



Exploration & Production

GENERAL SPECIFICATION

SAFETY

GS EP SAF 041

Technological risk assessment methodology

01	01/2011	Simplification / clarifications
00	10/2008	First issue - replaces GS EP EXP 401
Rev.	Date	Notes

Owner: EP/HSE

Managing entity: EP/HSE



Contents

1. Scope	6
1.1 General Principles	6
2. Reference documents.....	7
3. Terminology and definitions	9
3.1 Definitions	9
3.2 Abbreviations	13
4. Technological risk assessment	14
4.1 Five Steps of Risk Management.....	16
4.2 Two Parallel Methods for Risk Analysis.....	16
4.3 Life Cycle Risk Assessment	17
4.4 Scope of Work of Risk Assessment.....	17
4.5 Scenario Definition.....	20
4.6 Typical Upstream Scenarios.....	21
5. Hazard identification (HAZID).....	28
5.1 Objectives	28
5.2 Methods	28
6. Preliminary risk assessment.....	29
6.1 Objectives	29
6.2 Methods for Preliminary Risk Assessment	30
6.3 Scenario development	33
6.4 Frequency of Central Critical Event	35
6.5 Consequence Estimation.....	35
6.6 Frequency of Hazard Outcome.....	35
6.7 Damage Severity and frequency	36
6.8 Reporting	36
6.9 Preliminary Risk Assessment Validation Workshop	37
7. Risk management sheets	38
7.1 Objectives	38
7.2 Preparation of RMS Method	38



7.3	Review of Frequencies and Consequences	39
7.4	Format of Risk Management Sheets	39
7.5	RMS Reporting	40
7.6	Reporting and treatment of the other types of scenarios	41
8.	Detailed risk analysis of scenarios.....	42
8.1	Objectives	43
8.2	Review of Scenario	46
8.3	Frequency Analysis	46
8.4	Detailed Consequence Analysis	48
8.5	Escalation Potential	48
8.6	Sensitivity Studies	49
8.7	Probabilistic Estimation of Damage Category and Frequency	49
8.8	Risk Reduction Workshop	51
8.9	Updating of Detailed Risk Analysis	51
8.10	Reporting	51
9.	Quantitative Risk Analysis (QRA).....	52
9.1	Objectives	52
9.2	Preparation	54
9.3	List of Hazardous Events	54
9.4	Frequency Analysis	55
9.5	Consequence Analysis	55
9.6	Impact Analysis	55
9.7	Escalation Potential	56
9.8	Sensitivity Studies	56
9.9	Risk Presentation	56
9.10	Risk Reduction Workshop	57
9.11	Updating of QRA	57
9.12	Reporting	57
10.	Sensitivity analysis	58
10.1	Objectives	58
10.2	Defining Sensitivity Cases	58
10.3	Presentation of Sensitivity Analysis	59



11. Risk evaluation	59
11.1 Objectives	59
11.2 Evaluation Principles	59
11.3 Scenario Risk Evaluation	60
11.4 Quantitative Risk Evaluation	61
12. ALARP demonstration	63
12.1 Objectives	63
12.2 Targets for ALARP Demonstration	65
12.3 Risk Reduction Workshop	66
12.4 Qualitative Evaluation of Risk Reduction Measures	68
12.5 Quantitative Evaluation of Risk Reduction Measures	69
12.6 Cost Benefit Analysis	69
12.7 Reporting and ALARP Decision Tables	73
13. Major risk register	74
13.1 Objectives	74
13.2 Safety Critical Measures	74
13.3 Reporting	77
14. Audit and peer reviews	77
14.1 Objectives	77
14.2 Reporting Requirements	78
14.3 Audits	79
14.4 Peer Reviews	79
14.5 Terms of References of Reviews	80
14.6 Close out Audit and Peer Review Recommendations	80
Appendix 1 TRA Generic Scope of Work	81
1. Phase 1 PRA - Generic Scope of Work	81
2. Phase 2 DRA - Generic Scope of Work	82
3. Phase 3 – Alarp demonstration using Cost Benefit Analysis and Major Risk Register setting up Generic Scope of Work	84
Appendix 2 Hazard Identification (HAZID)	85
1. HAZID Checklist	85



2.	Hazard Identification Scheme	88
3.	Development Phases.....	89
4.	HAZID Leader and Team.....	90
5.	Reporting	91
6.	Follow-up of HAZID Recommendations	91
Appendix 3 Isolatable Sections and Hazardous Inventory		92
Appendix 4 HAZID Worksheet		94
Appendix 5 Critical Events Register		96
Appendix 6 Severity and Frequency Categories		98
1.	Damage Frequency Categories.....	98
Appendix 7 Hazard Intensity Thresholds		102
1.	Thresholds for Injury	102
2.	Hazard Intensity Thresholds for Environment.....	104
3.	Hazard Intensity Thresholds for Asset Damage	105
Appendix 8 FACILITATING TOOLS FOR PRA		106
Appendix 9 Assumptions Register		107
Appendix 10 Risk Management Sheets.....		110

1. Scope

The purpose of this general specification is to define methodology for performing technological risk assessment of onshore and offshore oil and gas upstream facilities.

The objectives of this specification are to enable setting scope of work for a technological risk assessment study, to provide essential information performing scenario based risk assessment and QRA studies and to interpret results of risk assessment studies.

- Basic Engineering Phase
- Detailed Design Phase
- Operation Phase
- Decommissioning Phase.

This specification does not cover the exploration phase and construction phase, as indicated in Table 1.

Table 1 - Applicability of GS EP SAF 041

Addressed in GS EP SAF 041	Not Addressed in GS EP SAF 041
Exploitation phase • Risk associated with accidental loss of containment • Risk associated with structural damage or stability impairment • Risk associated with natural hazards • Risk associated with Transportation risks (boat, helicopter...) QRA approach	Exploration Phase • Geological and Seismic campaign Occupational risks (Note 1) • Trips, slips, falls • Driving • Routine lifting or transfer • Short-term exposure to chemicals • Long term exposure to chemicals Construction risks (outside operating plant limits)

Note 1: When Individual risk is the criterion (QRA); occupational risks should be taken into account to estimate the overall level of individual risk for risk evaluation.

1.1 General Principles

The following are the main principles for applying this General Specification:

1. This specification is aimed at risk analysis specialists and safety engineers who are directly involved in risk assessment of upstream oil and gas facilities.
2. Detailed risk analysis estimates potential loss of life (PLL) associated with an event or during life of a facility. These numerical estimates of risks are based on historical statistics on failures which represent an average quality of safety management. These numerical values shall not be interpreted as unavoidable or absolute value of loss. Instead, these numerical values should be used to characterize potential accidents and thereby



developing risk reduction measures to prevent them, if not, minimize the likelihood and severity.

3. Company technological risk acceptance criteria discussed in this specification shall be considered as minimum requirements compared to respective local laws and regulations. Compliance with local or national regulatory requirements on risk acceptance criteria shall be considered as the primary requirement.
4. Scope of work shall be explicitly defined prior to commencement of any risk assessment programme identifying the boundaries, activities, methodology, risk acceptance criteria and validation method.
5. Quantitative Risk Analysis (QRA) and detailed risk analysis of scenarios give an impression of objective analysis. But these methods utilize a number of assumptions, input data which are often judgmental. These judgments may be explicit where areas in which data are reliable and where assumptions are realistic while there are also many implicit judgments where data are not directly available. Overlooking the significance of such assumptions and input data may lead to inaccurate estimation of risk.
6. The quality of modeling and input data will affect the robustness of numerical risk estimates. Therefore, uncertainties associated with risk results shall always be considered in the risk management process.
7. Technological Risk Assessment shall not be used in support of designs which are not in compliance with Total specifications Design of E&P oil and gas facilities is foremost based upon Total E&P's referential. This specification is not aimed at being utilized for risk based design. A deviation from Total E&P's referential shall be adequately justified in a derogation request even before referring to any risk assessment study given as a support.

2. Reference documents

The reference documents listed below form an integral part of this General Specification. Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published at the EFFECTIVE DATE of the CONTRACT.

Standards

Reference	Title
ISO 17776	Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment

**Professional Documents**

Reference	Title
Report N° 434-12	Risk Assessment Data Directory - Occupational risk, OGP, March 2010
Ministère de l'Ecologie et du Développement Durable, version Octobre 2004	Guide technique relatif aux valeurs de référence de seuils d'effets des phénomènes accidentels des installations classées
SPC/Tech/OSD/30	Indicative Human Vulnerability to the Hazardous Agents Present Offshore for Application in Risk Assessment of Major Accidents, Health and safety Executive, United Kingdom, version # 2, 2010/10/01
ISBN: 0-7506-7555-1	Lee's Loss Prevention in the Process Industries
CPR 16E	Methods for the determination of possible damage ("Green Book"), first edition, TNO, Apeldoorn, 1992

Regulations

Reference	Title
ISBN: 0105437743NT	Health and Safety at Work etc Act 1974 (Elisabeth II 1974 Chapter 37)
ISBN: 0717621510	Reducing Risks, Protecting People, HSE's decision –making process, Health and Safety Executive, United Kingdom, 2001

Codes

Reference	Title
Not applicable	

Other documents

Reference	Title
Not applicable	

Total General Specifications

Reference	Title
GS EP SAF 253	Impacted area, restricted area and fire zones

3. Terminology and definitions

There are three types of statements in this specification, the “shall”, “should” and “may” statements. They shall be understood as follows:

Shall	shall be understood as mandatory. Deviating from a “shall” statement requires derogation approved by the Company.
Should	shall be understood as strongly recommended to comply with the requirements of the specification. Alternatives shall provide a similar level of protection and this shall be documented.
May	Is used where alternatives are equally acceptable.

The specific terms and abbreviations used in this specification are presented below.

3.1 Definitions

Acceptance criteria	Criteria that are used to express a risk level that is considered acceptable for the activity in question (risk associated with a scenario, IRPA etc.)
Accident event	Event or chain of events that may cause loss of life, health, or damage to environment or assets.
ALARP	“As Low As Reasonably Practicable” A risk reduced to levels such that further risk reduction measures would be so disproportionate that it would be objectively unreasonable to implement them.
Barriers	Equipment, system or set of procedures (either hardware, software or organizational) which lowers the probability of hazard occurrence (prevention), or the severity level of the consequence (mitigation, reduction of the vulnerability of the object).
Blow down	Depressurization of process system.
Bow-tie	Bow-tie diagram is a representation of all the initiators and various consequences or event outcomes. At the centre of the diagram is the central critical event, to the left is what could cause the central critical event to occur from initiating events (including threats and preventative barriers) and the right contains potential consequences and mitigation barriers.
Central Critical event	Central Critical Event is same as Central Hazardous Event. Generic event conventionally defined within the framework of a risk analysis, as the centre of the accidental sequence. Generally it is about loss of containment. The events located upstream are called initiating events or intermediate events which are part of the fault tree while events located downstream the central critical event are part of the event tree.
Coastal area or fragile area	The area from the coastline extending up to 22 km (12 nautical miles) offshore. Or Fragile system area: areas where there are sensitive ecological receptors for example but not limitative freshwater source, ponds, rivers, threatened species, state



	protected areas, etc.
Company	Referred to TOTAL Exploration & Production or its affiliate.
Contractor	Any person or an organization who is directly involved in execution of prescribed work under a contract with the reporting to Company or Company representative.
Escalation	Spread of the impact of a hazardous event to equipment or other areas, thereby causing an increase in the consequence of the event.
Event tree analysis	Utilizes a graphical tree construction that shows the logical sequence of the occurrence of events in, or states of, a system following a central critical event. Events tree helps to quantify the frequencies of various hazard outcomes (thermal, explosion overpressure, toxic, missiles, structural stability etc.) from the frequency of central critical event.
FN (Curve)	Curve of "cumulative Frequency per year to have more than N fatalities". Similar concepts are utilized for Cost (F-C Curves), Spill (F-S Curves) and asset damage (F-D Curves).
Frequency	In risk analysis, frequency refers to the probable number of occurrences of an event or which have occurred of a state for finite period (number of occurrences per annum or million hours).
Hazard	The potential to cause harm, including ill health or injury; damage to property, plant products or the environment; production losses or increased liabilities.
Hazard outcome	This term describes the characteristics of the physical effects; chemical etc. associated a hazard concerned. Examples are thermal radiation, toxic concentration, overpressure, missiles, pollution, structural impairment, etc.
HAZID	Hazard Identification study: Set of methods to identify the potential hazards and mitigation measures of an installation.
IDLH	Immediately Dangerous to Life and Health. Maximum concentration during which an individual can be exposed at least 30 minutes without experiencing irreversible effect to health.
Individual Risk Per Annum	Individual Risk per Annum (IRPA) is defined as the frequency at which an individual may be expected to sustain lethal levels of harm from the realization of specified hazards. It is usually taken to be the risk of death, and expressed as a risk per year.
Isolatable Section	Part of the process facility which may be isolated by the ESD system. A scenario is related to a given isolatable section with a given hydrocarbon inventory and a given leak frequency related to the number and types of equipments pertaining to the isolatable section.
Jet Fire	The combustion of material emerging from an orifice with a significant momentum.



Leak (release)	Accidental escape to environment of liquid and / or gaseous components of process (or used in the process) which are normally contained in a process system.
LCx(y)	Lethal Concentration (LCx): Atmospheric concentration which, for a specified duration of exposure, will cause the death of x% of an exposed population after y minutes. e. g. LC1% (30) means 1% fatality after a 30-minute exposure.
LC1%	The lethal effect threshold corresponds to the value below which one does not observe more than 1% of deaths among the exposed population.
Major risk	The risks associated with scenarios having potential damage severity of "catastrophic" or above to people, environment or asset.
Major scenarios	The scenarios with potential damage severity of "catastrophic" or above to people, environment or asset.
Mitigation	Reduction of the effects of a hazardous event. Means taken to minimize the consequences of a major accident to personnel and the installation after the accident has occurred.
Off Shore (Environment Severity)	Further than 22 km (12 nautical miles) of coastal shores.
Parts Count	The counting of any piece of equipment pertaining to a given isolatable section. This task is handled in order to calculate a generic leak frequency value for generic (corrosion, erosion..) types of cause.
Pool fire	Combustion of flammable liquid spilled and retained on a surface.
Potential loss of life	A probable number of fatalities resulting from the realization of hazards for a finite period. The PLL is an indicator to be utilized as a theoretical tool for risk comparison purposes only with the objective of reducing risk to ALARP. The PLL in itself is not an absolute indicator of the level of risk to the people. In the QRA, PLL represents an aggregate probable fatalities resulting from all scenarios. A partial PLL can be calculated for a given scenario or a set scenarios in a scenario based risk analysis approach.
Probability	A number in a scale from 0 to 1 which expresses the likelihood that one event will succeed another.
Probit	The probit function is another name for the inverse of the cumulative Gaussian distribution, in risk assessment it is used for calculating probability of death of a person at a given exposure.
Public	Human beings, installations or organizations who are outside the installation's fence and who are not commissioned by company to conduct a work approved by them.

Quantitative Risk Analysis (QRA)	QRA is a mathematical means of estimating numerical risk from a particular hazardous activity. It involves making numerical estimates of hazard outcome in terms of frequencies and consequences, and aggregating them into overall measure of individual or group risks.
Register of Assumptions	An essential deliverable of any Risk Assessment study which shall trace out and document any major assumption or specific methodology or origin of data which might impact the results of the study.
Reliability	Probability that an item is able to perform a required function under stated conditions for a stated period of time or for a stated demand.
Risk	Two-dimensional entity characterizing an unwanted event by its likelihood of occurrence and the extent of consequences arising from the occurrence of this event.
Risk analysis	Quantification of the level of risk of an installation according to a given methodology.
Risk Assessment	Overall process of risk analysis and risk evaluation.
Risk evaluation	Judgment, on the basis of risk analysis, of whether a risk is tolerable
Risk Management	Continuous process during the life cycle of an installation, which include risk assessment of each phase of the life cycle (the process reviewed periodically during operation phase).
Risk matrix	A matrix depicting risks with increasing severity levels in rows and likelihood in columns.
Risk Reduction Measure	Action or measure taken as new barrier to lessen the frequency, negative consequences, or both, associated with a risk.
Safety Critical Measure	A measure comprises any item of equipment or procedure whose failure would immediately result in a major event with consequence category catastrophic or above, posing a risk of serious injury, death or an unacceptable contamination of the environment or damage to asset.
Scenario	Sequence of events leading to an accident. A scenario is defined based on a set of data and assumptions relating to the initiating event, intermediate event, prevention barriers, central critical event, mitigation barriers, hazard outcome, protection barriers, vulnerability sequence .
Technological risk	Risks associated with the use or processing of toxic, flammable and/or explosive substances.
Tolerable risk	Risk which is accepted in a given context based on the risk acceptance criteria.
Validation	Comparison of analytical results from the calculations with experience derived from reviewing results of large number of cases to ensure that the physical bases and assumptions of the model are appropriate and produce accurate results.

Vulnerability Susceptibility of a target (human beings generally) when subjected to a given type of effect. The vulnerability models make it possible to evaluate the gravity of damage to human, asset, environment associated with intensity of effects (for example: thermal, explosion overpressure, toxic, missiles, structural stability etc.).

3.2 Abbreviations

ALARP	As low as reasonably practicable
BLEVE	Boiling Liquid Expanding Vapor Explosion
CFD	Computational Fluids Dynamics
CHARAD	Collection of Hazard and Reliability Data (Company's internal database)
EERA	Escape, Evacuation and Rescue Assessment
EFFECTS®	Modeling software for the effects and consequences of accidental release of hazardous substances developed by TNO.
ESD	Emergency Shut-Down
FERA	Fire and Explosion Risk Analysis
FMEA	Failure Mode Effects Analysis
FN (Curve)	Curve of "cumulative Frequency per year to have more than N fatalities". Similar concepts are utilised for Cost (F-C Curves), Spill (F-S Curves) and asset damage (F-D Curves)
HAZID	Hazard identification Study
HAZOP	Hazards and operability Review
HIPS	High integrity protection system
HIPPS	High integrity pressure protection system
HSE (UK)	United Kingdom Health and Safety Executive
ICAF	Implied Cost to Avert a Fatality
IDLH	Immediately Dangerous to Life and Health. Maximum concentration during which an individual can be exposed at least 30 minutes without experiencing irreversible effect to health.
IEC	International Electro-technical Commission
IRPA	Individual Risk per Annum.
ISO	International Organization for Standardization
LCx(y)	Lethal Concentration (LCx): Atmospheric concentration which, for a specified duration of exposure, will cause the death of x% of an exposed population after y minutes. e. g. LC1% (30) means 1% fatality after a 30-minute exposure.
LC1%	The lethal effect threshold corresponds to the value below which one does not



observe more than 1% of deaths among the exposed population.

LSIR	Location Specific Individual Risk
OGP	The International Association of Oil & Gas producers
OREDA	Offshore Reliability Data
P&ID	Piping and instrumentation diagram
PFD	Process flow diagram or Probability of failure on demand
PHA ST ®	Process Hazards Analysis Software Tools - Det Norske Veritas (DNV).
PHA ST Risk ®	Process Hazards Analysis Software Tools with risk integration DNV
PLL	Potential Loss of Life
POB	Personal On Board
PRA	Preliminary Risk Assessment
QRA	Quantitative Risk Analysis (in this document). Aggregate individual risk assessment approach is denoted as QRA based risk assessment.
RMS	Risk Management Sheets (a method of detailed risk analysis for assessing risk less severe scenarios - moderate, serious and major severities)
RRW	Risk Reduction Workshop
SCM	Safety Critical Measures
SDV	Shut Down Valve
SEI	Seuil des Effets Irréversibles in French. It is the irreversible effect threshold corresponds to the value below which one does not observe significant effects for the majority of the individuals. (SEI for 30 minutes is equivalent to IDLH for toxic effects).
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TNO	Toegepast-Natuurwetenschappelijk Onderzoek (Netherlands Organisation)
TR	Temporary refuge
TRA	Technological Risk Assessment
UVCE	Unconfined vapor cloud explosion
WOAD	World-wide Offshore Accident Databank

4. Technological risk assessment

Technological risks are risks associated with flammable, toxic, or explosive substances handled or processed during oil and gas extraction, treatment, storage or transportation activities. These risks impact individuals and public (directly or indirectly involved in the activities), the environment, integrity of the installations and associated production.

Technological risk management involves periodic assessment of risks during development cycle of a facility and where mandatory assessment of appropriate risks reduction measures to bring levels of risk within the pre-defined risk tolerability criteria.

The simplified flow scheme of technological risk management process is shown in Figure 1.

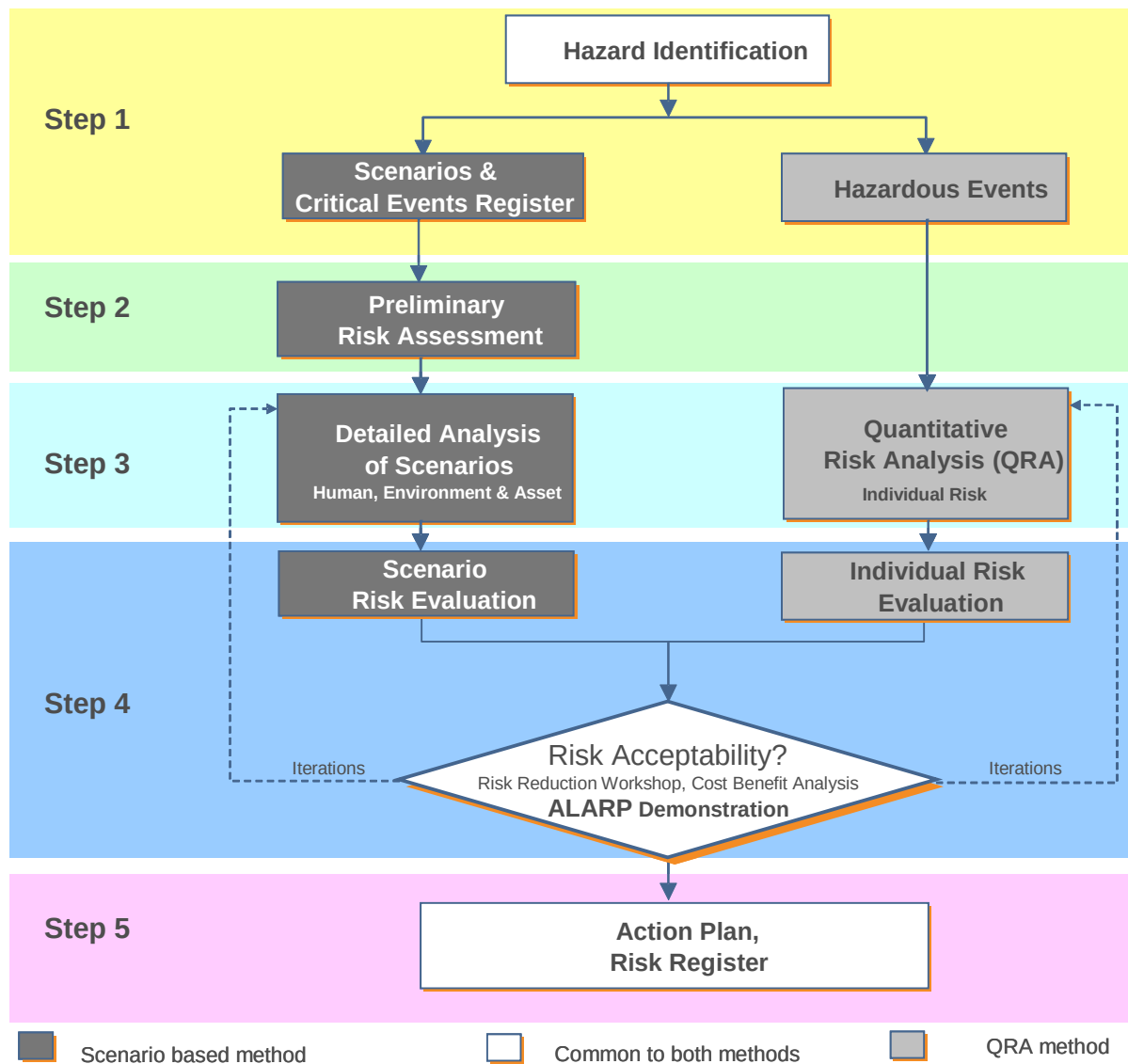


Figure 1 - Five Steps and two possible parallel risk analysis approaches

4.1 Five Steps of Risk Management

The five steps of technological risk management process are as follows (Figure 1):

Step 1	hazards Identification
Step 2	Development of scenarios and preliminary risk assessment
Step 3	Detailed risk analysis of selected scenarios and supplementary Quantitative Risk Analysis (QRA) for certain situations
Step 4	Risk evaluation and ALARP demonstration
Step 5	Action plan on the implementation of risk reduction measures (risk treatment)

Level of details and depth of the above steps differ considerably with development phases. For example, depth of risk assessment during pre-project phase may be limited to a semi-quantitative analysis to enable screening of major scenarios for detailed risk quantification during the subsequent phases.

4.2 Two Parallel Methods for Risk Analysis

As shown in Figure 1, the technological risk management process includes the following two parallel methods:

Application	Risk Analysis Method
Mandatory	Scenario based risk assessment This includes hazard identification, preliminary risk assessment, detailed analysis of "major scenarios" and evaluation risk acceptability of each scenario with respect to human, environment, and asset impact. Treatment of risk associated with major scenarios to meet Company's scenario risk acceptance criteria.
Supplementary (in certain conditions)	QRA based risk assessment This includes aggregation of risk to individuals from all scenarios including occupational and transportation risks to estimate Individual Risk Per Annum (IRPA). IRPA levels of the most exposed worker groups are evaluated with respect to risk acceptability criteria. Treatment of risk associated with major aggregate individual risk to meet Company's IRPA acceptance criteria.

Scenario based risk assessment is mandatory for all developments and existing facilities within Total E&P.

The QRA method is aimed at quantifying aggregated risks to human. This method is also mandatory if and only if, local regulation requires it. In such case QRA method may be considered as an alternate method to scenario method provided acceptance of a derogation request granted by DGEP/HSE/SEI. The derogation shall be supported by an analysis and treatment of all catastrophic and disastrous scenarios towards Environment and Asset.

However QRA may complement scenario risk based assessment in cases of:

- Large permanently manned Offshore facilities
- Facilities potentially impacting public safety
- Facilities which are outside Company operating experience
- Facilities incorporating major new technology and concept
- Specific request of the Responsible Entity in charge of Technological Risk Assessment in the affiliate or project.

4.3 Life Cycle Risk Assessment

The development cycle of an upstream facility shall include the following phases Figure 2):

- Exploration (seismic data gathering, exploration drilling)
- Feasibility and concept selection studies
- Pre-project
- Project (basic engineering, detailed design)
- Project (construction, installation, hook-up and commissioning)
- Development drilling
- Operations (including minor modifications)
- Revamping or modification (major modification is treated as pre-project and project)
- Decommissioning.

The details of risk assessment efforts may vary during the life cycle due to availability of details. Hazard identification shall universally be applied to all development phases.



Figure 2 - Development Phases of an Oil & Gas Installation

4.4 Scope of Work of Risk Assessment

Risk assessments whether carried out using internal Company resources or using Contractor shall have a clear scope of work which prepared in advance. Scope of work document shall be reviewed by competent specialists within Company.

No risk assessment shall be initiated without a written and approved scope of work. Scope definition shall describe battery limits, operational phases, methodology, risk acceptance criteria, input data and tools to be utilized for the assessment.

The scope of risk assessment shall be split into three distinctive phases (as indicated in Figure 3). The recommended phases are the following:

- Phase 1 (Steps 1 & 2) which includes hazard identification, development of scenarios, preliminary risk assessment, and PRA validation workshop
- Phase 2 (Steps 3 & 4) which includes detailed analysis of selected scenarios, QRA (if applicable), risk evaluation, risk reduction workshop, updating of risk analysis and input to Company's ALARP demonstration
- Phase 3 (Step 5) which includes Company's ALARP demonstration, preparation of action plan for management approval, major risk register including identification of safety critical measures.

For small facilities like a wellhead or receiving facility, preliminary risk assessment step can be eliminated and scenario risk assessment can be made directly using Steps 3 and 4.

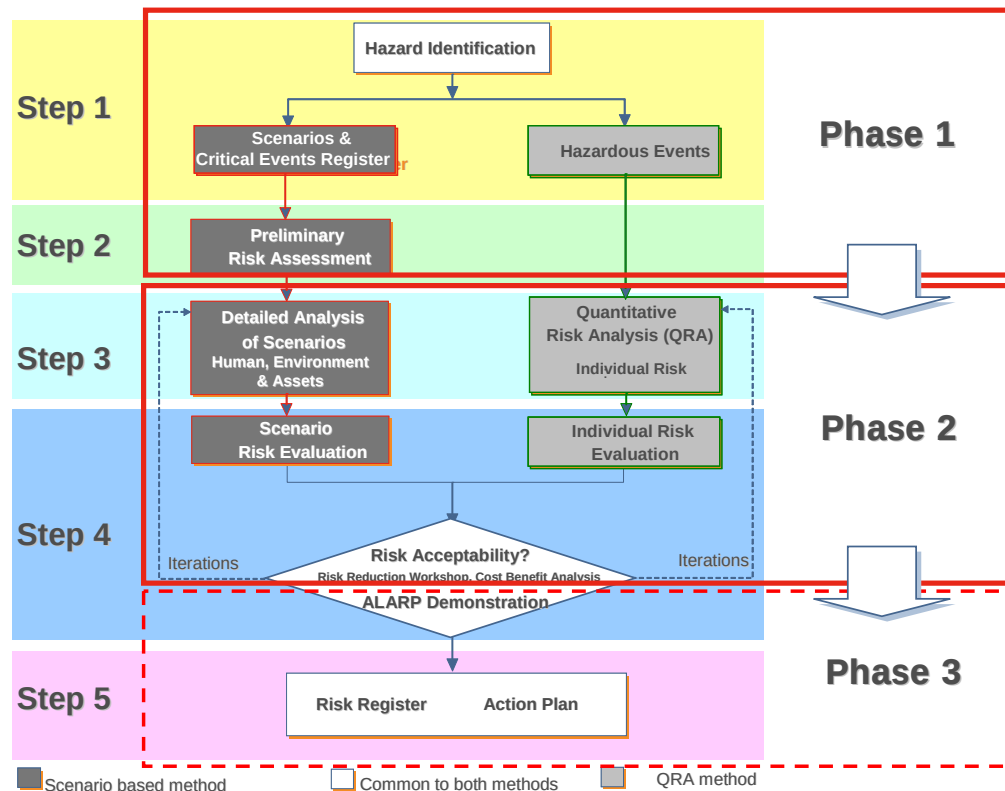


Figure 3 - Three distinctive Phases for the development Scope of Work

For simple and very similar types of normally unmanned installations (ex: simple wellhead platform) Technological Risk Assessment may be performed on a single representative case.

Justification of the right representativeness of the selected case shall be fully argued in the Register of Assumptions of the study.

Contents of generic scope of work associated with the three recommended phases are presented in Appendix 1. The scope of work shall be adapted to reflect the development cycle and complexity of development.



4.4.1 Documents Required for Performing Risk Assessment

The risk assessment requires facility documentation and availability of the documentation will depend on stage of development. The documents indicated in Table 2 should be made available for performing risk assessment.

Table 2 - Recommended set of documents for performing risk assessment

#	Documents
1	Process and Utility Flow Diagrams
2	Piping and Instrumentation Diagram
3	Layout Drawings
4	Plot plan and elevation drawings
5	General arrange drawings
6	Design Basis
7	Manning and population distribution
8	Material balance + compositions + Operating Conditions
9	Safety Concept Document
10	Operating and Maintenance Philosophy
11	Electrical single line drawing
12	Simplified Safety System PFDs (including ESD Logic diagrams)
13	Cause and effect charts
14	Process and Equipment datasheets
15	Previous HAZID, HAZOP, SPOT Reports
16	Previous Safety studies – Fire Zone, Restricted Area, Impacted Area drawings with calculations.
17	Previous Safety Studies – Blow out risk assessment
18	Previous Safety Studies – Dropped object risk assessment
19	Previous Safety Studies – Fire and risk assessment
20	Previous Safety Studies – Subsea Isolation risk assessment
21	Previous Safety Studies – Collision risk assessment
22	Previous Safety Studies – CFD Dispersion and Explosion assessment
23	Previous Safety Studies – HIPS Dossier
24	Previous Safety Studies – Flare radiation, flame out risk assessment
25	Escape and evacuation risk assessment
26	Site emergency response plan

#	Documents
27	Fire water network drawings – Fire water capacity calculations
28	Enclosure – ventilation and pressurisation schemes
29	Temporary refuge Impairment – Criteria
30	Active and Passive fire fighting system – description
31	Emergency depressurization – philosophy and description
32	Fire and Safety detector layout drawings
33	Hazardous area classification drawings (plan, elevations)
34	Life saving equipment description (lifeboat, capsules etc.)
35	SIMOPS / COMOPS (Matrix of permitted operations)
36	Historical site incident records (accidents and near misses)
37	Asset value register
38	Logistical information: marine traffic, vehicle profiles, helicopter traffic, lifting manifest, crane characteristics.

4.5 Scenario Definition

The term “scenario” has a specific meaning in the application of this specification. The definition of a scenario is as follows:

Scenario is a sequence of events leading to an accident. A scenario is further defined based on a set of data and assumptions which relate a hazard into an initiating event, prevention barriers, central critical event, mitigation barriers, hazard outcome, protection barriers, and damage sequence as illustrated below:

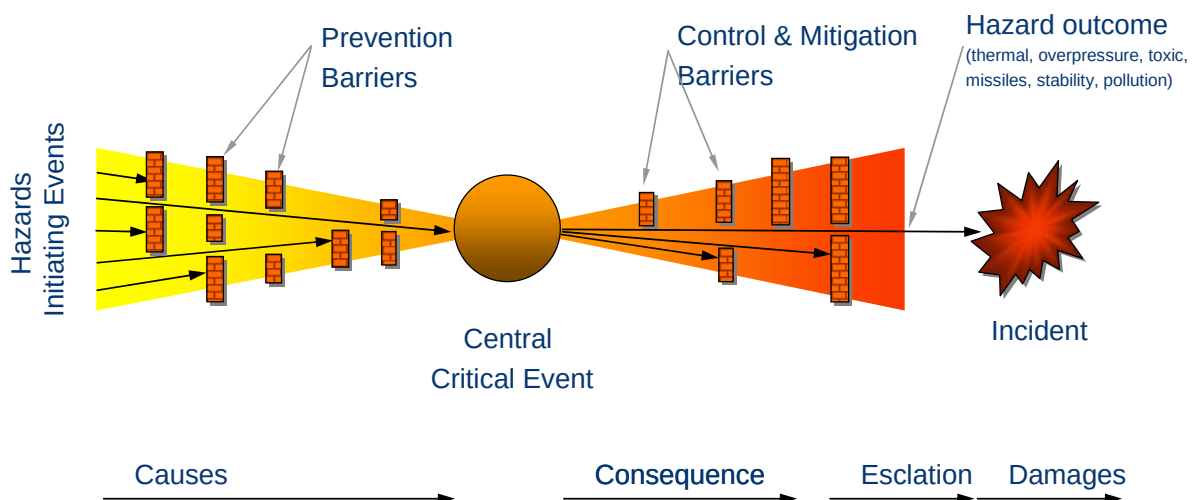


Figure 4 - Scenario as a sequence of events

In a scenario based risk assessment, acceptability of risk associated with each hazard outcome is judged with respect to the damage frequency and severity with respect to the Company risk acceptance matrix. Therefore, strict adherence to the definition shall be followed in a scenario based risk assessment.

As illustrated in Figure 5, a scenario shall consist of the following elements:

- An initiating event or events. (Note that all initiating events shall be considered if a scenario is associated with a generic process release)
- Unique central critical event. (e.g.: Loss of containment, small or medium or large)
- Unique hazard outcome based on isolated or un-isolated outcome. (Hazard outcomes are thermal radiation or dose, explosion overpressure, toxic dose, projectiles, pollution, stability impairment).

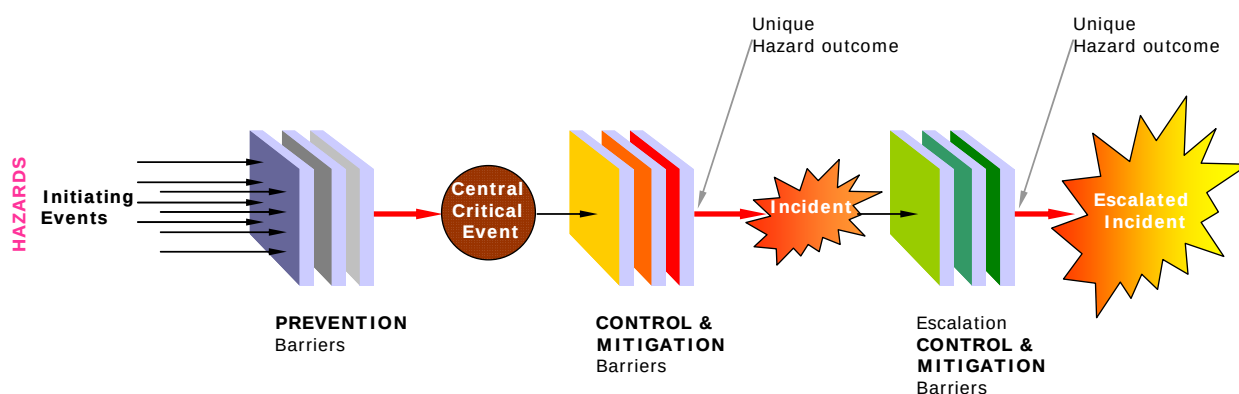


Figure 5 - Simplified illustration of a scenario

In general, frequency of central critical event is made using a fault tree analysis approach except if the hazard is related to generic process release. For generic process releases, the frequency of central critical event (loss of containment – small, medium or large) shall be based on approved database on process release (e.g. CHARAD).

Modeling of hazard outcomes shall be made using event trees analysis where likelihood of various event tree outcomes (for example, jet fire, pool fire, flash fire, explosion, dispersion, stability, structural failure etc.) shall be estimated from the central critical event frequency using branch probabilities.

The damages associated with a specific event tree outcome or combined event tree outcomes related to a unique hazard outcome (thermal radiation or dose, explosion overpressure, toxic dose, spill, structural impairment) shall be calculated using consequence and vulnerability models and the results shall be presented in terms of damage severity and damage frequency on the Company risk acceptance matrix.

4.6 Typical Upstream Scenarios

The following categories shall be reviewed for defining scenarios for risk assessment of upstream oil and gas facilities:

4.6.1 Blowout

Blowout is related to well systems and shall be reviewed with respect to phases of operation; (namely, drilling, well intervention, production, etc.).



- Initiating Events
 - Causes of blowout varies which includes loss of well control measures, failure of well control equipment, failure of well control procedures, failure of well control barriers, mechanical impact, etc. All causes during an operational phase shall be combined for defining the scenario related to blowout.
- Central Critical Events
 - Central critical events related to blowout shall be release of formation fluid to atmosphere. Frequency of central critical event shall be determined based on historical data and fault tree analysis.
- Hazard Outcome
 - Hazard outcome associated with blowout scenario shall be based on one of the following event tree outcomes as a physical effect:
 - . Jet / pool fire (thermal radiation, smoke - toxicity)
 - . Flash fire (thermal dose)
 - . Explosion (explosion overpressure)
 - . Spill (pollution)
 - . Toxic dispersion (toxic dose).

Examples are:

- Jet fire resulting from loss of containment during drilling operation due to well control failures
- Oil spill resulting from loss of containment during drilling operation due to well control failures.

4.6.2 Generic Process Release

Generic process releases are related to an isolatable section or part thereof of a facility. The release frequencies shall be estimated based on historical data of equipment release which include all generic causes leading to loss of containment.

- Initiating Events
 - Generic causes are corrosion, erosion, vibration, fatigue, construction defects, mechanical failure, human error, and contribution due to natural and impact events to any specific equipment or section.
- Central Critical Events
 - Central critical events shall be further developed based on three different release sizes as per Table 3.

Table 3 - Release sizes for scenario based risk analysis

Release size	Diameter range (mm) for frequency estimation	Representative diameter (mm) for consequence calculations
Small	1 – 5	5
Medium	5 – 65	65
Large	65 – full bore	Diameter of pipe or the largest flanged connection

- Small release size should only be utilized for process section handling high levels of H₂S or toxic fluids (0.2% mole fraction or higher) or operating above 100 barg or for oil or condensate unmanned installations with regards environment risk. For all other cases, medium and large release sizes shall be assessed for scenario based risk analysis.
- Frequency of central critical events shall be determined based on historical data using Company failure rate database, CHARAD. Company approval shall be sought for the use of additional historical data. For existing facilities, the frequency of leaks stemming from data base should be checked and may be adjusted referring to actual loss of containment incident reporting figures over a suitable period (5 years min). The adjusted value shall be documented in the assumption register.
- Fault tree analysis approach shall not be used for determining generic process release frequencies. However, the fault tree analysis shall be recommended for conditioning release frequencies with respect to a specific design/operation which are not at all representative to generic data.
- Hazard Outcome
 - Scenario shall be defined based on unique hazard outcome based on isolated or un-isolated consequence. Scenario shall be defined based on one of the following isolated or un-isolated event tree outcome:
 - . Jet / pool fire (thermal radiation, smoke - toxicity)
 - . Flash fire (thermal dose)
 - . Explosion (explosion overpressure)
 - . Spill (pollution)
 - . Toxic dispersion (toxic dose).

Examples of scenarios related to process release are:

- Isolated jet fire resulting from immediate ignition of medium release from vapor section of the test separator (D-100) during normal operation.
- Un-isolated explosion resulting from delayed ignition of vapor cloud associated with large release from liquid section of the deethaniser column (C-101) during normal operation.
- Isolated toxic dispersion resulting from a small release associated with condensate export pump (P-905).

4.6.2.1 Rules for Defining Isolatable Sections

The isolatable sections shall be defined and marked up either on P&IDs or on PFDs based on the following principles:

- The isolation boundaries shall be defined by ESD valves, blow down valves, control valves limiting the flow of hazardous gases to flare, and control valves with failure close position with input from shutdown system to close.
- In some instances, it is possible to define “pseudo Isolatable section” when the plant is not provided with ESDV or SDV (old installation). Manual valves and remote controlled valves may be considered as isolation boundaries. In that case the probability of failure of isolation should be assessed accordingly; time for isolation should also be taken into account for calculation of released material.

4.6.2.2 Rules for Defining Sections within an Isolatable Section

Sections within an isolatable section shall be defined based on the following hierarchy principles:

- Fluid phase (2-phase, vapor, liquid)
- Operating pressure differences within an isolatable section.

This is illustrated in Figure 6 as an example for an isolatable section. The sections for scenario risk assessment in this example are as follows:

- 2-phase fluid inlet section (inlet pipe work between inlet isolation valve and vessel inlet nozzle)
- Liquid outlet section (half the vessel and pipe work between liquid outlet nozzle and liquid outlet isolation valve)
- Vapor outlet section (half the vessel and pipe work between vapor outlet nozzle and vapor outlet isolation valve).

For each section, two or three release sizes (small, medium and large) shall be reviewed as defined in Section 4.6.2 for preparing the critical events register (ref to Section 6.3.2).

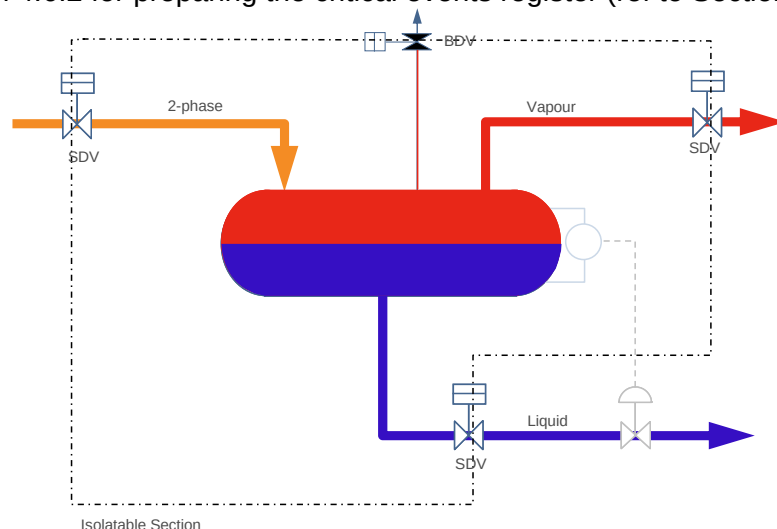


Figure 6 - An example of an isolatable section and subsections

4.6.3 Specific Major Process Hazards

Specific major process hazards are specific situations identified during either HAZID or process safety analysis. The initiating events, central critical events and hazard outcomes shall be defined on a case by case basis for defining scenarios related to specific major process hazards. Typical examples for scenarios associated with specific major process hazards are presented in Table 4.

Table 4 - Examples of scenarios associated with Specific Major Process Hazards

Initiating event(s)	Central Critical Event	Hazard outcomes
Specific overpressure protection system failure on demand.	Mechanical damage or loss of containment	Thermal radiation Toxicity, Spill Explosion/ BLEVE, Missiles
Specific under pressure protection system failure on demand	Mechanical damage or loss of containment	Thermal radiation Toxicity, Spill Explosion, Missiles
Overfilling of storage tanks and failure of level safety devices on demand. Human error	Loss of containment from storage tanks.	Thermal radiation Spill Explosion
Process control failure leading to ingress of air into process leading to a flammable mixture. Human error	Internal ignition	Internal Explosion, Missiles
Dust accumulation in silos or storage tanks.	Ignition of fine dust particles	Explosion, Missiles
Accidental process release from vent stacks	Ignition of release	Thermal radiation or dose
Flame out due to flare re-ignition failure	Flame out	Toxicity Thermal dose

4.6.4 Major Mechanical Impact Hazards

Major Mechanical Impact hazards are dropped or swinging objects, vessel collision, aircraft collision, projectiles, vehicle impact etc. Scenarios related to major mechanical impact hazards shall be reviewed based on site specific layout and operations characteristics. The central critical events can be either structural damage or loss of containment and shall be evaluated on a case-by-case using dedicated safety studies (for example dropped object risk analysis, collision risk analysis etc.)

The frequencies of central critical events shall be estimated using historical data coupled with fault tree analysis to incorporate site specific characteristics. Examples of scenarios related to major mechanical impact hazards are presented in Table 5.

Table 5 - Examples of scenarios associated with Major Mechanical Impact Hazards

Initiating event(s)	Central Critical Event	Hazard outcomes
Equipment failure or External or environmental influences or Human error	Major dropped object or swinging object	Structural impairment Thermal radiation Explosion Spill, toxicity
Aircraft impact	Mechanical damage /Loss of containment or structural damage	Structural impairment Thermal radiation Spill, toxicity Explosion
Vessel collision (offshore)	Mechanical damage / loss of containment	Stability impairment Thermal radiation Spill, toxicity Explosion
Vehicle impact (onshore)	Loss of containment	Thermal impairment Spill, toxicity Explosion
Anchor dragging, trawling (pipelines or subsea infrastructure)	Mechanical damage / loss of containment	Stability impairment Thermal radiation Spill
Mechanical failure or fatigue (mooring lines, tendons of tension leg platform, foundation, critical member fatigue)	Mechanical damage	Stability impairment

4.6.5 Natural Hazards

Natural hazards are associated with accidental events due to wind, current, wave, ice movement, earthquake, soil movements, subsidence, flooding, hurricanes or cyclones, tornado, tsunami, volcanic eruption etc.

Installations are designed to certain level of exceedance of the natural events. Therefore, scenarios to be reviewed shall be associated with residual risks beyond design safety levels.

Natural hazards shall be reviewed systematically or developing related scenarios. The central critical events can be structural damage, stability impairment or loss of containment and shall be evaluated on a case-by-case using site and design characteristics using dedicated safety studies (for example structural risk assessment.)

The frequencies of central critical events shall be estimated using historical data coupled with fault tree analysis to incorporated site specific and design characteristics. Examples of scenarios related to natural hazards are presented in Table 6.

Table 6 - Examples of scenarios associated with Natural Hazards

Initiating event(s)	Central Critical Event	Hazard outcomes
Extreme weather (wind, wave, current)	Loss of containment / structural damage	Structural Impairment Spill, toxicity Thermal radiation Explosion
Extreme seismic events	Loss of containment / structural damage	Structural Impairment Thermal radiation Spill, toxic dispersion Explosion
Icebergs	Loss of containment / structural damage	Structural Impairment Thermal radiation Spill, toxic dispersion Explosion
Subsidence	Loss of containment / structural damage	Structural Impairment Thermal radiation Spill, toxic dispersion Explosion
Punch through (jack-up rigs)	Structural damage	Structural Impairment Spill
Scouring	Loss of containment / structural damage	Structural Impairment Thermal radiation Spill, toxic dispersion Explosion
Flooding	Structural damage	Structural Impairment Spill
Tsunami	Structural damage to coastal facilities.	Structural Impairment Spill

5. Hazard identification (HAZID)

5.1 Objectives

The objective is to systematically identify all hazards which can potentially lead major incidents either directly or through escalation of events based on life cycle operation of a facility. This is the first step of any technological risk assessment as highlighted in Figure 7.

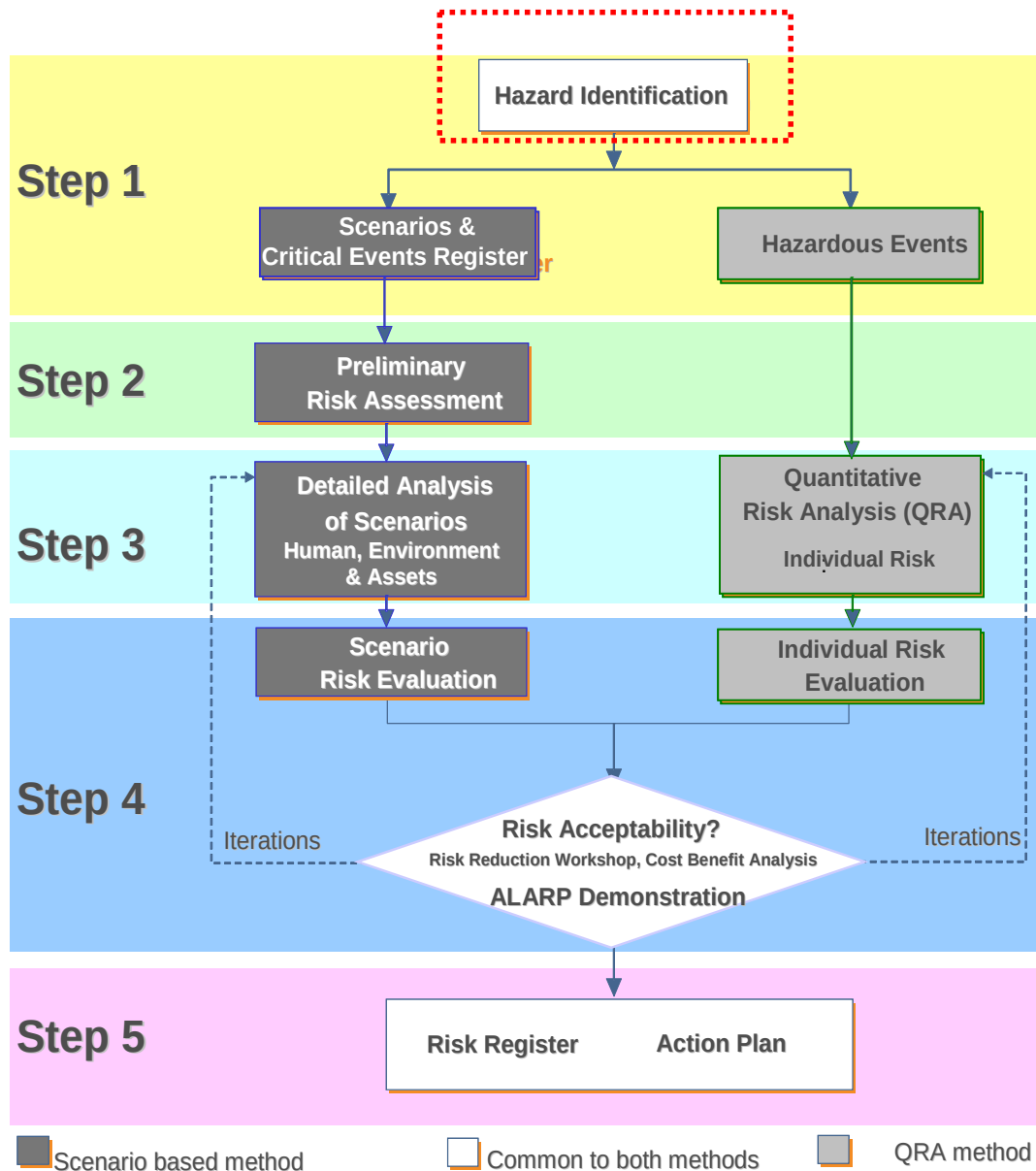


Figure 7 - Hazard Identification as part of the risk management process

5.2 Methods

HAZID shall be performed based on a structured brain storming session using an appropriate checklist. Complete life cycle of a facility shall be considered in the HAZID addressing simultaneous operations like drilling and production, well intervention and production,

construction and production, campaign maintenance and production, decommissioning some units. Pre project HAZID shall be entirely revised in order to include TRA requirements for scenario development.

HAZID session shall review non-process hazards and process hazards (hazards associated with unplanned releases). In particular, the following aspects shall be systematically reviewed:

- Impact of the facility to its surroundings
- Impact of the surroundings to the facility
- Interference between main units
- Location / orientation of plant and equipment
- Location / orientation of plant and equipment
- Unplanned releases for isolatable sections or units
- Environmental hazards, and natural hazards.

A checklist shall be prepared for facilitation of HAZID sessions to trigger quality brain storming. An example of a checklist is presented in Appendix 2. The checklist shall include the following elements:

- External Hazards
 - Natural and environmental hazards (impact of the environment on the plant)
 - Environmental Impact (impact of the plant on the natural environment)
 - Effect on the plant of man-made hazards
 - Hazards from the infrastructure supporting the facilities.
- Facility Hazards
 - Process Hazards (based on isolatable sections), specific process: gas blow by, blocked outlet, packing depacking situations, piping rating change, etc.
 - Utility Systems Hazards (loss of utilities)
 - Other hazards within the facilities (e.g. material handling, crane operation, electricity, radio- active substances, object under induced stress, etc.).

6. Preliminary risk assessment

6.1 Objectives

Objective of the preliminary risk assessment is to conservatively establish scenarios to be studied in detailed risk analysis. The risks associated with scenario hazard outcomes to human, environment and assets are screened with respect to damage frequency and severity categories using the Company risk screening matrix (refer to Figure 11) to establish the list of scenarios to be studied in detail.

The preliminary risk assessment is applicable only for scenario based risk analysis. The role of PRA in the overall technological risk management process is highlighted in Figure 8. For small upstream facilities like wellhead platform, minimal facility gathering, wellheads, manifold station

etc , the preliminary risk assessment can be eliminated all together and detailed risk analysis can be directly used for estimating risks associated with scenarios.

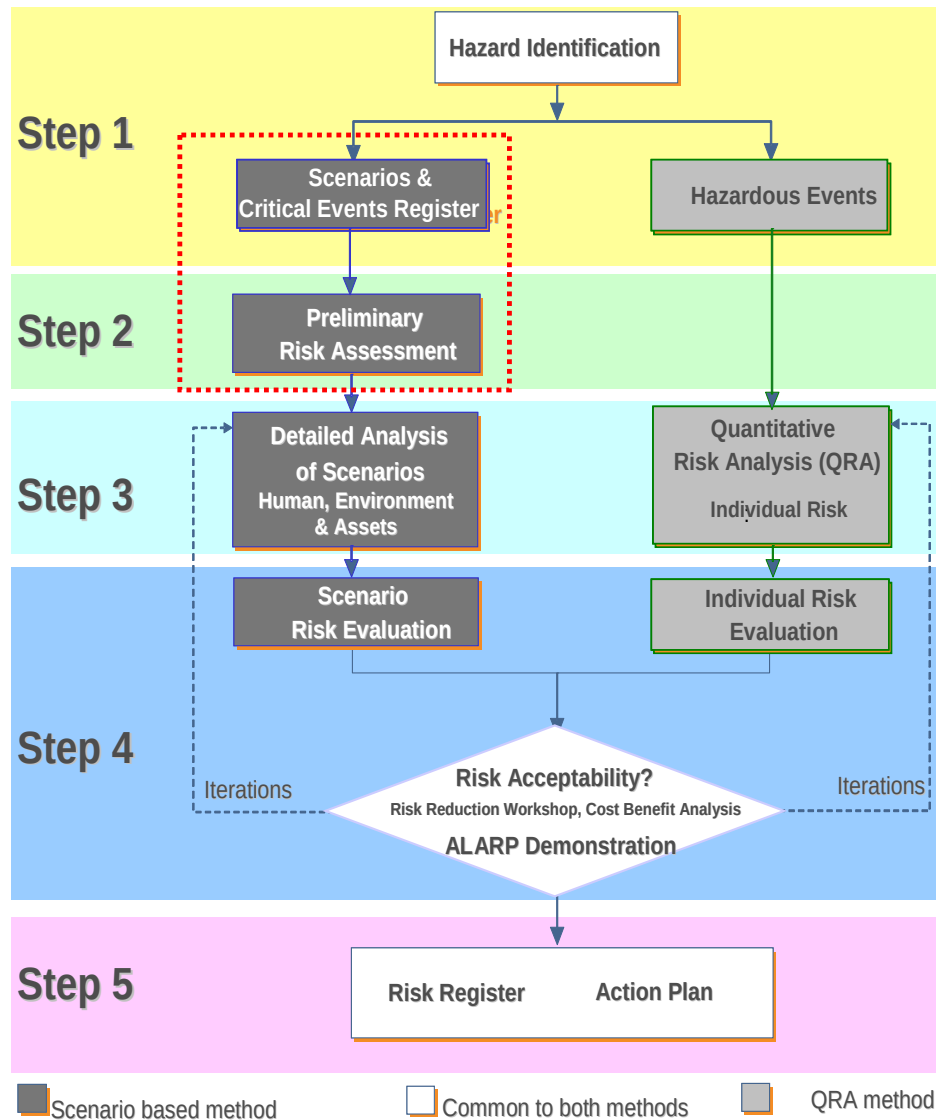


Figure 8 - PRA as part technological risk assessment

6.2 Methods for Preliminary Risk Assessment

Preliminary risk assessment involves semi-quantitative estimation of scenario risk to human, environment and asset.

Two methods are utilized for the preliminary risk assessment, namely:

- simplified method and
- rigorous method.

The preferred method is the rigorous method but in some instances the simplified PRA approach may suffice subject upon Company approval.

**The simplified PRA approach:**

This may apply to below concerned facilities:

- Facilities at Pre-project development stage
- Facilities in Project and Operational phases and contain only standard non toxic fluids below 100 barg
- Facilities in Project and Operational phases and contain only standard simple equipments like standard separators, piping.. New technologies are excluded.

The simplified PRA approach is very similar to ranking hazards following a hazard identification study using a team of experts with competence in performing risk analysis of oil gas upstream facilities. However the simplified PRA approach is not a purely qualitative exercise which may be biased by subjective risk perception. The simplified but conservative consequence and frequency assessment shall be performed based on the utilization of simplified consequence modeling tools and generic part count tools based on recognized historical data base.

In the simplified PRA approach, Hazid study is immediately followed by a ranking of hazards based on simplified but conservative estimation of gravity and frequency.

All calculations assumptions shall be documented in an assumptions register.

Conservative and simplified estimation of gravity:

Consequence modeling: ie use of abacus or simplified consequence excel tool and simplified but conservative personal distribution.

Conservative estimation of frequency:

Specific Excel tool like generic part counts tools can be utilized in order to get quickly the frequency of the Central Critical Events (loss of containment: medium and large).

CHARAD access data base can be used in order to get ignition probability based on initial release rate and type of fluid (liquid or gas). Appendix 8 briefly describes Total in house simplified modeling tools.

The rigorous method involves systematic identification of scenarios, development of consequences and frequencies (based on detail part counts and event trees) to establish conservative estimate of damage severities and consequences of each scenario.

The rigorous PRA method shall systematically be applied to the following situations:

- Facilities with potential impact to public safety
- Large permanently manned facilities
- New technologies and operations involving significant hazards to people which are considered outside the experience envelope of Company.

Main differences between rigorous PRA method and DRA:

The rigorous PRA method uses generally coarse and conservative consequence model (initial flow rate, simple but conservative ignition model, etc.)

At PRA level many factors may not be taken into account: direction of Jet Fire, screen effect to thermal impact due to high level of congestion of installation, provision for deluge, PFP, blow down, manning distribution accuracy, detail meteorological conditions.

The preliminary risk assessment shall include the following steps as illustrated in Figure 9:

- Scenario development
- Frequency of central critical events
- Consequence of scenario hazard outcome.
- Frequencies of hazard outcome
- Severity level of damage (human, environment and asset)
- Reporting
- PRA validation workshop.

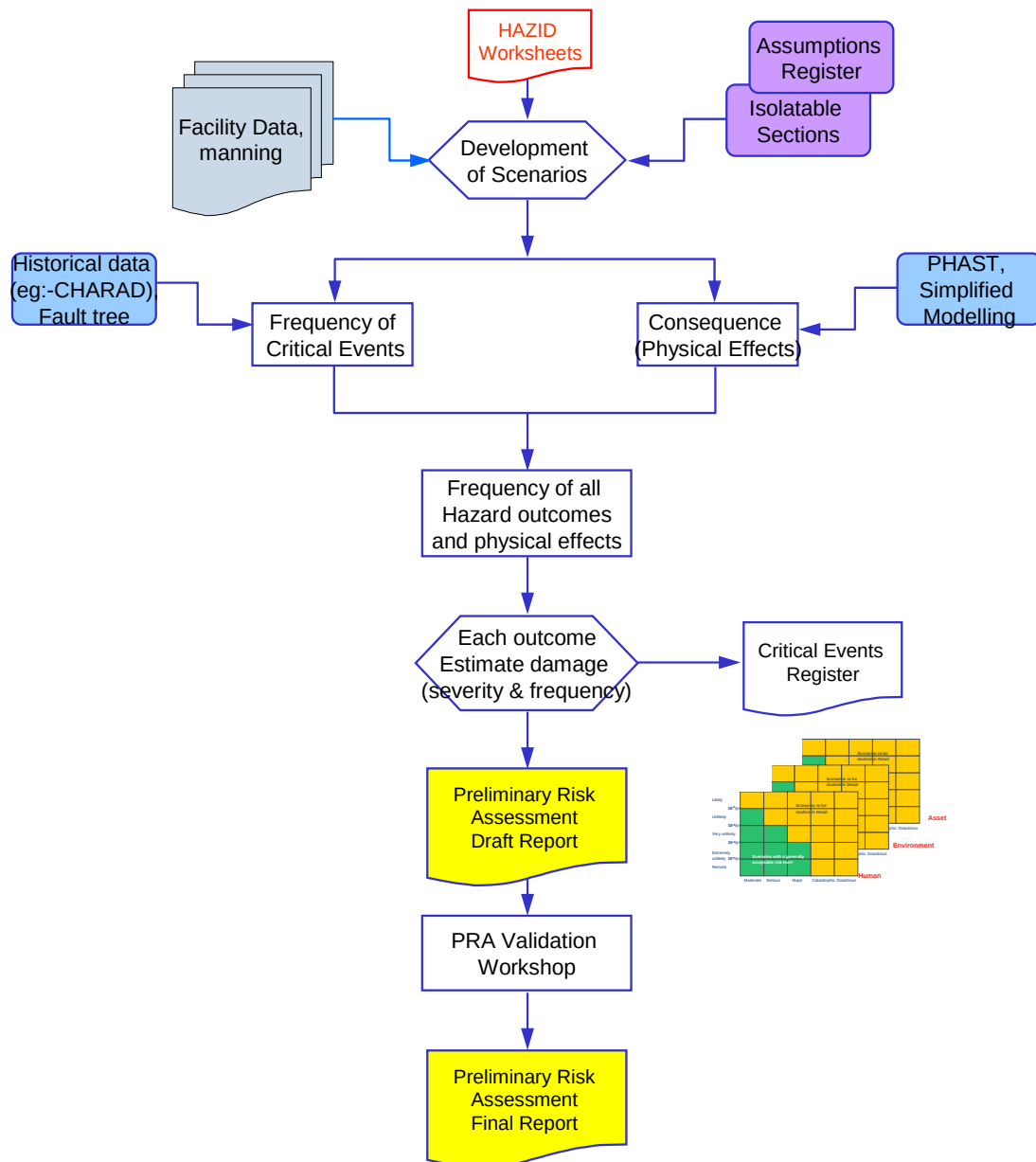


Figure 9 - Steps involved in a "rigorous" Preliminary Risk Assessment



6.3 Scenario development

6.3.1 Preparation

The preparation for the scenario development shall include the following activities:

- Prepare a list of documents with document number, title, revision number
- Prepare a list of isolatable sections indicating stream numbers, pressure, temperature, isolating devices (upstream and downstream), list of equipment, estimate of vapor volume, liquid volume within an isolatable section
- Prepare a file of PFDs and on P&IDs with marked-up isolatable sections
- Prepare a marked up copy of layout drawings
- Compile environmental data (wind, wave, current, etc. if applicable), including wind directionality data (wind rose diagram)
- Obtain production characteristics and composition of process streams
- Obtain manning levels and distribution
- Obtain population data surrounding the facility
- Obtain rough estimate values of equipments
- Obtain high level operating and maintenance philosophy
- Obtain lifting data (nb of lifts/ year, weight/lift, etc.)
- Obtain ship traffic data around the installation
- Review of HAZID worksheets and reports
- Prepare a set of assumptions to be compiled in the assumptions register

The level of details the above varies depending on the phase of development.

6.3.2 HAZID Worksheets to Critical Events Register

The objective of this task is to develop specific scenarios from the hazard identification worksheets. A review of the HAZID worksheet shall be carried out to define scenarios as per definitions given in Sections 4.5 and 4.6.

The expected output is to produce a list a comprehensive scenarios (known as critical events register) which shall include description of the system or section, initiating events, preventive barriers, central critical event, mitigation barriers, consequences (hazard outcomes), protection measures and duration of hazard outcome. Critical event template presented in Appendix 5 shall be utilized for preliminary risk assessment.

During the review, preparing a complete list of all possible process release scenarios can be cumbersome. Therefore, process release scenarios shall be sorted in such way that only representative scenarios shall be selected for evaluation.

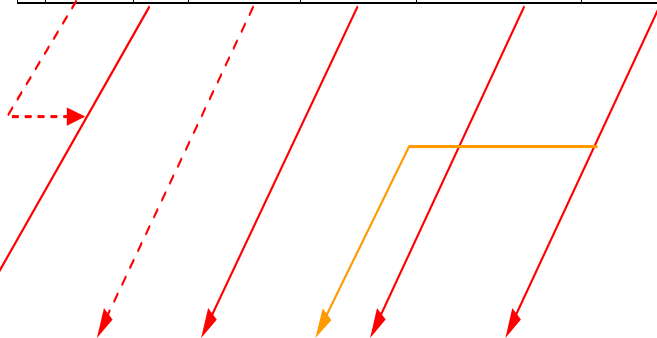
The sorting shall be based on similar characteristics of frequency of central critical event, consequence of hazard outcome and damage potential to people, environment or asset

The translation of HAZID worksheets to Critical Events Register is illustrated in Figure 10 Expert judgment is always involved in this task and therefore all assumptions made by the expert shall

be systematically documented using an “Assumptions Register”, which shall be updated and maintained throughout the risk assessment process. Format of the assumption register is presented in Appendix 6.

HAZID Worksheets

No	System Node	Unit Location	Guideword	Cause	Potential consequences	Safeguards	Recommendations / Remarks	Priority



Critical Events Register

Functional Blocks	Operating or environment parameter	Central Critical Events	Causes	Preventive measures	Hazard outcomes	Mitigation measures	Duration of the Hazard outcome	Ref. #	Damage Severity & Damage Frequency						Comments
									Human severity	Human frequency	Environ-severity	Environ-frequency	Asset severity	Asset frequency	

Figure 10 - Translation of HAZID Sheets to Critical Events Register

A complete inventory of “Individual” Central Critical Events (CCE) can rapidly generate an excessive number of scenarios to be considered. It is therefore recommended to group together similar events and to choose one representative CCE for this group in order to obtain smaller representative set of Central Critical Events. Regrouping criteria are:

- Equipment of similar design, including the associated safety systems, located in the same area of the plant
- Equivalent operating conditions and product properties
- Similar type of leak or rupture and same level of frequency
- Similar consequences.



The representative CCE may be associated with the combination of the most severe frequency and consequence

The list of facilities and grouped events shall be justified and appropriately recorded in the assumption register.

6.4 Frequency of Central Critical Event

The next task is to conservatively estimate frequency of the central critical event of all selected scenarios of the critical event register. The frequency estimation shall be based on historical data. Fault trees analysis may be considered as an option if there are no relevant historical data available to estimate the frequency.

The main sources of historical data are as follows:

- WOAD (Worldwide Offshore Accident Databank)
- OREDA (Offshore Reliability Data)
- CHARAD Database (Company internal database).

Parts count method shall be utilized in the rigorous PRA method for determining central critical event frequencies associated generic process releases (small, medium and large).

6.5 Consequence Estimation

Consequence analysis shall be carried out to estimate physical effects associated with each hazard outcome. For scenarios with loss of containment as the central critical events, this task is relatively easy. The physical effects associated with a hazard outcome shall be estimated using commercial tools such as PHAST or EFFECTS or simplified consequence analysis tables. Approval from Company shall be sought for the use of software/tools and tables for consequence estimation.

The following parameters shall be evaluated for estimating damage severity:

- Duration of release (with and without isolation)
- Distance to hazard intensity levels - (SEI if relevant, LC1% if relevant and fatality)
- Kinetics and escalation potential.

For scenarios associated with non-process events, the consequences shall be based on engineering estimate with the help of structural and hydrodynamic expertise. The hazard intensity threshold for defining SEI, LC1% and fatality zones shall be as per Appendix 7.

6.6 Frequency of Hazard Outcome

A simplified event tree analysis shall be considered for determining the frequency of the hazard outcomes. The following hazard outcomes shall be reviewed for estimating frequencies:

- Thermal radiation (jet / pool fires)
- Thermal dose (flash fire)
- Explosion overpressure (UVCE, BLEVE)
- Spill (un-ignited liquid release)