

Figure 1. *LOPA methodology flowchart.*

7.4 Initiating Events

Following the determination of event scenarios to be included within a LOPA, the initiating events for each scenario and their frequencies should then be identified. Initiating events could be (see Figure 2):

- Equipment Failure:
  - Control system failures may arise due to components, software, or utility failures.
  - Mechanical failures can be due to numerous reasons, such as corrosion, fatigue, vibration, etc.
- Human Error:
  - Improper execution of steps for a task.
  - Failure to respond appropriately to process upset conditions or prompts in the system.

A typical frequency data for different initiating events is illustrated in Annex A. If an Initiating event is not listed in Annex A, the LOPA team shall look for the data from a reliable source (e.g., CCPS, OREDA). Each initiating event frequency should be calculated for the scenario with more than one event. The final unmitigated event frequency for the scenario should be the sum of all the individual frequencies.

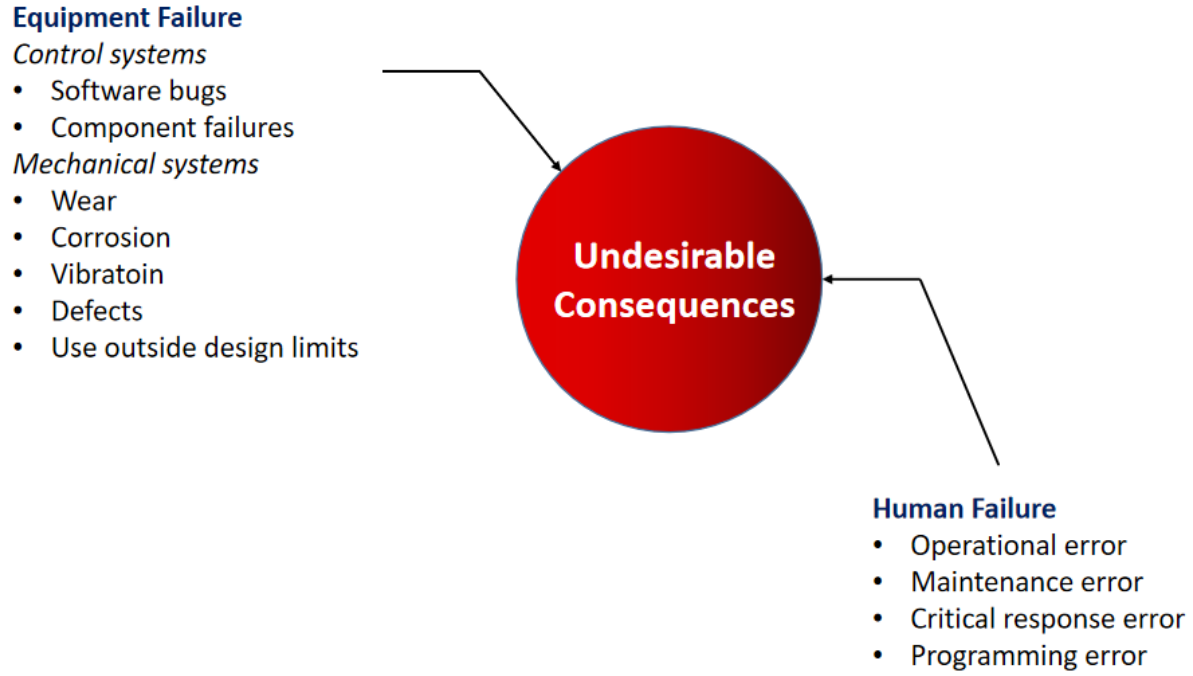

***Figure 2**. Initiating events categories.*

7.5 Independent Protection Layers Identification

An independent protection layer (IPL) is a device, system, or action that can prevent a scenario from proceeding to its undesired consequence or mitigate the consequences, as illustrated in Figure 3. There are nine criteria for protection layers to be considered as IPLs:

1. **Independence** is achieved when the performance of one IPL is not affected by the initiating event or by the failure of any other IPL to operate. The LOPA team should pay particular attention to the common cause failures which may affect several protection layers.
2. **Functionality** is required to perform its intended function under the actual process operating conditions during the event.
3. **Integrity** is a property of the IPL that measures its capability to satisfy its specified requirements.
4. **Reliability** is an attribute of a protection layer related to its equipment operating as intended, under stated conditions, for a specified period.
5. **Auditability** reflects the ability of an organization to inspect procedures, records, previous validation assessments, and other documented information to ensure that design, testing, maintenance, and operation continue to conform to expectations.
6. **Access security** includes using physical and administrative controls to reduce the chances of unauthorized system changes that may impair a safety device.
7. **Management of change (MOC):** It is a formal process to review, approve, and document changes. Modifications may create new LOPA scenarios or reduce the effectiveness of existing IPLs.
8. **Survivability** refers to how the IPL will perform after a major accident has occurred, i.e., how well it will survive a fire, explosion, etc.
9. **Effectiveness:** Sizing and choosing protection system criteria shall be consistent with the consequence magnitude of the scenario.

The IPLs could be classified as:

- Passive IPLs, such as:
  - Dikes/Bunds.
  - Open vents.
  - Blast walls/Bunkers.
  - Flame/Detonation Arrestors.

- Active IPLs, such as:
  - BPCS control functions.
  - Alarms and associated human response.
  - Relief devices.
  - Other SIS functions.

Each IPL should be assigned a probability of failure on demand (PFD) to indicate its effectiveness in reducing the risk. Annex B provides generic PFD and details for frequently used IPLs in the oil, gas, and petrochemicals industry. For IPL, which is not listed in Annex B, the PFD should be obtained from reliable sources. For an IPL to be valid, the organization needs to maintain the underlying management systems that ensure the IPL will meet the assigned value (PFD). It shall be noted that although some safeguards may be included and listed in HAZOP, they cannot be considered as an IPL in the case of LOPA unless the criteria validate them. Examples of safeguards that do not meet the IPL criteria are summarized in Table 2.

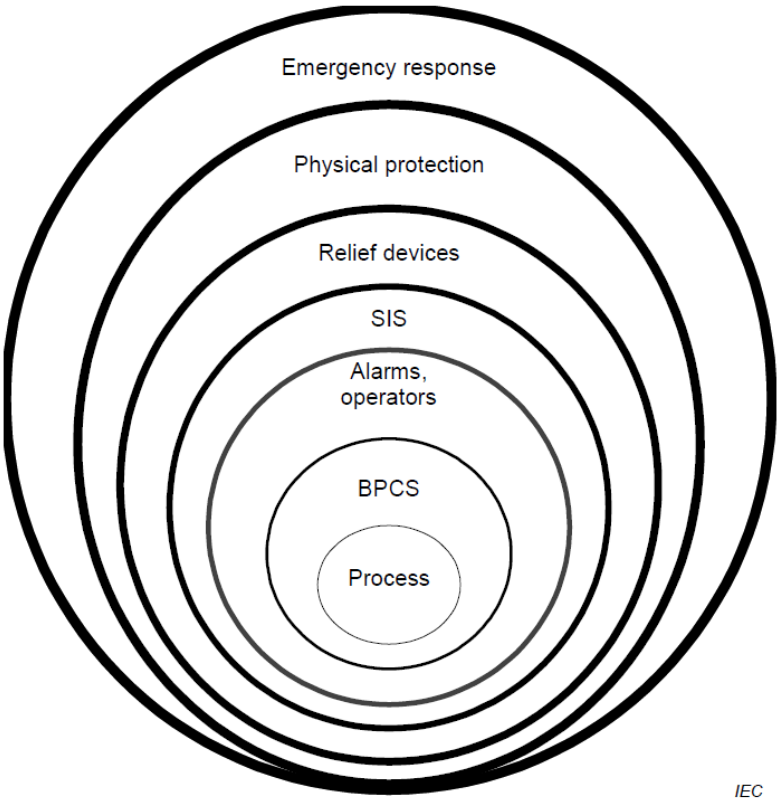

Figure 3. *Layers of protection.*

Table 2 *Safeguards not considered as IPLs.*

Safeguards not Considered IPLs	Comments
Training and Certification	These factors may be considered in assessing the PFD for operator action but are not IPLs.
Procedures	These factors may be considered in assessing the PFD for operator action but are not IPLs.
Normal Testing and Inspection	These activities are assumed to be in place for all hazard evaluations and form the basis for judgment to determine PFD. Normal testing and inspection affect the PFD of certain IPLs.
Maintenance	This activity is assumed to be in place for all hazard evaluations and forms the basis for judgment to determine PFD. Maintenance affects the PFD of certain IPLs.
Communications	It is a basic assumption that adequate communications exist in a facility. Poor communications affect the PFD of certain IPLs.
Signs	Signs by themselves are not IPLs. Signs may affect the PFD of IPLs

7.6 Enabling Conditions

The enabling condition considers the conditions necessary for an abnormal situation to proceed to the consequence of concern. The enabling condition is expressed as a probability. In combination with the initiating event, frequency represents the times per year an abnormal situation would be encountered that could lead to a loss event. For example, if the scenario is expected during loading operation, which takes around one day every month. In this situation, enabling conditions probability would equal 12 days/365 days or 0.033.

The following are typical situations where a LOPA team should avoid the use of enabling conditions:

- The LOPA analyst(s) have insufficient knowledge of enabling conditions to employ them correctly.
- Insufficient data or information is available to assess the probability of being assigned to an enabling condition.
- The company or facility established LOPA procedure indicates that enabling conditions cannot be used in its LOPA studies for whatever reason.
- The company or facility does not have the resources, capability, or practices in place to properly assess and document the use of enabling conditions and maintain their ongoing validity.

For further details, refer to " Center for Chemical Process Safety (CCPS), Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis, Wiley, 2013".

7.7 Conditional Modifier

A conditional modifier is one of several possible probabilities that could reduce the consequence of a specific scenario. For example, if the consequence is "Fatality due to fire," the ignition probability would affect the calculations for that category (but still needed for the consequence to be realized). Conditional modifiers include, but are not necessarily limited to:

- Probability of ignition and explosion.
- Probability of personnel presence or occupancy.
- Probability of injury or fatality.
- Probability of equipment damage or other financial impacts.
- Probability of environmental damage.

Conditional modifiers should be considered consequence-specific but not Initiating Event-specific. As such, care should be taken to only credit conditional modifiers for consequence categories where the team reasonably expects them to bring the consequence into existence, i.e., occupancy is not a valid conditional modifier considering harm to the environment. Make sure that if the LOPA team selects a conditional modifier probability, it is realistic to expect the probability to be valid over time. Some common pitfalls in the usage of conditional modifiers include:

- Being overly optimistic in estimating conditional modifier probabilities.
- Including more conditional modifiers until the desired risk level is reached.
- Using conditional modifiers to justify avoiding a standard practice, such as not including overflow protection in a tank design.

For further details, refer to " Center for Chemical Process Safety (CCPS), Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis, Wiley, 2013".

7.8 Intermediate Event Likelihood (IEL)

The intermediate event likelihood for a specific scenario is calculated as follows:

$$IEL = IEF \times PFD_1 \times PFD_2 \times PFD_n \times P_{EC} \times P_{CM}$$

Where:

IEL = intermediate event likelihood for the specific initiating event–consequence pair

IEF =Initiating Event Frequency

PFD =Probability of Failure on Demand for valid IPLs (where n is the number of IPLs)

P_{EC} = probability of enabling condition

P_{CM} = probability of conditional modifiers.

If there is more than one initiating event for a selected scenario, the IEL should be calculated similarly for each initiating event. The total IEL for the selected scenario is then calculated by summing all IELs as follows:

$$IEL_{total} = \sum IEL$$

7.9 Evaluation of SIS Integrity Level

- If the $IEL_{total} < TMEL$, then further risk reduction is not appropriate.
- If the $IEL_{total} > TMEL$, then existing protection layers are considered insufficient to mitigate risk.
- Recommendations should be made to use inherently safer design strategies to redesign the system, add additional protection layers, or add a SIF.
- If it is decided to add SIF, based on the identified scenarios, the integrity level for this SIF should be determined regarding safety (SIL), environment (EIL), and Financial (FIL), as illustrated in the following equations:

$$PFD_{SIF}\ (health\ \&\ safety) = \frac{TMEL_{safety}}{IEL_{Total}}$$

$$PFD_{SIF}\ (environmental) = \frac{TMEL_{environment}}{IEL_{Total}}$$

$$PFD_{SIF}\ (financial) = \frac{TMEL_{financial}}{IEL_{Total}}$$

- The required SIL level will be the highest of the three calculated categories.
- The integrity level for each PFD_{SIF} is illustrated in Table 3.

***Table 3**. Integrity levels for SIF.*

Required SIL, EIL, FIL	PFD $_{SIF}$	RRF = (1/PFD)
SIL 1, EIL 1, FIL 1	$10^{-2} \leq PFD < 10^{-1}$	$10 < RRF \leq 100$
SIL 2, EIL 2, FIL 2	$10^{-3} \leq PFD < 10^{-2}$	$100 < RRF \leq 1{,}000$
SIL 3, EIL 3, FIL 3	$10^{-4} \leq PFD < 10^{-3}$	$1{,}000 < RRF \leq 10{,}000$
SIL 4, EIL 4, FIL 4	$10^{-5} \leq PFD < 10^{-4}$	$10{,}000 < RRF \leq 100{,}000$

8. LOPA Timing

- LOPA should be conducted with or immediately after the HAZOP for all major events identified in the detailed engineering phase and for identified and proposed Safety Instrumented Functions (SIFs) during the HAZOP.
- LOPA could be carried out at an earlier phase (e.g., basic engineering), as identifying the SIS needs at this stage will lead to more satisfactory and effective design work.
- LOPA could be conducted as a part of a general review (revalidation) of risk studies.
- LOPA could be conducted to manage change for modifications to an existing facility.

9. LOPA Team Roles and Responsibilities

9.1 LOPA Study Coordinator

The LOPA study coordinator, typically the process safety lead, shall consolidate the activities related to the study. The responsibilities can include:

- Definition and verification of data needs, coordination of data collection efforts, and resolution of data collection issues.
- Engaging with the approved leaders and scribes.
- Working with project management to obtain appropriate team members to participate in the study.
- Management of schedules, tracking progress against plan, understanding delays, communicating and resolving schedule issues.
- Developing terms of reference (TOR) for the study in conjunction with the leader and obtaining approval.
- Handling meeting administrative and logistical aspects.

9.2 LOPA Study Leader

The LOPA study leader shall:

- Be independent of the project or the facility.
- Ensure time pressure does not compromise quality.
- Advise leadership of issues that could affect the integrity of the study, for example, inadequate experience or makeup of the team, fatigue issues, team members not present, and process safety information lacking / not available.

- Have the necessary training and experience in the application of the LOPA methodology.
- Understand events' likelihood and potential consequences, including developing conditional probabilities of different outcomes.
- Have an overview understanding of safety-instrumented systems for the process industry sector.
- Be certified by a recognized functional safety certification body such as *TÜV* or EXIDA.

The LOPA study leader is responsible for the following:

- Facilitating the LOPA study sessions so that the assessment process runs per the procedure and the team remains actively involved and focused on the study's objectives.
- Ensuring that all required documents for the LOPA study are available and updated.
- Ensuring that the team composition and experience are adequate for LOPA study.
- Ensuring the comprehensiveness of all notes taken to support the team's decision.
- Ensuring proper LOPA software is available.
- Issuing the final report for the LOPA study.

9.3 Scribe

The scribe shall be responsible for recording the meeting discussion using the worksheets or the software used during the session. The LOPA scribe should have a technical background and previous experience in the software to be used during the assessment. The partnership between the leader and scribe can impact study efficiency.

9.4 Other Team Members

The team members are responsible for participating in the review meetings and providing accurate feedback from their area of expertise, usually process safety, instrumentation & control, and operations. The number of full-time members, including the leader and scribe, should be ten or less. LOPA shall be performed using a multidisciplinary team, including persons who have:

- Understanding and experience of the process design and intent.
- Understanding and experience with instrument and control.
- Understanding and experience with day-to-day operations.
- Experience with process safety.

- Understanding and experience with equipment, design limits, and materials of construction.
- A technical representative for licensed technologies or packages vendor.
- Other disciplines as required.

It is recommended to minimize position matching when personnel from the engineering contractor and company representing the same function attend a study. This practice potentially increases the number of participants to an unmanageable number.

10. LOPA Documentation

10.1 LOPA Terms of Reference (TOR)

A TOR shall be developed for each study and formally agreed upon between the company and the LOPA study leader before the study commences. The TOR document should include the following:

1. Objectives.
2. Scope.
3. Methodology including software, values, and assumptions that may be used.
4. Personnel required to attend the meeting.
5. Schedule and deliverables.
6. Distribution list.
7. Reference documents (e.g., HAZOP, Cause and Effects, and P&IDs).

10.2 Documents Required for LOPA

The last version of the following documents should be available before the start of the LOPA study:

- Cause and effect chart.
- HAZOP worksheets with a clear and complete definition of hazard scenarios, their consequence, and safeguards, including the layers of protection.
- Complete set of P&IDs.
- Plot plan and equipment layouts.
- The clear and complete definition of instrumented systems and their interrelations.
- SIL ratings that have been previously determined for existing SISs.
- SRS for existing SIS (if the SIF already exists).

- Pressure relief (or safety) valves design data.
- Vessel/equipment design data.
- F&G detection layouts.
- Operating and control procedures.
- Equipment datasheets.
- Instrument and control philosophy.
- Flare load summary/relief and blowdown summary providing all overpressure scenarios.
- Basic Process Control Systems, ESD systems, and interlock information.
- Relevant Safety Study Reports include ENVID, HAZID, FERA, QRA, etc.

10.3 LOPA Report

A LOPA report shall include the following:

1. Main report
    a. Principal recipient of the report.
    b. Executive summary.
    c. Scope of the study.
    d. Process or system description and design intent.
    e. Identification of numerical values used in their sources and any assumptions made.
    f. LOPA team members and their roles.
    g. Recommendations summary.
    h. References (list of documentation and drawings used).
    i. Distribution list.
2. Appendices
    a. List of attendees.
    b. Assumptions.
    c. LOPA worksheets.

10.4 Follow-up

The company should ensure that an effective means of tracking recommendations are in place and accomplishes the following:

- Track the status of open action items.
- Track the fulfillment of the required risk reduction achievement either by adding a SIF or other risk reduction measures.
- Record the action item closure and approval by the project or site authority (approved action response sheets should be retained).
- Track the transfer of action items between delivery teams (e.g., project to commissioning).
- Provide the technical reasons for recommendation resolution, including the suggestion of different action or rejection in writing and retained.
- Ensure that agreed recommendations are resolved appropriately as dictated by the project schedule.
- The site MOC process shall be followed for approved changes resulting from LOPA recommendations for the operating facilities.

11. References

[1] International Electrotechnical Commission (IEC), "Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidelines for the determination of the required safety integrity levels (IEC 61511-3)," 2018.

[2] Egyptian General Petroleum Corporation (EGPC), "Risk-Management Standard (EGPC-PSM-ST-001)," 2021.

[3] Egyptian General Petroleum Corporation (EGPC), "Egyptian General Petroleum Corporation (EGPC) Process Safety Studies in Oil & Gas Major Projects (EGPC-PSM-GL-002)," 2022.

[4] Center for Chemical Process Safety (CCPS), Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis, Wiley, 2013.

[5] Center for Chemical Process Safety (CCPS), Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, Wiley, 2015.

[6] Center for Chemical Process Safety (CCPS), Layer of Protection Analysis, Wiley, 2001.

[7] A. W. Cox, F. P. Lees, and M. L. Ang, Classification of Hazardous Locations, IChemE, 1990.

12. List of Annexes

- **Annex A -** Initiating Events Frequencies.
- **Annex B -** Independent Protection Layers PFD Data.
- **Annex C -** Enabling Conditions and Conditional Modifiers.
- **Annex D -** LOPA Worksheet Example.

Annex A - Initiating Events Frequencies

The initiating events (IE) data table in this Annex provides a typical generic initiating event frequency (IEF). These IEF values are generally considered conservative under the specified conditions. If, however, a site has data indicating that the actual IEF is higher than that shown in the data table, the actual site value should be used. It is also possible that site-specific data collection or a more quantitative risk assessment may indicate that a lower IEF may be used.

Reference: Center for Chemical Process Safety (CCPS), Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, Wiley, 2015.

Initiating Cause	Frequency (events/yr)
Aboveground piping full breach failure (pipe size <= 150 mm, 6 in)	1.00E-06 /m
Aboveground piping full breach failure (pipe size > 150 mm, 6 in)	1.00E-07 /m
Aboveground piping leak (pipe size <= 150 mm, 6 in)	1.00E-05 /m
Aboveground piping leak (pipe size > 150 mm, 6 in)	1.00E-06 /m
Underground piping leak (full breach)	1.00E-06 /m
Atmospheric tank catastrophic failure	1.00E-05
Atmospheric tank leak, 10-mm diameter, continuous	0.0001
BPCS control loop failure	0.1
Cooling water failure	0.1
Cooling water failure with redundant cold-water pumps and diverse drivers	0.01
Crane load drop	0.001 /lift
External fire, large (aggregate causes)	0.01
External fire, small (aggregate causes)	0.1
External impact (by a backhoe, vehicle, etc.)	0.01
Exchanger tube rupture (not leak)	0.001
Failure of check valve (high demand)	0.1
Failure of double check valves in series (high demand)	0.01
Hose leak (non-vibrating)	0.1
Hose leak (vibrating)	1
Hose rupture (non-vibrating)	0.01
Hose rupture (vibrating)	0.1
Human error during a task performed less than once per month	0.01
Human error during a task performed more than once per month but less than once per week	0.1
Human error during a task performed once per week or more often	1
Lightning strike	0.001

Initiating Cause	Frequency (events/yr)
Operator failure (to execute a complete, routine procedure; well-trained operator, unstressed, not fatigued)	0.01 /Opportunity
Premature opening of the spring-loaded relief valve	0.01
Pressure regulator failure	0.1
Pressure vessel catastrophic failure	1.00E-05
Pump seal complete failure	0.1
Pump seal complete failure (double mechanical with the ability to detect the primary failure and resulting action)	0.01
Pump seal leak	1
Pump, compressor, fan, or blower failure	0.1
Screw conveyor failure	1
Screw conveyor overheating of materials	0.1
Single circuit loss of power	0.1
Spurious operation of safety controls, alarms & interlocks	0.1
Turbine/diesel engine overspeed with casing breach	0.0001

Annex B - Independent Protection Layers PFD Data

Reference: Center for Chemical Process Safety (CCPS), Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, Wiley, 2015.

B.1. PFD for Passive IPLs

Passive IPL	Generic PFD	Special Considerations
End-of-line deflagration arrester	0.01	• The deflagration arrester is installed in the appropriate location and orientation per the manufacturer's recommendations. • The device does not impose excessive flow restrictions on the process, and any fouling issues have been addressed. • The device is used in the service for which it has been certified and tested. • An end-of-line device must be clear of ice and snow, debris, and nesting creatures that could block the device and impair its performance. • Elements are periodically inspected for polymer or other plugging material and internal corrosion of the flame arrester element.
In-line deflagration arrester	0.1 (without temperature monitoring and shutdown or isolation response). 0.01 (with temperature monitoring and shutdown or isolation response).	• The piping between a potential ignition source and the arrester is well below the run-up distance required to allow a transition to detonation (DDT). It does not include turbulence-inducing fittings that could cause DDT. • The deflagration arrester is installed in the appropriate location and orientation per the manufacturer's recommendations. • The device does not impose excessive flow restrictions on the process, and any fouling issues have been addressed. • Temperature monitoring with a thermocouple directly in contact with the hot side of the device is recommended to allow operations to recognize when the device is being challenged. The use of temperature monitoring with response increases the reliability of the device. • The device is used in chemical services for which it has been certified and tested.

Passive IPL	Generic PFD	Special Considerations
		Detonation arresters built to meet older standards (pre-1990s) are not guaranteed to prevent the passage of a deflagration.
In-line stable detonation arrester	0.1 (without temperature monitoring and shutdown or isolation response). 0.01 (with temperature monitoring and shutdown or isolation response).	• The device is installed in the appropriate location and orientation per the manufacturer's recommendations. • The device does not impose excessive flow restrictions on the process, and any fouling issues have been addressed. • Temperature monitoring with a thermocouple directly in contact with the hot side of the device is recommended to allow operations to recognize when the device is being challenged. The use of temperature monitoring with response increases the reliability of the device. • The device is used in chemical services for which it has been certified and tested.
Unstable (overdriven) detonation arrester	0.1 (without temperature monitoring and shutdown or isolation response). 0.01 (with temperature monitoring and shutdown or isolation response).	• The device is installed per the vendor recommendations, including location in the line and orientation (horizontal or vertical). • The device does not impose excessive flow restrictions on the process, and any fouling issues have been addressed. • Temperature monitoring with a thermocouple directly in contact with the hot side of the device, with reliability corresponding with the claimed value for the system, is recommended to allow operations to recognize when the device is being challenged. • Unstable detonation arresters require specific empirical determination of proper sizing for each stream composition.
Overflow line with no impediment to flow	0.001	• The overflow line is properly sized with no valves that could be closed, seal legs that could be frozen or blocked, or rupture disks that could fail to operate. • This failure rate assumes that the overflow line is in a clean service and not prone to fouling, plugging, or polymerization.

Passive IPL	Generic PFD	Special Considerations
		• The overflow line is designed to allow for inspection and to prevent blockage due to snow, ice, nests, or other debris. • The overflow line does not have a vertical rise above the top of the vessel or drum, which could result in the sum of the hydraulic and dynamic pressure being greater than the MAWP of the vessel.
Overflow line containing a passive fluid or with a rupture disk	0.01	• The overflow line is properly sized with no valves that could be closed or sealed legs with fluid that could freeze or foul. • This failure rate assumes that the overflow line is in a clean service and not prone to fouling, plugging, or polymerization. • The overflow line is designed to allow for inspection and to prevent blockage due to snow, ice, nests, or other debris. • The overflow line does not have a vertical rise above the top of the vessel or drum, which will result in the sum of the hydraulic and dynamic pressure being greater than the MAWP of the vessel. • For installations including rupture disks, the criteria, and considerations provided in the data tables for rupture disks also apply. The rupture disk opening pressure needs to be low enough that the vessel will not be over-pressurized if overfilling does occur.
Overflow line containing a fluid with the potential to freeze	0.1	• The overflow line is properly sized, and there is a possible impediment to flow, such as a seal leg that could freeze or a valve that could be closed. • It is assumed that reasonable design and maintenance precautions are taken to prevent situations that could result in freezing or an improperly closed valve. • The system is designed to allow for periodic inspection. • The PFD is higher than the PFD of the simple overflow line due to the increased failure rate associated with possible isolation of the line due to human error, mechanical failure, or weather.

Passive IPL	Generic PFD	Special Considerations
		• The overflow line does not have a vertical rise above the top of the vessel or drum, which will result in the sum of the hydraulic and dynamic pressure being greater than the MAWP of the vessel.
Dikes, berms, and bunds	0.01	• A management system is in place to ensure that drain valves on passive containment are maintained in the correct position and subject to a valve inspection program. • For the case of vessel failure, the containment systems are typically sized to contain the greatest amount of liquid that may be released from the largest storage tank within the diked area, providing a sufficient allowance for precipitation (refer to NFPA 30). • To use the containment system as an IPL in an overflow scenario in which the source of the overflow has a greater volume than the maximum dike capacity of the receiving tank (such as a pipeline), the capacity of the system is sufficient to ensure that the leak is detected before the dike capacity is exceeded. • The containment system height can withstand the hydraulic wave effects with minimal slosh over the dike walls.
Drainage to dikes, berms, and bunds with remote impoundment	0.01	• A management system is in place to ensure that drain valves on passive containment systems to remote impoundment are subject to a valve inspection program and maintained in the appropriate positions. • Rainwater is pumped from the deep impoundment to the appropriate sewer system to maintain adequate spill containment capacity. • Any pipe or trench used to transmit liquid to the remote impoundment is free of impediments to flow, such as insulation materials or debris from trees and shrubs. • For the case of vessel failure, the dike plus impoundment volume is generally sized to contain the greatest amount of liquid that

Passive IPL	Generic PFD	Special Considerations
		may be released from the largest storage tank within the diked area, providing a sufficient allowance for precipitation (refer to NFPA 30). • To use the containment system as an IPL in an overflow scenario in which the source of the overflow has a greater volume than the maximum dike capacity of the receiving tank (such as a pipeline), the capacity of the system is sufficient to ensure that the leak is detected before the dike capacity is exceeded. • The containment system height can withstand the hydraulic wave effects with minimal slosh over the dike walls.
Permanent mechanical stop that limits travel	0.01	• The stop is set and verified initially, with adjustment or slippage not possible afterward (such as welding the stop in place). • The reason for the placement of the mechanical stop must be understood and documented so that the stop is not inadvertently eliminated when equipment is replaced.
Fire-resistant insulation and cladding on the vessel	0.01	• ANSI/API 521 allows fire-resistant insulation as an alternative to a relief device sized for the fire case when an engineering analysis indicates that additional protection provided by the relief device serves little value in reducing the likelihood of vessel rupture. Vessels containing only vapor or high boiling liquids are mentioned as specific examples. • In some instances, only a limited amount of fuel is available to sustain a fire for a given period (the fire duration). The fire duration can be determined from a conservative estimate of the available fuel, combined with fuel burning rates available in the literature (e.g., Mudan 1984). • ANSI/API 521 also provides equations for calculating the heat input to the vessel, based on insulation conductivity and thickness, that can be used to calculate the time required to heat the vessel contents to

Passive IPL	Generic PFD	Special Considerations
		a vapor pressure corresponding to the vessel MAWP or relief device setpoint. When this heat-up time (with the fire insulation installed) is greater than the length of the fire, based on the burning rate and the amount of fuel available, fireproof insulation is a potential IPL to prevent overpressure and rupture of the vessel due to fire. • Process or storage vessels may contain materials that could, at elevated temperatures, react and generate heat or rapidly decompose. • This could result in potentially generating pressures or temperatures that may exceed the vessel MAWP and may not be relievable with conventional pressure relief devices. • Appropriate thermal stability testing may be necessary to establish conservative, safe temperature limits. • If fireproofing prevented the vessel from reaching an unsafe temperature before the fuel available was consumed, it could be a valid IPL in LOPA. • NOTE: If fire cladding was assumed in the calculation of the size of a relief valve that is claimed as an IPL in the LOPA scenario, then the combined PFD of the insulation plus relief valve is 0.01 (without a block valve in the relief line).

B.2. PFD for Active IPLs

Active IPL	Generic PFD	Special Considerations
Safety control loop	0.1	• A safety control loop consists of a sensor, controller, final control element, support utilities, and interfaces. It normally operates to support process (or regulatory) control. Its operation may be continuous or intermittent in responding to process deviations within the normal operating envelope, and its actions are sufficient to achieve or maintain a safe state of the process. • Equipment (or loop) failures may be revealed through process operation, automated diagnostics, or ITPM activities. The risk of continued process operation with a detected failure of the safety control equipment is assessed, and compensating measures are implemented to address any increased risk. • Changes to the safety control loop hardware and software are controlled using a MOC process. During any process operating mode where the scenario could occur, the safety control loop is only bypassed (placed into manual control) by the procedure since manual operation depends on the operator's response to changes in the process variable.
Safety interlock	0.1	• A safety interlock consists of a sensor, controller, final control element, support utilities, and interfaces. It acts to achieve or maintain a safe state of the process in response to a deviation from normal operation. • Equipment (or loop) failures may be revealed through process operation, automated diagnostics, or ITPM activities. The risk of continued process operation with a detected failure of the safety interlock equipment is assessed, and compensating measures are

Active IPL	Generic PFD	Special Considerations
		implemented to address any increased risk. • Changes to the safety interlock hardware and software are controlled using a MOC process. During any process operating mode where the scenario of concern could occur, the safety interlock is only bypassed with administrative approval and the implementation of any necessary compensating measures. Administrative approval may involve formal MOC, implementing bypass procedures with event tracking, following operating procedures, etc.
SIS loop	SIL 1 - 0. 1 SIL2 - 0.0 1 SIL 3 - 0.00 1	• SIL refers to the performance achieved by the SIS loop, given its probability of random and systematic failure in the operating environment. Each SIS loop achieves or maintains a safe process state concerning a specific scenario. Sensors, logic solvers, final elements, and related equipment that are required for the SIS loop to operate according to its specification are considered in the PFD calculation. The achievement of a PFD of < 0.1 requires rigorous design and management practices to ensure that the SIS loop is capable of achieving the claimed risk reduction in the specific operating environment, including sufficient protection against systematic and common cause effects. Unless it is intended to implement the equipment within the BPCS per IEC 61511, the equipment executing the SIS loop must be independent and separate from the BPCS equipment to the extent that the safety integrity of the SIS is not compromised (IEC 61511 Clause 11.2.4). For the PFD claimed above to be valid for SIL 2 and SIL 3 systems, the design of human interfaces for operations and maintenance should minimize the potential for human error

Active IPL	Generic PFD	Special Considerations
		during installation, maintenance, testing, and bypassing. • Equipment (or loop) failures may be revealed through process operation, automated diagnostics, and ITPM activities. The risk of continued process operation with a detected failure of the SIS equipment is assessed, and compensating measures are implemented to address any increased risk. • Changes to the SIS loop hardware and software are controlled using a MOC process. During any process operating mode where the scenario could occur, the SIS loop is only bypassed with administrative approval and the implementation of any necessary compensating measure. Administrative approval may involve formal MOC, implementing bypass procedures with event tracking, following operating procedures, etc. • The design, operation, configuration management, and ITPM practices ensure that the actual performance of the installed SIS loop achieves the target SIL.
The spring-operated pressure relief valve	0.01	• If there is an isolation valve (block valve) upstream or downstream of the relief device, then the suggested PFD is 0.1 unless there is a management system in place to ensure that valves are returned to service in their proper positions after maintenance and that they remain in the appropriate state during operation. • If fire cladding was assumed to be in place on the protected vessel in the calculation of the relief valve size, then the combined PFD of the insulation plus the relief valve is 0.01. • The PRV is sized for the scenario being considered.

Active IPL	Generic PFD	Special Considerations
		• The inlet and outlet piping are sized correctly and are mechanically adequate for relief flow. • The relief valve is in clean service, and the metallurgy is corrosion-resistant to the particular service. • The service under evaluation does not have the potential for freezing the process fluid before or during relief; if freezing is possible, then adequate heat tracing of the relief valve and piping is installed and maintained.
Dual spring-operated pressure relief valves	No isolating valves present: 0.001 A single valve that could isolate one PRV: 0.01 A single valve that could isolate both PRVs simultaneously: 0.1	• If a robust management system is in place to ensure valves are returned to service in their proper positions after maintenance and remain in the appropriate state during operation, it may be appropriate to claim an improved PFD reflective of actual system performance. A better PFD may be applicable if a thorough review of the equipment, process conditions, and management systems indicate the potential for common cause failure is sufficiently managed. • The PRVs are sized for the scenario being considered. • The inlet and outlet piping are sized and mechanically designed properly. • The relief valves are in clean service, and the metallurgy is corrosion-resistant to the particular service. • If the service under evaluation has the potential to freeze the process fluid before or during relief, developing a site-specific PFD is recommended.
The pilot-operated pressure relief valve	0.01	• If there is an isolation valve (block valve) upstream or downstream of the relief device or on the pilot line, then the suggested PFD is 0.1 unless there is a management system in place to ensure that valves are returned to service in their proper positions after maintenance and

Active IPL	Generic PFD	Special Considerations
		that they remain in the appropriate state during operation. • The PRV is sized for the scenario being considered. • The inlet and outlet piping are sized correctly and are mechanically adequate for relief flow. • The relief valve is in clean service, and the metallurgy is corrosion-resistant to the particular service. • The service under evaluation does not have the potential for freezing the process fluid before or during relief; if freezing is possible, then adequate heat tracing of the relief valve and piping is installed and maintained.
Gas balance/adjustable set pressure surge relief valve	0.01	• If there is an isolation valve (block valve) upstream or downstream of the relief device, then the suggested PFD is 0.1 unless there is a management system to ensure that valves are returned to service in their proper positions after maintenance and that they remain in the appropriate state during operation. • Valves may or may not include a set pressure spring. • The relief valve is in clean service, and the metallurgy is corrosion-resistant to the particular service. • The surge relief valve is sized for the scenario being considered. • The inlet and outlet piping are sized correctly and are mechanically adequate for relief flow. • Modeling confirms that response time is adequate for the application.
Buckling pin relief valve	0.01	• If there is an isolation valve (block valve) upstream or downstream of the relief device, then the suggested PFD is 0.1 unless there is a management system in place to ensure that valves are returned to service in their proper positions after

Active IPL	Generic PFD	Special Considerations
		maintenance and that they remain in the appropriate state during operation. • The buckling pin relief device is confirmed to be sized for the scenario. • The inlet and outlet piping are sized correctly and mechanically adequate for relief flow. • The relief valve is in clean service, and the metallurgy is corrosion-resistant to the particular service. • The service does not have the potential for freezing the process fluid before or during relief; if freezing is possible, then adequate heat tracing of the relief device and piping is installed and maintained.
Buckling pin isolation valve (BPIV)	0.01	• If there is an isolation valve (block valve) upstream or downstream of the BPIV, then the PFD is taken as 0.1 unless there is a management system in place to ensure that valves are returned to service in their proper positions after maintenance and that they remain in the appropriate state during operation. • The buckling pin valve is used in a clean service, and the metallurgy is corrosion-resistant to the particular service. • The buckling pin valve is properly rated to close at a pressure that will protect the downstream vessel.
Rupture disk	0.01	• If there is an isolation valve (block valve) upstream or downstream of the relief device, then the PFD is taken as 0.1 unless there is a management system in place to ensure that valves are returned to service in their proper positions after maintenance and that they remain in the appropriate state during operation. • The rupture disk (RD) is confirmed to be sized for the scenario. • The inlet and outlet piping are sized correctly and are mechanically adequate for relief flow.

Active IPL	Generic PFD	Special Considerations
		• The RD is in clean service, and the metallurgy is corrosion-resistant to the particular service. • The service under evaluation does not have the potential for freezing the process fluid before or during relief; if freezing is possible, then adequate heat tracing of the RD and piping is installed and maintained.
Spring-operated pressure relief valve with rupture disk	0.01	• If there is an isolation valve (block valve) upstream or downstream of the relief device, then the PFD is taken as 0.1 unless there is a management system in place to ensure that valves are returned to service in their proper positions after maintenance and that they remain in the appropriate state during operation. • The rupture disk and relief valve meet the special considerations for the individual devices. • The downstream side of the rupture disk is monitored to ensure the continued integrity of the RD. • Monitoring the space between the RD and PRV can be done using a pressure transmitter or switch with an alarm or a pressure gauge with routine operator inspections. Using the PRV/RD combination in the plugging service may also require flushing the process side of the rupture disk to keep it clean. • A non-fragmenting type of rupture disk is used to avoid blockage and reclosing of the relief valve by debris. • The metallurgy is corrosion-resistant to the particular service. • The service under evaluation does not have the potential for freezing the process fluid before or during relief; if freezing is possible, then adequate heat tracing of the relief device and piping is installed and maintained.

Active IPL	Generic PFD	Special Considerations
Conservation vacuum and/or pressure relief vent	0.01	• If there is an isolation valve (block valve) upstream or downstream of the relief device, then the PFD is taken as 0.1 unless there is a management system in place to ensure that valves are returned to service in their proper positions after maintenance and that they remain in the appropriate state during operation. • The relief vent is confirmed to be sized for the scenario being considered. • The vent is properly implemented; one reference is API 2000. • The inlet and outlet piping are sized correctly and are mechanically adequate for venting. • The vent is in clean service, and the metallurgy is corrosion-resistant to the particular service. • The device is operating in low-demand mode. • If freezing the process fluid or atmospheric moisture is possible, adequate heat tracing of the vent and piping is installed and maintained.
Vacuum breaker	0.01	• If there is an isolation valve (block valve) upstream or downstream of the vacuum breaker, then the PFD is taken as 0.1 unless there is a management system in place to ensure that valves are returned to service in their proper positions after maintenance and that they remain in the appropriate state during operation. • The vacuum safety valve, vacuum relief valve, or vacuum breaker is confirmed to be sized for the scenario being considered. • The inlet and outlet piping are sized correctly and are mechanically adequate for vacuum relief flow. • The service is non-fouling, and the vacuum breaker has no history of fouling. • The metallurgy is corrosion-resistant to the particular service.

Active IPL	Generic PFD	Special Considerations
		• The device is operating in low-demand mode. • The service does not have the potential to freeze the process fluid before or during relief. If freezing is possible, adequate heat tracing of the vacuum relief valve and piping is installed and maintained.
The frangible roof on a flat-bottom tank	0.01	The purpose of a frangible roof is to provide a venting area to protect against a bottom-seam failure of a flat-bottom storage tank, resulting in the tank being propelled from its foundation and instantaneously releasing the tank contents. Frangible roofs are useful in providing emergency venting where such a large venting area is required that other means of venting are impractical. The tank design basis is reviewed to ensure that the tank is designed appropriately and well-secured to the foundation. Key design features include: • The top seam will fail at the target pressure and below the lift pressure of the tank. • The specifications of the top angle ring (or its supports) are not exceeded since this is the critical element that is expected to fail first. Also, anything that increases the strength/stiffness of the top head (beyond specifications) could increase the failure pressure and is evaluated to ensure that the design will perform as originally specified. • The design of the tank anchor chairs, bottom ring, number of anchor bolts, and the diameter and length of the bolts is sufficient to keep the tank in place during a relief event. • The tank foundation is in an acceptable condition, with the anchor bolts well secured to the foundation. • No walkways, piping, or other obstructions would prevent the frangible roof from fully

Active IPL	Generic PFD	Special Considerations
		opening and relieving the necessary pressure.
Explosion isolation valve	0.1	• Refer to NFPA 69 Standard on Explosion Prevention Systems. • Explosion isolation valves can mitigate deflagration scenarios but not detonation scenarios.
Explosion panels on process equipment	0.01	• Explosion panels protect against vessel overpressure from dust/vapor/gas explosion. They are properly designed per NFPA 68 or the appropriate standard for the material being handled in the equipment. • Associated piping systems have proper relief design or have appropriate explosion prevention systems designed as per appropriate standards. • The explosion is routed to a safe location. • Explosion panels can protect against internal deflagrations but not detonations.
Vent panels on enclosures	0.01	• Vent panels are designed with sufficient relief area to prevent overpressure at the maximum temperature expected by a qualified expert using a proven method such that the panels will operate with a fast enough response time to mitigate the event effectively. This may require considering the momentum and backpressure of panels during an as well as the dynamic loading of receptors (e.g., walls). • For potential vacuum in the equipment, if applicable, the panels will remain reliable under actual process conditions. • To incorporate means to prevent injury to personnel and other equipment. These may include hinges and cables to prevent the panels from becoming projectiles and restrict personnel entry into the venting area. • Each ductwork has a clear path, with no resistance to flow that can impede the device's effectiveness.

Active IPL	Generic PFD	Special Considerations
		• Designed such that the panels can be periodically inspected/maintained. • References for design include NFPA 68, European VDI 3673, and ATEX Directive 94/9/EC.
Check valve	0.1	• The check valve operates in the low-demand mode. • The service is assumed clean, with no fouling or corrosion expected. • Even properly inspected and maintained check valves might not eliminate check-valve seat leakage. Consequently, the user should be aware that isolation of the low-pressure system upstream of the check valve can still result in overpressure. • The user must define the tolerable leakage rate for the scenario and determine whether a specific check valve is a valid IPL for the scenario of concern.
Pressure reducing regulator	0.1	• The pressure-reducing regulator operates in low-demand mode. • The service is assumed clean, with no fouling or corrosion expected. • The spring tension device is manually adjusted to the proper set point.
Multiple mechanical pump seal systems with seal failure detection and response	0.1	• The multiple mechanical pump seal system includes at least two mechanical seals, with means to detect and indicate a failure of the primary or secondary seal to the operator. Detection of leakage of one of the seals in a multiple mechanical seal system can be performed by online monitoring of the pressure of the barrier fluid or the level in the tank supplying barrier fluid to the seal. Once a seal leak is identified, the pump is isolated and repaired promptly before another seal fails. • The operator's response to shut down the pump and isolate the source of the leak is documented in a procedure, and the operator is trained to perform the task.

Active IPL	Generic PFD	Special Considerations
		• The task can be completed within the allowable response time. • Properly sizing the pump for the application will increase the seal's life. • Pump foundation design, piping design, installation, and pump alignment can all significantly impact the seal life on a pump.
Continuous ventilation *without* automated performance monitoring	0.1	This IPL is valid when released into an enclosure or room, creates a consequence of concern, and the ventilation is determined to be capable of mitigating the potential hazard.
Continuous ventilation *with* automated performance monitoring	0.01	This IPL is valid when released into an enclosure or room, creates a consequence of concern, and the ventilation is determined to be capable of mitigating the potential hazard. Performance monitoring: • The preferred alarm is based on a reliable measurement that ensures airflow exceeds a minimum value. The alarm functions independently of the loss of power to the ventilation fan. • Some performance measurement devices are also interlocked to shut down the operation upon loss of the fan.
Emergency ventilation is initiated by safety controls, alarms, and interlocks (SCAI)	0.1	• This IPL is valid only if the ventilation can mitigate the potential hazard. • The overall ventilation system, including the SCAI equipment, the fan or blower, and the power supply for the system, achieves the required performance claim. • The instrumentation used to start this emergency system meets the requirements for either a safety interlock IPL or a SIL 1 loop IPL.
Mechanically activated emergency shutdown/isolation device	0.1	The IPL is designed to meet the requirements of the specific system.
Mechanical Overspeed trip on a turbine	0.1	• This IPL represents a fully mechanical machine protection system. It usually consists of a bolt, a tripping mechanism

Active IPL	Generic PFD	Special Considerations
		that drains the control oil, and the trip and throttle (or stop) valve. • Other Overspeed protection devices consist of sensors, a logic solver, and final elements. These are considered SCAI and are credited as a safety interlock or an SIS IPL.
Automatic fire suppression system (within process equipment)	0.1	Several standards can guide automatic fire suppression systems for process equipment: • NFPA 11 *Standard for Low-, Medium-, and High-Expansion Foam* guides foam systems used in storage tanks. • NFPA 69 *Standard on Explosion Prevention Systems* guides the use of suppression systems in process equipment. • NFPA 91 *Standard for Exhaust Systems for Air Conveying of Vapors, Gases, Mists, and Noncombustible Particulate Solids* provides guidance on automatic extinguishing systems in process equipment. • NFPA 654 *Standard for the Prevention of Fire and Dust Explosions from the Manufacturing, Processing, and Handling of Combustible Particulate Solids* guides solids handling systems. • DIN EN 14373 is the European standard for explosion suppression systems. • ISO 6184-4 *Explosion protection systems - Part 4: Determination of Efficacy of Explosion Suppression Systems* (1985) is the ISO standard covering these systems.
Automatic fire suppression system for local application	0.1	Refer to: • NFPA 17 *Standard for Dry Chemical Extinguishing Systems.* • NFPA 2001 *Standard on Clean Agent Fire Extinguishing Systems* for information on dry powder clean agents and other flooding systems.
Automatic fire suppression system for a room	0.1	Refer to: • NFPA 17 *Standard for Dry Chemical Extinguishing Systems*.

Active IPL	Generic PFD	Special Considerations
		• NFPA 2001 *Standard on Clean Agent Fire Extinguishing Systems* for information on dry powder, clean agent, and other flooding systems.
Automatic explosion suppression system for process equipment	0.1	• The suppression system is mounted to the system to be protected and propels the extinguishing agent. • To be effective, the system is rapidly actuated. • For additional guidance, refer to NFPA 69 Standard for Explosion Prevention Systems.
Human response to an abnormal condition	0.1	• When the trigger for the human response is a safety alarm, the alarm is understandable and available to the operators in their usual work location(s). • When the trigger for the human response is a check or field sample, a procedure indicates the need for this check or sample and the required frequency. There is also written guidance on what to do if the check shows the reading to be out of a tolerable range. Readings are recorded in a checklist, in an appropriate form, or some form of a database. • The operator has sufficient time available to respond to the indication of an abnormal condition and complete the required action. This time is less than the time it takes for an event to become unavoidable. • There are clear procedures for the operator to follow to complete the response. The response task is low complexity, with step-by-step instructions and minimal diagnostics or calculations. • The operator is trained on the response task. • The operator taking the corrective action can do so without being put into a dangerous situation to accomplish the action.

Active IPL	Generic PFD	Special Considerations
		• The human factors related to oral communication, human-system interface, and work environment have been reasonably optimized.
Human response to an abnormal condition with multiple indicators or sensors and the operator has > 24 hours to accomplish the required response action	0.01	To achieve the generic PFD for this IPL: • There are multiple, unambiguous cues that there is an abnormal condition. • The available time for the operator to respond to the alarm and complete the required action is less than the time it takes for an event to become unavoidable. • There are clear procedures for the operator to follow to complete the response. • The operator is trained on the response task. • The operator taking the corrective action can do so without being put into a dangerous situation to accomplish the action. • The human factors related to oral communication, human-system interface, and work environment have been reasonably controlled.

Annex C - Enabling Conditions and Conditional Modifiers

C.1. Time at Risk

Time risk is set equal to 1 for continuous processes and for the discontinuous process, which works for more than 10% of the overall time. For a discontinuous process that works for less than 10% of the overall time (e.g., loading from a tank truck), the time risk is equal to 0.1.

C.2. Probability of Ignition and Explosion

Suggested values for the probability of ignition and explosion are illustrated in Table 4.

Reference: A. W. Cox, F. P. Lees, and M. L. Ang, Classification of Hazardous Locations, IChemE, 1990.

Table 4. *Probability of ignition and explosion.*

Release Rate	Ignition probability of a Gas or Mixture	Ignition Probability of a Liquid	Fraction of explosions given ignition of a Gas, Liquid or Mixture
<1 kg/s	0.01	0.01	0.04
1-50 kg/s	0.07	0.03	0.12
>50kg/s	0.3	0.08	0.3

C.3. Vulnerability (Probability of Injury/Fatality).

The vulnerability factor considers the probability of a person being directly involved in the effects of an undesired event. The factor shall consider the dynamics of the final scenario (e.g., fire) and the effective presence of people in the area where the impact is expected. Suggested values of vulnerability are illustrated in Table 5.

Table 5*. Vulnerabilities values.*

Event	Vulnerability Value
Jet fire/explosion in frequently manned areas	1
Jet fire/explosion in not frequently manned areas	0.5
Pool fire/flash fire in frequently manned areas	0.5
Pool fire/flash fire in not frequently manned areas	0.1

Annex D - LOPA Worksheet Example

Scenario Number: 01	Equipment Number: V-01	Scenario Title: V-01 Liquid Overfill
Consequence Description / Category	**Liquid carryover to the compressor train could lead to jet fire and a single fatality.**	
Target Mitigated Event Frequency	**Single Fatality**	**1.00E-05**
Initiating Event	**LICA-01 Failure**	**Operator Error**
Initiating Event Frequency	**0.1**	**0.01**
Layers of Protection		
Process Design	1	1
BPCS	1	0.1
Alarm and Human Intervention	1	1
Other IPL	1	1
Conditional Modifiers		
Time at Risk	1	1
Vulnerability	1	1
Ignition Probability	**0.03**	**0.03**
Frequency of Mitigated Consequences	**0.003**	**0.00003**
Total Mitigated Event Frequency	**0.00303**	
PFD - Target	**3.3E-03**	
SIL - Required	**SIL-2**	

Recommendations:
Install a SIL-2 high-level trip on V-01 to prevent liquid carryover to the compressor train with PFD = 3.3E-03

Notes and Assumptions:

- The target mitigated event frequency for one fatality is assumed to be 1E-5 (See Table 1).
- In this example, human error frequency is 0.01 (Human error during a task performed less than once per month) (Annex A).
- BPCS PFD is 0.1.
- The ignition probability is 0.03 (1 to 50 Kg/s liquid release) (Annex C).
- The operator is assumed to be 100% vulnerable (Jet fire/explosion in frequently manned areas) (Annex C).