bp

Document No. GP 48-03
Applicability Group
Date 5 June 2008

GP 48-03

Layer of Protection Analysis (LOPA)

This Group Defined ETP has been approved by the GVP Safety and Operations for implementation across the BP Group.

BP GROUP
ENGINEERING TECHNICAL PRACTICES

Foreword

This revision of Engineering Technical Practice (ETP) GP 48-03 includes the following changes:

- Clarification of scope and applicability.
- Reference to the risk matrix contained in GDP 31-00-01, Assessment, prioritization and management of risk (issued 30 January 2008 as an implementation draft).
- Alignment of definitions with other internal and external standards.
- Alignment of the severity levels to GDP 31-00-01.
- Revision of the TMELs to the risk matrix in GDP 31-00-01.
- Requirements on vessel rupture and pipework loss of containment.
- Modifications to numerical values for PSVs and human factors.
- Greater guidance on LOPA supporting documentation and reporting.
- Greater definition on responsibilities for LOPA associated tasks.
- Revisions to the flowchart (slightly) and modified the following sections accordingly.
- Clarification on initiating causes.
- Greater clarification on independence of systems.
- Clarification on ignition probabilities.

Table of Contents

List of Tables

List of Figures

1. Scope

The scope and applicability of this GP are as follows.

a. This GP describes the method used to evaluate the effectiveness of independent protection layer(s) in reducing the likelihood or severity of an undesirable event.

b. It is applicable to Major Projects as defined by MPep (E&P) and Pep (R&M). This includes onshore and offshore hydrocarbon and chemical process facilities, excluding subsea facilities.

c. The LOPA method may be applied to other facilities such as subsea, drilling, marine, and alternative energy and will require review and adaptation of the numerical values contained in this GP or development of appropriate values.

d. If a SIF is involved and the demand frequency is less than the testing frequency, then the PFD determined from LOPA is not the appropriate method to define the required integrity.

Refer to GP 30-76 in such cases.

e. If consequences are in levels A or B of GDP 31-00-01, Appendices 1 or 2, LOPA is not an appropriate analysis method. Methods such as fault tree analysis, failure modes and effects analysis, or quantitative risk analysis should be applied in pursuit of risk reduction options.

f. If LOPA indicates requirement for SIL 3 or higher SIFs, other methods of hazard evaluation should be applied to better understand the risks and alternatives should be sought that include inherently safer design strategies and alternative risk management approaches.

The planned Group Recommended Operating Practice on Selection of hazard evaluation and risk assessment techniques will give further guidance on the appropriate techniques.

2. Normative references

The following referenced documents may, to the extent specified in subsequent clauses and normative annexes, be required for full compliance with this GP.

- For dated references, only the edition cited applies.
- For undated references, the latest edition of the referenced document (including any amendments) applies.

BP

GDP 31-00-01	Assessment, prioritization and management of risk.
GP 30-75	Safety Instrumented Systems (SIS) - Management of the Safety Lifecycle.
GP 30-76	Safety Instrumented Systems (SIS) - Development of Process Requirements Specification.
GP 30-80	Safety Instrumented Systems (SIS) - Implementation of the Process Requirements Specification.
GP 30-81	Safety Instrumented Systems (SIS) - Operations and Maintenance.
GP 48-50	Major Accident Risk (MAR) Process, Annex B.

3. Terms and definitions

For the purposes of this GP, the following terms and definitions apply.

Availability
Fraction of time that a safety system is able to perform designated safety service if required for use. Availability = 1 - Probability of failure on demand (PFD).

Basic process control system (BPCS)
A system that responds to input signals from the process and/or from an operator, and generates output signals, causing the process to operate in the desired manner. The BPCS consists of a combination of sensors, logic solvers, process controllers, and final control elements which automatically regulate the process within normal production limits. Includes a HMI (human machine interface). Also referred to as process control system.

Commercial integrity level (CIL)
Level for specifying commercial integrity requirements of commercial function allocated to safety instrumented systems (SIS).

Common cause failure
Failure of more than one device, function, or system due to the same cause.

Competent
Describes an individual with knowledge and skills deemed acceptable by the EA to perform a task. Appropriate knowledge and skill may be acquired through training, experience, qualifications, or some combination of these.

Demand
Condition or event that requires a protective system or device to take appropriate action to prevent or mitigate hazards.

Entity (BP entity or Operating entity)
Whilst these terms are not used in this GP they have a specific meaning in OMS. If this GP refers to BP Operation it should be interpreted as BP Entity or Operating Entity when working to OMS.

Environmental integrity level (EIL)
Level for specifying environmental integrity requirements of environmental function allocated to SIS.

Hazard
Condition or practice with the potential to cause harm to people, the environment, property, or BP's reputation.

Independent protection layer (IPL)
Device, system, or action that is capable of preventing 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 layer of protection analyses.

Initiating cause
A failure, error, situation, or condition that results, or may result, in the propagation of a hazardous event.

Initiating event

The minimum combination of failures (or errors) necessary to start the propagation of a hazardous event. It can be comprised of a single initiating cause, multiple causes, or initiating cause(s) in the presence of enabling conditions.

Integrity level (IL)

More general description than safety integrity level (SIL), referring to highest integrity level required for safety of onsite personnel, offsite personnel, environmental issues, and commercial issues. Follows same four levels as SIL.

Layer of protection analysis (LOPA)

Method for evaluating the effectiveness of protection layers in reducing the frequency and/or severity of hazardous events.

Probability of failure on demand (PFD)

The probability that a system will fail to perform a specified function on demand.

Protection layer

A device, system, or action that is capable of preventing a postulated accident sequence from proceeding to a defined, undesirable endpoint.

Reliability

The 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

A measure of loss/harm to people, the environment, compliance status, Group reputation, assets or business performance in terms of the product of the probability of an event occurring and the magnitude of its impact. Throughout this Practice the term "risk" is used to describe health, safety, security, environmental and operational (HSSE&O) undesired events.

Risk reduction factor (RRF)

Measurement of performance of SIF (RRF = 1/PFD).

Safety instrumented function (SIF)

Safety function with specified integrity level that is necessary to achieve functional safety by putting process to a safe state or maintaining it in a safe state under predefined conditions. SIF is implemented using SIS.

Safety instrumented system (SIS)

Instrumented system used to implement one or more SIF. SIS is composed of sensors, logic solvers, and final control elements. An emergency shutdown system (ESD) is a specific example of an SIS.

Safety integrity level (SIL)

Numerical representation of the integrity required, and capability of SIF. It addresses hardware reliability and capability to avoid systematic faults. SILs for SIFs operating in demand mode are defined for hardware reliability in terms of probability of failure on demand (PFD). (IEC 61511 and IEC 61508) See Table 15 for details of SIL levels.

Safety lifecycle

Necessary activities involved in the implementation of a SIF occurring during time period that starts at concept phase of project and ends when all SIFs are no longer required and facility is decommissioned.

Target mitigated event likelihood (TMEL)
Maximum frequency for specified severity of consequence.

Vulnerability
Probability that persons will suffer a specified health and safety impact level if exposed to hazard.

4. Symbols and abbreviations

For the purpose of this GP, the following symbols and abbreviations apply:

BPCS	Basic process control system.
CIL	Integrity level for equipment damage and business value lost.
EA	Engineering authority.
EIL	Environmental integrity level.
ESD	Emergency shutdown.
HAZOP	Hazard and operability (study).
IC	Initiating cause.
ICL	Initiating cause likelihood.
IEL	Intermediate event likelihood.
IL	Integrity level.
I/P	Current to pneumatic transducer.
IPL	Independent protection layer
LOPA	Layer of protection analysis.
P&ID	Process and instrumentation diagram.
PFD	Probability of failure on demand.
PHA	Process hazards analysis.
PSV	Pressure safety valve.
QRA	Quantitative risk analysis.
RRF	Risk reduction factor.
SIF	Safety instrumented function.
SIL	Safety integrity level.
SIS	Safety instrumented system.
SRS	Safety requirement specification.

TMEL Target mitigated event likelihood

5. LOPA overview

5.1. What is LOPA

a. LOPA is a method for evaluating the effectiveness of protection layers in reducing the frequency and/or consequence severity of hazardous events.

b. LOPA provides specific criteria and restrictions for evaluation of IPLs, reducing 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.

5.2. Protection layers

a. As shown in Figure 1, a scenario may have one or more protection layers of various types, depending on complexity of process and potential severity of consequence.

Protection layers, or safeguards, do not need to be independent from each other unless they are classified as IPLs.

b. LOPA provides a consistent basis for judging whether there are sufficient independent protection layers against hazardous events to achieve the required risk reduction target.

5.3. Independent protection layers

a. LOPA considers safeguards that meet IPL criteria.

LOPA considers only IPLs whereas a HAZOP may include safeguards that are not independent layers of protection.

b. IPLs shall conform to the following criteria:

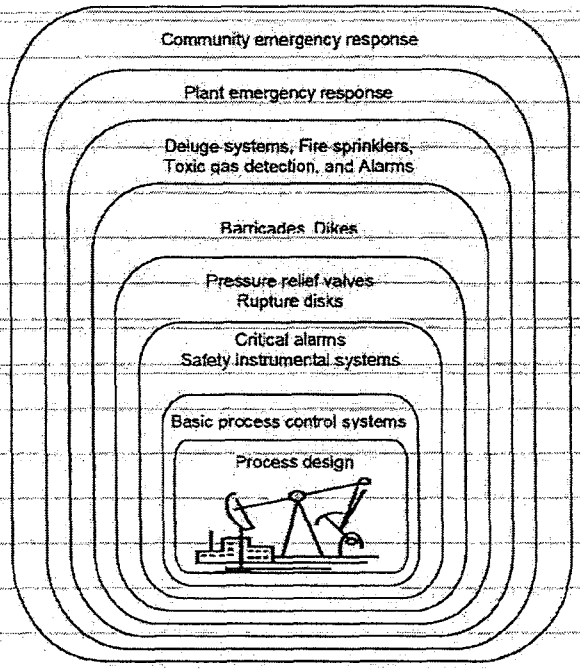
IPLs may be active or passive.

1. Specificity: IPL is designed to prevent a postulated accident sequence from proceeding to a defined, undesirable endpoint (e.g., runaway reaction, release of toxic material, loss of containment, or fire). Multiple initiating causes may lead to same hazardous event, and therefore, multiple event scenarios may initiate action of one IPL. If an event can be initiated by different initiating causes, different IPLs can apply to the different initiating causes.
2. Independence: IPL is independent of all other protection layers associated with identified potentially hazardous event. Independence requires that performance not be affected by failure of another protection layer or by conditions that caused another protection layer to fail. Protection layer are also independent of initiating cause.
3. Dependability: Protection provided by IPL reduces identified risk by known and specified amount.
4. Auditability: IPL is designed to enable periodic validation of protective function. Periodic testing and maintenance of IPL is required.

c. Instrumented IPLs shall have controlled access.

For example, set points on a high level alarm credited as an IPL should require review and approval prior to change.

Figure 1 - Example of protection layers



5.4. Advantages and limitations

Advantages and limitations of the LOPA process include the following.

a. LOPA advantages

1. LOPA is effective in resolving disagreements related to risk.
2. LOPA determines whether SIS or alternative means of protection are required and associated SIL if SIS is chosen.
3. LOPA conforms to industry standards.

   IEC 61511, clauses 8 and 9.
4. LOPA facilitates the analysis of protective layers addressing health and safety and environmental, and may also be applied to risks due to equipment damage and business value lost.

b. LOPA limitations

1. LOPA is not a method for identifying hazards.
2. LOPA may be excessive for simple or low risk decisions.
3. LOPA may be overly simplistic for complex systems.
4. LOPA is not a method to analyze escalation events.
5. LOPA is not a method to analyze risks associated with escape and evacuation.
6. Risk comparison scenarios are only valid if same LOPA method is used throughout.

5.5. Safety lifecycle

a. LOPA is part of safety lifecycle activities for independent protective layers, including SIS.

b. Refer to GP 30-75 and GP 30-76 for details of management of instrumented systems safety life cycle activities.

c. If credit is taken during a LOPA for an independent protection layer, there shall be associated maintenance, testing, and verification of that layer of protection at the performance level assumed in the LOPA study. The devices forming the IPL should be recorded in the BP Operations "register of protective devices" or list of "safety critical equipment".

d. Proposed changes identified from the LOPA process shall be formally reviewed using appropriate MoC procedures.

e. If the outcome of the LOPA demonstrates the need for a SIL rated SIF this shall be specified, installed, and maintained in conformance with GP 30-80 and 30-81 respectively.

5.6. LOPA timing and application

a. For operating facilities, the BP Operations EA shall be responsible for assuring the LOPA planning, conduct, documentation, and resolution of action items.

b. For projects, the Project EA shall be responsible for assuring the LOPA planning, conduct, documentation, and resolution of action items.

c. For operating facilities that have not conducted LOPAs, they shall be conducted either: in conjunction with HAZOP (and HAZOP revalidation) schedules, in conjunction with other risk management activities, or in a risk prioritized programme.

d. For operating facilities that have conducted LOPAs and for projects, when a HAZOP (or HAZOP revalidation) is preformed, a LOPA shall be performed either during or immediately after the HAZOP (and revalidation).

Refer to GP 48-02 for guidance on HAZOP.

Given efficiencies in coordinating process hazard analysis studies and LOPA studies, industry practice is to conduct a LOPA either immediately following or in conjunction with these process hazard analysis studies. This generally saves time because the LOPA team does not have to relearn scenario under consideration.

e. LOPA shall be performed for each hazard identified in a HAZOP that has corresponding severity level D to F in GDP 31-00-01, Appendices 1 or 2.

f. If the severity level is C in GDP 31-00-01, Appendices 1 or 2, LOPA shall be performed unless other techniques described in 5.6 h are used instead. In addition to LOPA, other techniques shall be considered where the risk reduction is provided by a single protection device eg check valve, relief valve. The techniques shall be subject to approval by the BP Operation EA.

At severity level C it is not appropriate to rely on a single system such as SIS and two independent physical methods provide higher protection.

g. LOPA may be performed for hazard scenarios that have severity levels G and H on the risk matrix described in GDP 31-00-01, Appendices 1 or 2.

h. If severity levels are A or B in GDP 31-00-01, Appendices 1 or 2, LOPA is not an appropriate method and a more rigorous analysis shall be used. Methods such as fault tree analysis, failure modes and effects analysis, or quantitative risk analysis should be applied. The proposed method shall be subject to approval by BP Operation EA.

6. LOPA study team

6.1. Team leader

a. The BP Operations EA or Project EA shall be responsible for endorsing the LOPA team leader and study team selection.

b. A LOPA team leader shall:

1. Be trained and experienced in application of the LOPA methodology. These skills can be gained through attendance at a BP or recognized industry LOPA training course.
2. Have a clear understanding of this GP and its requirements.
3. Be able to provide training to the team prior to the LOPA sessions.
4. Have an understanding of likelihood and potential consequences of events, including developing conditional probabilities of different outcomes.
5. Have an overview understanding of safety instrumented systems for the process industry sector including the equipment and design requirements for SIS.

   This industry approach is described in IEC 61511.
6. Have necessary leadership skills.
7. Before leading a LOPA, the leader shall have actively participated in a number of LOPA studies under the leadership of a competent LOPA Team Leader.

   It is advantageous for the LOPA Team Leader to have experience in other process hazards analysis or risk assessment techniques such as consequences analysis, reliability analysis, and QRA.

c. The LOPA team leader shall be responsible for:

1. Advising the BP Operations leader of issues that could affect the integrity of the study and working with them to ensure an effective resolution.
2. Being alert to time pressures and ensure that it does not compromise the quality, thoroughness, or integrity of the review.
3. Advising the BP Operations leader of the need to delay/ postpone the study until issues affecting the integrity of the LOPA can be resolved. This can include, but is not limited to the following:
   a) Inadequate experience/ expertise or make-up of the LOPA team for an effective review.
   b) Core LOPA team member roles as agreed in the TOR are not in attendance.
   c) Required process safety information is inaccurate or not available.

6.2. Other team members

a. The LOPA team leader shall select and appoint competent LOPA team members based on their experience of the type and scale of the LOPA being conducted.

b. LOPA shall be performed using a multidisciplinary team.

1. The core LOPA team shall include the following expertise:
   a) Understanding/experience with the process/facility design and process intent.

   This may be the process or facility engineer depending on the engineering contractor's practices and terminology. For chemical processes, this may be someone familiar with process chemistry.

b) Understanding/experience with instrument or controls - control and shutdown hardware and logic solvers.

c) Understanding/experience with day to day operations.

d) Understanding/experience with process safety.

2. Other technical expertise should include, as warranted:

a) Scribe

The Scribe role may be filled by one of the team members or the team leader

b) Understanding/experience with equipment, design limits, materials of construction, and condition of equipment.

c) Corrosion and materials.

d) Maintenance.

e) Mechanical.

f) Technical representative for licensed technologies and/or vendor package.

g) Other disciplines as required.

c. Number of full time members should be between three (in addition to the facilitator and scribe) and six to enable effective analysis and decision taking.

7. LOPA documentation

7.1. Terms of reference (TOR)

a. A TOR shall be developed for each study and formally agreed between the BP Operations Leader or delegate and the LOPA Study Leader before the study commences.

b. The TOR document shall include objectives, scope, methodology including parameters and deviations to be used, personnel required to attend the meeting, schedule and deliverables, principal report recipient, distribution list, and reference documents (e.g., HAZOP, P&IDs).

c. The TOR should also identify and be forwarded to the BP Operation EA or Project EA responsible for the hazard and risk management at that facility or on that project.

Developing the TOR helps ensure a consistent understanding of the LOPA method and its application will be established between LOPA Leader, project/ site management, and the LOPA team.

7.2. Supporting documents

a. Key documents that shall be available during LOPA are:

1. Clear and complete definition of hazard scenarios, their consequence, and layers of protection (i.e., safeguards).

HAZOP worksheets in conformance with GP 48-02 provide this information.

2. Clear and complete definition of instrumented system loops and their interrelationships, and the cause and effects of the instrumented functions.

3. P&IDs.

4. SIL ratings that have been previously determined for existing SISs

b. Key documents that should be available during LOPA are:

1. SRS for existing SIS.

2. Cause and effect chart.
3. PSV design data.
4. Vessel design data.
5. Operating procedures.
6. Consequence analysis studies.

7.3. LOPA study report

a. The LOPA leader shall be responsible for issuing the formal LOPA report to the principal recipient of the study defined in the TOR.

The LOPA report serves as the permanent record of the LOPA study and will be used by people that were not a part of the LOPA team. Over time, the LOPA report is the only indicator of the quality and completeness of the LOPA study, and serves as a record of the team's diligence. It is important that the LOPA Team Leader and team have the attention to detail to ensure clarity and accuracy of the log sheets and report.

b. Documents used to support the study documents shall be collected and archived for future reference. The responsibility for doing this rests with:

1. The project team who should hand over study documents to client or asset, or
2. The person in an existing asset who coordinates LOPA documentation.

c. LOPA documentation shall be retained for the life of the facility. This report should be prepared and filed in accordance with local document control procedures.

Retention of LOPA documentation ensures its availability for reference in MOC and revalidation.

d. A LOPA report shall include following:

1. Main report
   a) Principal recipient of the report.
   b) Executive summary.
   c) Scope of study.
   d) Process or system description and design intent.
   e) Verification that LOPA method described in this GP was used.
   f) Identification of numerical values used, and their sources.
   g) LOPA Team members and their roles.
   h) Recommendation summary.
   i) References (list of P&IDs and other data used).
   j) Distribution list.
2. Appendices
   a) ToR for the LOPA study.
   b) Assumptions.
   c) LOPA Log sheets.
   d) List of recommendations from the study.
   e) Team attendance for each session.

f) Information that was referenced in the logsheets or used extensively by the team.

This can include calculations, detailed consequence analyses, or other useful information compiled for or during the LOPA that would be useful reference material for future MoC or safety issues.

7.4. Follow-up

a. BP Operations EA or Project EA should ensure that an effective means of tracking recommendations is in place and accomplishes the following:

1. Track the status of open action items.
2. Record the action item closure and approval by project or site authority (Approved action response sheets should be retained with the log sheets).
3. Include or reference documentation requirements.
4. Track the transfer of action items between delivery teams (e.g., project to commissioning).

To facilitate future reviews and the use of material for training purposes, it is useful if the logsheets are updated to include the actual actions taken when the recommendations are closed out.

5. Provide for a confirmation of completion including by field-verification for operating facilities.

b. The technical reasons for recommendation resolution, including suggestion of a different action, or rejection, shall be clearly stated in writing and retained.

c. If recommendation and actions cannot be agreed with the project or BP Operation to the satisfaction of the LOPA team leader then the Project EA or BP Operations EA shall be informed. The EA shall attempt to get resolution with the Project Manager or BP Operation leader but if this is not possible the EA shall raise the issue to a higher EA until agreement is reached with the BP Operation leader.

d. For projects, the Project manager shall ensure that agreed recommendations are resolved in an appropriate timescale as dictated by project schedule.

The PHSSER teams review and audit action progress at various stages of CVP in accordance with GP 48-01.

Completion of recommendations should also consider the amount of work involved in completing the tasks. Administrative and documentation recommendations should be completed in a reasonably short period while recommendations requiring extensive engineering and installation during unit downtime may require years to complete.

e. BP Operations leader shall ensure that agreed actions are followed through to an appropriate conclusion. A person should be nominated to do this and instructed to report formally at regular intervals while the action remains outstanding.

f. For projects and operating facilities, complete auditable responses and actions concerning the recommendations shall be documented and retained for the life of the operating facilities.

Report recommendations, BP Operations responses, and supporting documentation should ideally be recorded in a records system, which permits ready retrieval, status reporting, progress chasing, and independent audit. The supporting documentation should include appropriate reports, memos, drawings, and other communications demonstrating that the recommendations arising from the LOPA have been carried out or otherwise resolved.

g. Relevant recommendations and actions from LOPA reports and related study documents shall be communicated to members of the BP workforce who may be affected by them.

Local law may impose additional communication requirements, including a requirement to make the risk assessment accessible to persons who work with or near the studied risk.

h. For operating facilities, site MOC process shall be followed for approved changes resulting from LOPA recommendations.

MOC ensures that employees are advised on changes to procedures and/or equipment and any relevant training provided at the time of change. It also guards against the resolution of the recommendation inadvertently introducing a new risk.

8. LOPA method steps

The LOPA method shall follow the steps in Figure 2:

a. Identify hazardous scenarios that result in consequence levels requiring a LOPA. The following information should be obtained from the HAZOP:

1. Scenario description (including consequence description).
2. Consequence ranking.
3. List of initiating causes.
4. List of safeguards for consideration as IPLs.

Preloading the HAZOP scenario data into the LOPA documentation tool prior to start of the LOPA team meeting provides a more efficient approach.

b. Identify initiating causes of the hazardous scenario and determine the initiating cause frequency of failure based on Table 1 for equipment and Table 2 and Table 3 for human error. Frequency modifiers described in 9.4 are also considered in determining scenario likelihoods.

c. Determine or verify the consequence level of the initiating causes hazardous consequences in terms of health and safety and environmental, and optionally, in terms of equipment damage and business value Determine the TMEL for the hazardous scenario using Tables 6, Table 7, and Table 8.

d. Decide if the initiating event frequency is less than or equal to the TMEL. If it is, proceed to the next scenario. If not, proceed to the next step.

e. List the IPLs (existing and future) that can mitigate the initiating causes. Assess the type and integrity of the IPL.

f. Decide if the IEL is less than or equal to the TMEL. If it is, proceed to the next scenario. If not, proceed to the next step.

g. Evaluate whether there is an inherently safer design option. If there is, recommend it. If not, proceed to the next step.

Refer to GP 48-04 on inherently safer design.

The use of a SIS should not be the first choice in protection as it may not be the most inherently safer option.

h. Identify any existing SISs.

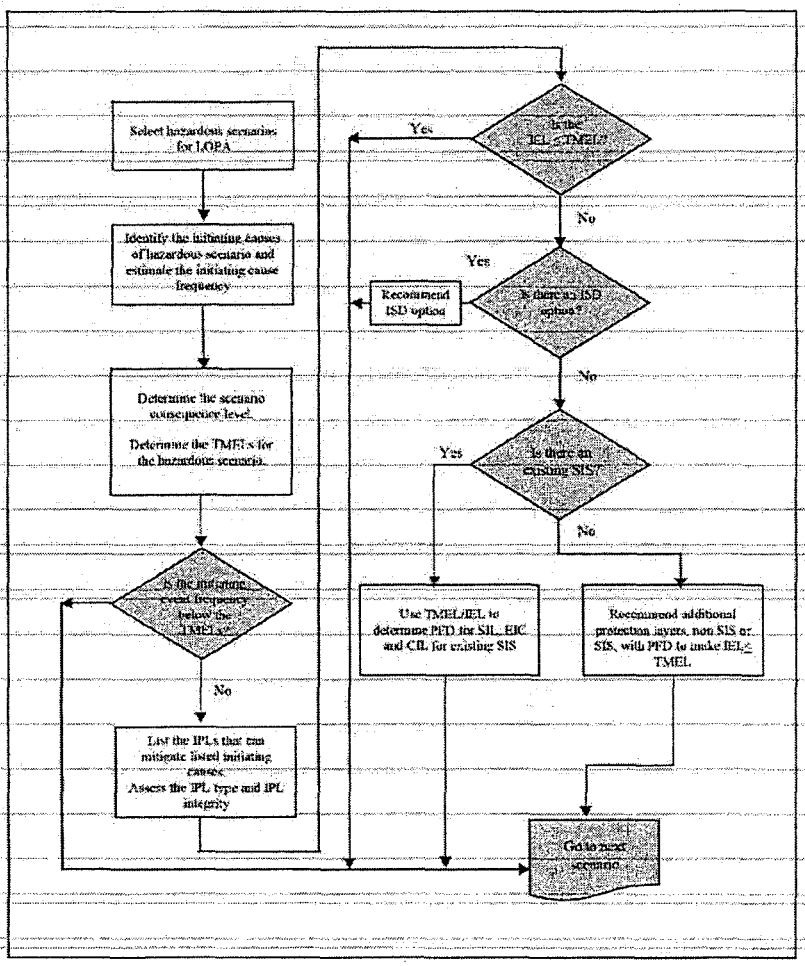
i. For any existing SISs, if the SIS lifecycle has been managed and documented in accordance with GP 30-75, GP 30-76, GP 30-80 such that the actual PFD can be determined (or probability of ineffectiveness for non SIS layers) then this PFD should

be used. The PFD should be used for the SIL, EIL, and optionally CIL for the SIS. Refer to Table 11, Table 12, and Table 13.

2. If there are not any existing SISs, recommend additional protection layers, non SIS or SIS, with PFD to make the IEL ≤ TMEL.

i. Proceed to the next scenario until analysis of all scenarios is completed.

Figure 2 - LOPA process



9. Initiating causes, likelihood, and frequency modifiers

9.1. General

a. Initiating causes of hazardous scenarios normally identified in HAZOPs generally fall into two categories:

1. Equipment and BPCS failure

BPCS is often historically referred to as DCS or instrumented control system.

a) Equipment related initiating events can either be due to failure of basic process control system or mechanical failure.

Pump failure is an initiating cause for LOPA that covers mechanical and electrical issue related to impeller or the pump, and the electrical system.

b) Control system events may be caused due to component failures (e.g., transmitters, switches, valves), software faults, human intervention, or utility failures (electricity or instrument air).

c) Mechanical failures could be due to any number of reasons, including corrosion, fatigue, improper design, vibration, and hydraulic hammer.

Design errors should not be addressed with LOPA. IPLs should not be used to correct process conditions caused by design errors.

Corrosion caused by failure of inhibitor injection system or by abnormal corrosive conditions caused by other process control failures can be valid LOPA initiating events. However, general corrosion is not a LOPA initiating cause. It is an integrity management and maintenance issue.

2. Human error events are classified as errors of omission or errors of commission, including:

a) Failure to properly execute steps of task in proper sequence or omitting steps, e.g., valve misalignment.

b) Failure to observe or respond appropriately to conditions or other prompts by system or process (something done wrongly).

9.2. Likelihood of initiating cause

a. Initiating cause likelihood values shall be taken from the lookup tables provided as Table 1, Table 2, and Table 3 or permission to use alternate values shall be obtained from the BP Operations EA.

Values in Table 1 and Table 2 are consistent with values suggested in "Layer of Protection Analysis" published by CCPS of AIChE.

Values provided in Table 1 are based on "average" process conditions (i.e., clean service, well maintained equipment, available auxiliary systems).

b. If the action is more frequent than once per month, Table 2 shows the suggested base human error rate that can be used for the estimation of human error frequency.

c. If the action is less frequent than once per month, then the frequency of human error likelihood can be estimated based on the human error rate and the number of operations per year using Table 3.

Table 1 - Equipment initiating causes and likelihood of failure

Initiating cause (IC)	Likelihood of failure (events/yr)
BPCS instrument loop failure	1×10^{-1}
Regulator failure	1×10^{-1}
Fixed equipment failure (e.g., exchanger tube failure)	1×10^{-2}
Pumps and other rotating equipment	1×10^{-1}
Cooling water failure (e.g., redundant cold water pumps, diverse drivers)	1×10^{-2}
Loss of power (e.g., redundant power supplies)	1×10^{-1}
Safety valve opens spuriously (PSV)	1×10^{-2}
Pump seal failure	1×10^{-1}
Unloading/loading hose failure	1×10^{-1}

Table 2 - Human error frequency for actions taken at least once per month

Conditions	Likelihood of error
Operator well trained with stress	1/yr
Operator well trained with no stress	1×10^{-1}/yr
Operator well trained with no stress, and with independent verification	1×10^{-2}/yr

Table 3 - Base human error rate

Conditions	Probability of error
Operator well trained with stress	1×10^{-1}/opportunity
Operator well trained with no stress	1×10^{-2}/opportunity
Operator well trained with no stress, and with independent verification	1×10^{-3}/opportunity

Sources of failure rate data for initiating event frequencies include the following:

- *CCPS Guidelines, 1989.*
- *CCPS Concept Book, 2001.*
- *IEEE, 1996.*
- *IIT Research, 1987.*
- *ISA TR 84.00.02.*
- *OREDA 1984, 1992, 1997, and 2002.*
- *Reliability, Maintainability and Risk (Smith).*
- *Proprietary data base that BP collected from many sources.*

9.3. Multiple causes

For multiple initiating causes of the same hazardous scenario, initiating cause likelihood values shall be handled by either addressing:

a. Each IC separately with its protection layers and evaluating the total IEL for the hazardous scenario, or,

b. A single initiating cause value if summing the initiating causes will not mathematically impact the outcome.

In the strict application of the LOPA method, initiating cause likelihoods that lead to the same consequence and can be mitigated by the same IPLs, should be added as they all refer to a single scenario. However, in many cases, there are 1-3 initiating causes and the difference between using a single initiating cause likelihood and adding 3 together does not impact the outcome. The LOPA facilitator should be able to analyze this and decide if there is value gained in the exercise of identifying and adding initiating cause likelihoods.

9.4. Frequency modifier

9.4.1. General

a. While considering the initiating event likelihood, the LOPA team may consider the potential frequency modifiers: time at risk, occupancy factor, and ignition probability.

Caution should be used when applying frequency modifiers. If incorrectly estimated, and applied in determining event likelihood, the risk may be underestimated.

If these frequency modifiers are not used a conservative modifier of 1 is effectively applied.

b. Some initiating events might be given in terms of likelihood per action. In this case, the team needs to consider how often this action takes place in 1 year.

9.4.2. Time at risk factor

a. For systems that are not continuously operated (loading/unloading, batch process, etc.) the initiating cause likelihood is adjusted to reflect the fraction of time the hazard is present.

b. Time at risk factor can be determined by dividing the time that the process is in the hazardous mode of operation by total time (1 calendar yr).

c. The following equation shows how time at risk factor can be used to modify ICL:

$$ICL\ (modified) = ICL \times P_t$$

Where: –

ICL = initiating cause likelihood.

P_t = time at risk/total time.

d. Factor P_t is only valid if a failure that would cause demand outside of the operational time is detected and repaired outside the operational time (before the operational time begins).

e. Time at risk shall not be used for startup scenarios. Startup activities do not include non continuous operations described in 9.4.2.a.

9.4.3. Occupancy factor

a. To be a health and safety hazard scenario, personnel need to be in an area that could be impacted by the hazard. Credit should be taken for time that personnel are not in the area if the hazard may result in health and safety impacts.

For example, if a pump seal fire were to occur and cause a safety hazard, an operator would have to be present, say during his normal operator rounds. The Operator may only be near pump for 30 min of a shift. In this case, presence factor is 0.5 hr/12 hr = 0.04, and likelihood of event would be modified by multiplying it by this presence factor to obtain the modified frequency.

b. The following equation shows how occupancy factor can be used to modify ICL:

$$ICL\ (modified) = ICL \times P_p$$

Where:

ICL = initiating cause likelihood.

P_p = occupancy factor = time present to hazard/total time.

c. Factor P_p is only valid if a person's presence is random with respect to the hazard causes. If hazard only occurs at start-up and persons are always present at startup, then the occupancy factor is 1.

Operator response should be considered for occupancy if a proposed event is not considered an instantaneous incident. If operator response can be expected, no credit for occupancy factor should be taken.

If an alarm is considered as an IPL, then occupancy factor should be applied cautiously as the alarm may draw the operator into the area.

d. Occupancy factor is not used for environmental and commercial scenarios.

9.4.4. Ignition probability

a. The ignition probability shall relate to the hazardous scenario being analyzed as described below.

1. Onshore facilities

a) If the scenario involves an immediate ignition, then the ignition probability shall be 0.1 unless the scenario involves a high energy mechanical impact when the ignition probability shall be 0.3.

b) If the scenario involves a delayed ignition, then the ignition probability shall be 0.5 where the vapour cloud encounters on site ignition sources. Where the vapour cloud extends off site then the ignition probability shall be 0.9. Where it can be demonstrated that a particular scenario will not generate a large flammable vapour cloud then the immediate ignition probabilities should be used.

In general, the probability of delayed ignition if the cloud drifts into areas of uncontrolled ignition sources, such as residential areas, will be greater than that where ignition sources are controlled, for example, on oil or chemical sites. Some materials in given ambient conditions and depending on the nature of the release will not form large flammable vapour clouds.

c) Where the temperature of a released material is above its autoignition temperature , then the ignition probability shall be 1.0.

These values were selected by reviewing the ignition probabilities in GP 48-50 and selecting the most appropriate value for each case.

2. Offshore facilities shall use ignition probability data provided in Table 4 and Table 5.

3. Permission to use numerically lower ignition probability values shall be obtained from the BP Operations EA and shall be justified based on relevant data.

Table 4 - Generic ignition probabilities for offshore facilities

Fluid	Situation	Release rate kg/s	Nominal Ignition Probability
Gas/Condensate	Confined	>50	0,5
		1 to 50	0,15
		<1	0,05
	Semi confined	>50	0,3
		1 to 50	0,05
		<1	0,01
	Open	>50	0,2
		1 to 50	0,03
		<1	0,002 5
Oil	Confined	>50	0,15
		1 to 50	0,08
		<1	0,05
	Semi-confined	>50	0,08
		1 to 50	0,05
		<1	0,03
	Open	>50	0,05
		1 to 50	0,025
		<1	0,01

These values are based on the report referenced in GP 48-50 for offshore, IP Research Report, Ignition Probability Review, Model Development and Look-up Correlations, Table 1.9.

Table 5 - Method for assigning offshore ignition timings

Situation	Relative probability of ignition	
	Immediate	Delayed
Congested plus hot work	0,7	0,3
Congested - no hot work	0,35	0,65
Non-congested plus hot work	0,5	0,5
Non-congested - no hot work	0,35	0,65

These values are based on the report referenced in GP 48-50 for offshore, IP Research Report, Ignition Probability Review, Model Development and Look-up Correlations, Table 1.10.

9.5. Target mitigated event likelihood

a. The risk matrix that shall be used during LOPA studies is provided in GDP 51-00-01 Appendices 1, 2 and 3.

b. During the LOPA analysis, the team shall identify the mitigated event likelihood for health and safety and environmental risks for each scenario.

c. During the LOPA analysis, the team may identify the mitigated event likelihood for risks of equipment damage and business value lost.

d. The TMELs shall be obtained from Table 6, Table 7, and Table 8.

e. The TMEL for risks of equipment damage and business value lost is one order of magnitude higher than that of other risk categories reflecting the BP emphasis on considering health and safety and environmental risks first.

The use of TMELs does not imply that BP accepts or tolerates risks at the level of any given TMEL. LOPA is applied in the context of continuous risk reduction.

Table 6 - TMEL for health and safety hazards

Severity level	Health and Safety Consequences	TMEL
A	Comparable to the most catastrophic health/ safety incidents ever seen in industry. The potential for 200 or more fatalities (or onset of life threatening health effects) shall always be classified at this level.	--
B	Catastrophic health/ safety incident causing very widespread fatalities within or outside a facility. The potential for 50 or more fatalities (or onset of life threatening health effects) shall always be classified at this level.	--
C	Catastrophic health/ safety incident causing widespread fatalities within or outside a facility. The potential for 10 or more fatalities (or onset of life threatening health effects) shall always be classified at this level.	1×10^{-6}/yr
D	Very major health/ safety incident * The potential for 3 or more fatalities (or onset of life threatening health effects) shall always be classified at this level. * 30 or more injuries or health effects to BP workforce, either permanent or requiring hospital treatment for more than 24 hr.	1×10^{-5}/yr
E	Major health/safety incident * 1 or 2 fatalities, acute or chronic, actual or alleged. * 10 or more injuries or health effects to BP workforce, either permanent or requiring hospital treatment for more than 24 hr.	1×10^{-4}/yr
F	High impact health/ safety incident * Permanent partial disability(ies) * Several non-permanent injuries or health impacts. * DAFWC	1×10^{-3}/yr
G (optional)	Medium impact health/ safety incident * Single or multiple recordable injury or health effects from common source/event.	1×10^{-2}/yr
H (optional)	Low impact health/ safety incident * First aid * Single or multiple over-exposures causing noticeable irritation but no actual health effects	1×10^{-1}/yr

Table 7 - TMEL for environmental hazards

Severity level	Environmental consequence (1)	TMEL
A	* Future event, e.g., unintended release, with widespread damage to any environment and which remains in an "unsatisfactory" state for a period > 5 yr.	
	* Future event with extensive damage to a sensitive environment and which remains in an "unsatisfactory" state for a period > 5 yr.	- -
	* Future event with widespread damage to a sensitive environment and which can only be remediated to a "satisfactory" / agreed state in a period of 2 yr to 4 yr.	
B	* Future event with extensive damage to a non-sensitive environment and which remains in an "unsatisfactory" state for a period > 5 yr.	
	* Future event with extensive damage to a sensitive environment and which can only be remediated to a "satisfactory" / agreed state in a period of 2 yr to 4 yr.	
	* Future event with widespread damage to a non-sensitive environment and which can only be remediated to a "satisfactory" / agreed state in a period of 2 yr to 4 yr.	- -
	* Future event with widespread damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of @ 1 yr.	
C	* Future event with extensive damage to a non-sensitive environment and which can only be remediated to a "satisfactory" / agreed state in a period of 2 yr to 4 yr.	
	* Future event with widespread damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of @ 1 yr.	1×10^{-4}/yr
	* Future event with extensive damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of @ 1 yr.	
	* Future event with widespread damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of months.	
D	* Future event with extensive damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of @ 1 yr.	1×10^{-5}/yr
	* Future event with localized damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of @ 1 yr.	
	* Future event with widespread damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of months.	
	* Future event with extensive damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of months.	
E	* Future event with localized damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of @ 1 yr	1×10^{-6}/yr
	* Future event with extensive damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of months.	
	* Future event with localized damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of months.	
	* Future event with extensive damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of days or weeks.	
F	* Future event with localized damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of months.	1×10^{-7}/yr
	* Future event with immediate area damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of months.	
	* Future event with extensive damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of days or weeks.	
	* Future event with localized damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of days or weeks.	
G (optional)	* Future event with immediate area damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of months.	1×10^{-8}/yr
	* Future event with localized damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of days or weeks.	
	* Future event with immediate area damage to a sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of days or weeks.	
H (optional)	* Future event with immediate area damage to a non-sensitive environment and which can be remediated to a level which restores its environmental amenity in a period of days or weeks.	1×10^{-9}/yr

Table 8 - TMEL for equipment damage and business value lost hazards

Severity level	Consequence in terms of equipment damage and business value lost	TMEL
A	Greater than $10 billion	--
B	$5 billion to $10 billion	--
C	$0,5 billion to $5 billion	1 x 10^{-5}/yr
D	$100 m to $0,5 billion	1 x 10^{-4}/yr
E	$5 m to $100 m	1 x 10^{-3}/yr
F	$500 k to $5 m	1 x 10^{-2}/yr
G (optional)	$50 k to $500 k	1 x 10^{-1}/yr
H (optional)	<$50 k	1/yr

10. Estimating consequences

10.1. General

a. Health and safety and environmental consequences shall be assessed.

Consequence of potential hazards can be obtained from the HAZOP worksheets.

Care should be taken when assessing the consequences. Underestimating can lead to insufficient layers of protection being applied and risk being insufficiently managed. Overestimating can lead to more layers of protection being applied than are warranted for the risk level which, over the lifecycle of the operation, will result in additional cost, inspection, and maintenance requirements.

b. Equipment damage and business value lost consequences may be assessed.

c. If the consequences are not clearly identified, further analysis shall be completed before LOPA can proceed.

d. If the consequences are identified, but not fully defined, the LOPA team may complete the definition or seek assistance from process safety and risk specialists to estimate the consequences.

This could include estimate of flammable cloud extent or explosion overpressure distance.

e. If the LOPA team feels that the HAZOP has underestimated or overestimated the consequences, the LOPA team should consult with:

1. HAZOP team representatives to understand their rationale.
2. Process Safety Engineering professionals to better understand potential consequences.

The consequence severity level utilised in the LOPA should be seen as the case with a reasonable probability of occurrence and not specifically the worst case scenario. The consequence severity level should include the vulnerability.

f. The LOPA team should consider previous consequence analyses and aspects of the scenario to estimate possible outcomes such as potential fire or explosion, including:

1. Release: size, material, operating pressure and temperature.
2. Ambient conditions.
3. Locations of persons, both onsite and offsite.
4. Escalation potential.

g. Costs associated with environmental impacts including cleanup, outage, and legal support for environmental risks should be considered under equipment damage and business value lost impacts.

h. The LOPA team should include the following when considering equipment damage and business value lost impacts:

1. Replacement and repair costs.
2. Cost of lost or deferred production during replacement and repair.
3. Costs of penalties for non delivery of contracted production.
4. Environmental cleanup costs.
5. Legal costs.

i. To support an efficient LOPA, it is recommended to develop a rule set for equipment damage and business value lost impacts specific to the facility being evaluated before the LOPA begins.

Such rules may include the cost of lost or deferred production per event plus per hour or day.

10.2. Vulnerability factor

a. Vulnerability shall not be used in the LOPA calculation.

b. The consequence severity level in 10.1.a, c, d, e, and f above shall include the vulnerability.

10.3. Consequences of loss of containment from vessels and associated pipework

a. Potential consequences considered for over pressuring of pressure vessels beyond their rated design pressure are provided in Table 9.

b. Table 9 may be used only if the current vessel design pressure is known, inspection/testing has confirmed vessel integrity, and this documentation is included in the LOPA report. If these conditions cannot be met then Table 9 shall not be used and instead either:

1. Vessel rupture shall be assumed or
2. Pressure vessel TA should determine the consequences based on a review of the tolerance of the vessel to over-pressure given the circumstances which apply.

The probability is based on the assumption that the vessel is well maintained and the current condition meets the design intent.

A full list of modes of failure and material damage mechanisms is given in section 5 BS 7910.

In Table 9, the sole failure mode which needs to be considered is plastic collapse. Fatigue cracking, for example, would be detected in inspection and need not be taken into account. It is very important that fatigue cracking, which is the main source of pressure vessel failure, is not present, and that the quality of manufacture is as stated in the original specification.

c. If the actual thickness of the vessel components is considerably larger than the thickness required to contain the design pressure, the factors given in Table 9 may be conservative. A pressure vessel TA may determine the consequences based on a review the tolerance of the vessel to over-pressure given the circumstances which apply.

d. Consideration should be given to the failure of devices and instruments attached to the vessel, e.g., sight glasses.

Table 9 - Vessel over pressure and associated pipework probable consequence

Multiple of over pressure	Probability of vessel failure	Probability of gasket leakage seals, etc.	Most likely consequence
1-,0 1,5 x the design pressure	0	0	Potential for gasket leakage, likely no permanent damage to vessel
1,5- 2,0 x design pressure	0	0,5	Gasket Leakage is likely. There is potential of permanent vessel deformation.
2,0- 2,5 x design pressure	0,001	1	Gasket Leakage is very likely and very likely to result in permanent vessel deformation
2,5-3,0 x design pressure	0,01	1	Gasket Leakage and vessel deformation leading to vessel leakage
3,0-3,5 x design pressure	0,1	1	1/10 chance of vessel failure (ductile failure, not catastrophic brittle failure)
3,5 and higher x design pressure	1,0	1	Likely bursting of vessel

11. Independent protection layers

11.1. General

a. There are two types of IPLs:

1. Passive IPL
   a) Dike/bund.
   b) Open vent.
   c) Blast wall/bunker.
   d) Flame/detonation arrestors.
   e) Restriction orifice.
2. Active IPL
   a) BPCS.
   b) Human response to alarm.
   c) Pressure relief device.
   d) SIS.
   e) Other design specific IPLs (e.g., mechanical stop for a valve).

b. The LOPA team should review safeguards from the HAZOP and identify those that meet the criteria for an IPL. Many safeguards identified in the HAZOP will not meet the criteria specified for IPLs in a LOPA analysis.

c. Assessment of IPLs shall be performed to determine amount of risk reduction provided by each, its dependability, and its independence from other IPLs.

d. Protection layers shall be assessed to verify that they meet the four criteria described in 5.3.b: specificity, independence, dependability, and auditability.

e. IPLs credited for startup scenarios shall be verified to be functional (not bypassed or disabled) during startup.

The process hazards during startup are likely to be mitigated by IPLs (including SIS) for normal operations. During startup there may be other transient (non-steady state operation) conditions that are not addressed by the normal operation IPLs.

f. Table 10 - lists examples of safeguards that are not considered as IPLs.

Table 10 – Examples of safeguards not considered IPLs

Safeguards not usually considered IPLs	Comments
Training and certification	Factors that may be considered in assessing PFD for operator action but are not IPLs.
Design to code and standard	Forms basis for deciding if, for example, loss of containment is credible but are not IPLs.
Procedures	Factors that may be considered in assessing PFD for operator action but are not IPLs.
Normal testing and inspection	Activities assumed to be in place for all hazard evaluations and form basis for judgment to determine IPLs and PFDs. Normal testing and inspection affects PFD of certain IPLs. Lengthening testing and inspection intervals may increase PFD of IPL.
Maintenance	Activity assumed to be in place for all hazard evaluations and forms basis for judgment to determine IPLs and PFDs in Table 6 and Table 8. Maintenance affects PFD of certain IPLs.
Communications	Basic assumption is that adequate communications exist in a facility. Poor communications affect PFD of certain IPLs.
Signs	Signs are not IPLs. Signs may be unclear, obscured, or ignored. Signs may affect PFD of certain IPLs.
Fire protection	Active fire protection is not often considered an IPL, as it is post event for most scenarios, and its availability and effectiveness may be affected by fire/explosion that it is intended to contain. (1) However, if company can demonstrate that active fire protection meets IPL for given scenario it may be used (e.g., if activating system, such as plastic piping of frangible switches, are used). Fireproof insulation can be used as IPL for some scenarios if it meets API and corporate standards. Note: Fire protection is mitigation IPL, as it attempts to prevent larger consequence subsequent to event that has already occurred.
Older process control systems	Pneumatic or hydraulic shutdown systems for which IL ratings can not be determined because the PFDs of the existing components are not available

11.2. Mechanical pressure relief devices - relief valves

The following rules shall apply to use of pressure relief valves as IPLs.

a. Pressure relief systems are sized to completely mitigate scenario under consideration.

Guidance on sizing is provided in GP 44-70 and GP 44-80.

b. If relief discharge can result in toxic, flammable, or environmental release, then this secondary scenario is evaluated in LOPA as initiating event.

c. Maintenance and testing procedures are developed and followed to ensure that relief valves are in satisfactory operating condition.

11.3. Check valves

a. Check valves may be used as a layer of protection only if leakage is tolerable.

API RP 521 describes potential leakage flow rates.

b. When a check valve is used as a layer of protection it shall be:

1. Used in a clean service.

2. Used in a non-vibrating, non-pulsating service.

3. Maintained and tested, to a defined performance standard and frequency.
4. Considered a safety critical device, and listed on the register of safety critical equipment.
5. Endorsed by the BP Operations EA or BP Projects EA for use as a layer of protection based on the points listed above.

c. The PFD for a check valve shall be 1×10^{-1}.

This PFD value includes an additional safety factor of 10 above that stated in bibliography reference Smith, 1985.

d. Use of a lower PFD value to that stated in c shall be subject to approval by the BP Operations EA for all check valve configurations.

11.4. BPCS

a. The following rules shall apply to basic process control systems (BPCS) that have been identified as IPLs.

1. Typically, the IPL credit for a BPCS control loop is taken as 0.1
2. Credit can be taken for a two semi-independent layers of protection (e.g., initiating event, alarm, second control loop) in a BPCS loop using the following rules.
   a) The LOPA team shall justify the PFDs for each element based on actual site testing records.
   b) If the common element between two semi-independent layers of protection has a PFD that is at least one order of magnitude less than the PFD for the loop, a PFD for one IPL is taken as 0.1 and for the second IPL is taken as 0.3.
   c) If the common element between two semi-independent layers of protection has a PFD that is at least one order of magnitude greater than the PFD for the loop, then a PFD for one IPL is taken as 0.1 and for the second IPL is taken as 1.0.

Independence between protection layers is a necessary principle for the math in LOPA to be correct. Practically, however, the failure rate for the processor is much lower than for an I/O card and for field sensors and final elements. If the processor is the only common element between a BPCS loop and an alarm, taking credit for both as though they were truly independent is only slightly optimistic mathematically.

The partial credit on semi-independent BPCS is dependent on the relative values of the PFD loops and components. These values vary depending on the manufacturer and type. It is not easy to determine these values for each scenario during the LOPA. Typically the PFD of the loop is calculated during SIL verification (not during LOPA) based on testing intervals.

3. Credit shall not be taken for more than two semi-independent IPLs.
4. Failure mode of final element is to safe state for the specific scenario.
5. If the control valve is used for final actuation of the SIF, the solenoid valve is located between the I/P converter and the actuator, and no bypass around the control valve is installed.
6. Operations is trained that the BPCS loop is a protective function (e.g., clarify that the loop should not be put in manual control).
7. If a tight shut-off is required, the BPCS valve meets this criteria and is tested and maintained.

b. BPCS credit as IPL should be minimized because the BPCS is subject to the same requirements as any other IPL (i.e., periodic testing, controlled access, availability, etc.).

Because of the access control requirement, the operators cannot be allowed to change the set points for the control loops or alarms that are credited as IPLs. This limitation may impact the operator flexibility to control the process. The control loop needs to be periodically tested and documented to meet the availability and reliability requirements.

11.5. Operator response to alarm

a. Operator response to alarms counted as single protection layer shall meet the following conditions.

1. Alarm is independent of cause and is independent of any BPCS control loop claimed as an IPL. BPCS control loop claimed as an IPL and alarm that share the same input card or processor are not independent.
2. Operator is always present and available at alarm point (e.g., control room is continuously staffed).
3. Alarm is allocated a high priority and gives clear indication of hazard.
4. Operator detects alarm among potentially many other alarms.
5. Operator is trained in proper response and operations procedures associated with alarm state and has time to take corrective action prior to the event.

b. If several independent human errors are required (i.e., as in the case when a scenario progresses slowly and operators from two or more shifts commit the same mistake) then the PFD can be reduced one order of magnitude.

c. Alarm set point and priority, corrective response, and time available to diagnose and correct hazard should be documented in LOPA.

d. An MOC and review of associated risks shall be required to modify alarm set points.

11.6. SIS

a. An SIS may be used to reduce the likelihood of a hazardous event.

Safety instrumented systems should be considered after more inherently safer approaches have been identified and considered.

b. SISs should be allocated a SIL in relation to the credit given for risk reduction. The following conditions shall be met:

1. SIS is separate and independent from the cause of demand.
2. SIS is separate and independent from any other SIS that is used to reduce the intermediate event likelihood to the TMEL.

The SIS and associated SIL for one instrumented system protecting against as scenario is independent (and independently calculated) from a separate SIS and associated SIL protecting against the scenario.

Independence between protection layers is a necessary principle for the math in LOPA to be correct. Practically, however, the failure rate for the processor is much lower than for an I/O card and for field sensors and final elements. If the processor is the only common element between a BPCS loop and an alarm, taking credit for both as though they were truly independent is only slightly optimistic mathematically.

11.7. Other types of IPLs

a. Non-instrumented systems may be used as IPLs. If they are credited as IPLs in a LOPA scenario, they shall conform to the criteria for IPLs defined in 5.3.b.

There is a joint industry project that is currently addressing the topic of non-instrumented IPLs. As this project identifies appropriate values to be used, they will be considered as updates to this GP.

b. The preferred approach is to consider the successful performance of passive devices, such as fire/blast wall, when estimating the appropriate consequence level (as opposed to inclusion in the LOPA math as an IPL).

c. If a passive device is considered in estimating the consequence level for a scenario, credit for this same device as an IPL (refer to Table 11) shall not be taken

12. Determining intermediate event likelihood

12.1. General

a. Intermediate event likelihood is the product of the initiating event likelihood, enabling event probabilities, PFD of IPL, and frequency modifiers. The result is compared to TMEL for the consequence category.

b. Calculation is generally performed on a logsheet, spreadsheet, or proprietary software.

12.2. PFD for IPLs

a. Risk reduction for each IPL is based on its PFD.

b. The lookup tables provided as Table 11, Table 12, Table 13, and Table 14 shall be used to estimate the PFD.

These lookup tables are developed based on rules suggested in Layer of Protection Analysis published by CCPS.

c. Permission to use alternate PFD values shall be obtained from the BP Operations EA and request to use an alternate value shall include the following, as applicable.

1. A quantitative method shall be used to justify the alternate value.

For example, if a team wants to claim a lower PFD for operator response than the values specified in Table 14, then a human factor analysis can be performed to determine the appropriate PFD.

2. If protection layers are not fully independent and it is desired to claim credit for all the layers, quantitative method shall be used to determine the amount of credit to be given taking into account of common mode and common cause failure.

Table 11 - PFD for passive IPLs

Risk Reduction Measures	PFD	Comments
Dike/Bund	1×10^{-2}	Will reduce frequency of large consequences (widespread spill) of tank overfill/ rupture/spill.
Underground drainage system	1×10^{-2}	Will reduce frequency of large consequences (widespread spill) of tank overfill/ rupture/spill.
Open vent (no valve)	1×10^{-2}	Will prevent overpressure.
Fireproofing	1×10^{-2}	Will reduce rate of heat input and provide additional time for depressurising/firefighting.
Blast wall/bunker	1×10^{-3}	Will reduce frequency of large consequences of explosion by confining blast and protecting equipment/buildings.
Flame/detonation arrestors	1×10^{-2}	If properly designed, installed, and maintained, should eliminate potential for flashback through piping system or into vessel or tank.

Table 12 - PFD for active mechanical risk reduction measures

Risk reduction measures	PFD	Comments
Relief valve	1×10^{-2}	Clean service and PRV shall be sized to completely mitigate the scenario.
Relief valve	1×10^{-3}	Multiple full-load PRVs are available to mitigate scenario.
Relief valve	1×10^{-2}	Multiple partial-load PRVs are available and sized such that more than one PRV would need to fail for the scenario to occur.
Relief valve	1×10^{-1}	Multiple partial-load PRVs are available, but more than one is required to mitigate the full load. This includes staged release PRVs.
Relief valve	1	Plugging service with no protection. An unprotected PRV used in plugging service is not considered sufficient for consideration as an IPL.
Relief valve	1×10^{-2}	Plugging service with protection. The design is based on prior history in similar services and may include the use of specially designed PRVs, inlet header purges, and close coupled rupture disks. If plugging can be caused by polymerization during venting these special designs are generally insufficient.
Vessel rupture disc	1×10^{-2}	Shall be designed to mitigate scenario.
Vacuum breaker	1×10^{-2}	Designed for the hazard and inspected periodically.
Blow out panel	1×10^{-2}	Shall be designed to mitigate scenario.

Table 13 - PFD for active instrumented risk reduction measures

Risk reduction measures	PFD	Comments
Basic process control system (BPCS) control loop	1×10^{-1}	*Can be credited as independent protection layer if not associated with initiating event being considered.* *If claims are made that BPCS has failure rate less than 10-5/hr, BPCS needs to be implemented in accordance with IEC 61511.* *IEC 61511 places limit of 0.1 for PFD of BPCS, unless BPCS is designed and maintained as safety system in accordance with IEC 61511.*
Safety instrumented function (interlocks)	See GP 30-75, 76, 80 and 81IEC 61508 and IEC 61511 for lifecycle requirements and additional discussion.	
SIL 1 SIS	1×10^{-2} to 1×10^{-1}	Typically consists of single sensor, single logic solver, and single final element.
SIL 2 SIS	1×10^{-3} to 1×10^{-2}	Typically consists of multiple sensors (for fault tolerance), multiple channel logic solver (for fault tolerance), and multiple final element (for fault tolerance).
SIL 3 SIS	1×10^{-4} to 1×10^{-3}	Typically consists of multiple sensors, multiple channel logic solver, and multiple final elements. Requires careful design and frequent proof tests to achieve low PFD figures.
Note: If the SIL level has been verified for a specific SIS, that value should be used as opposed to the range listed above.		

Table 14 - Example PFD for human actions

Risk reduction measures	PFD	Comments
Human action with 10 min response time	0.1 to 0.5	Simple well documented action with clear and reliable indications that action is required.
Human response with 20 min response time	0.1	Simple well documented action with clear and reliable indications that action is required.

12.3. PFD of SIF

a. If protection is currently provided by SIF or if a SIF is recommended, the target SIL for a SIF can be determined from LOPA.

b. The selected SIL represents the probability category for SIF failure on demand that ensures the mitigated event likelihood does not exceed the maximum likelihood target or TMEL.

c. Simple calculations shall be performed as follows to determine PFD_{SIF}. These build on the use of the numerical values identified in preceding steps.

1. Determine ICL and PFD of each IPL identified.

2. Determine IEL for each initiating cause by multiplying ICL and PFD of each IPL identified. If there is more than one initiating cause for the same hazard, the IELs of each initiating cause should be calculated.

3. Determine if the sum of the IELs ≤ TMEL.

$IEL_1 + IEL_2 + IEL_3 + \ldots \leq TMEL_{(H2S,\ E,\ or\ Damage)}$ (Table 6, Table 7, or Table 8)

Where:

TMEL = TMEL from table indicated.

IEL_i = Intermediate event likelihood (ICL_i*PFD_1*PFD_2...*Ptr*Pp*Pi).

ICL = initiating cause likelihood (Table 1 and Table 2).

PFD_1, PFD_2 = PFD for each IPLs (Tables 11, Table 12, Table 13, and Table 14).

P_{tr} = probability of time at risk (see 9.4.2).

P_p = probability of persons present (see 9.4.3).

P_i = probability of ignition (see 9.4.4).

4. If the sum of the IELs ≤ TMEL, then further risk reduction is not appropriate.

5. If the sum of the IELs > TMEL and there is existing SIF, then the ratio of TMEL to the sum of the IELs, PFD_{SIF}, should be calculated to determine the SIL, EIL, CIL of the existing SIF.

$$PFD_{SIF}(HealthandSafety) = \frac{TMEL(Table5)}{IEL1 + IEL2 + IEL3 + ...}$$

$$PFD_{SIF}(Environmental) = \frac{TMEL(Table6)}{IEL1 + IEL2 + IEL3 + ...}$$

$$PFD_{SIF}(Equip.damageandvaluelost) = \frac{TMEL(Table7)}{IEL1 + IEL2 + IEL3 + ...}$$

6. If the sum of the IELs > TMEL and there is not an existing SIF, then existing protection layers are considered insufficient to mitigate risk. Recommendation should be made to use inherently safer design strategies to redesign system, add additional protection layers, or add a SIF.

7. Recommendations for SIFs should use the ratio of TMEL to the sum of the IELs, PFD_{SIF} , to determine the SIL, EIL, CIL of the new SIF.

13. Evaluation of SIS integrity levels

13.1. ILs

a. If protection is currently provided by SIF or if a SIF is recommended, the LOPA determines the PFD to reduce the risks to below the TMEL for that consequence category.

b. The procedure for determining SIL, EIL, and CIL shall be as follows:

1. Calculate PFD_{SIF} without giving any credit to SIF (12.3).

2. Determine required SIL, EIL, and CIL from Table 15.

3. Select highest integrity level (the lowest PFD_{SIF}) and use it as design basis for SIF.

c. The PFD of the SIF shall be less than or equal to the lowest of PFD_{SIF} for all hazards for which the SIF provides protection.

d. Determination of IL for pushbutton initiation of isolation or depressurisation as part of ESD system shall be performed in accordance with GP 30-76, Annex E.

Table 15 - ILs for SIF

Required SIL, EIL, CIL	PFD_{avr}	RRF = (1/PFD)
SIL 0, EIL 0, CIL 0 - No special integrity requirements	$10^{-1} \leq PFD$	$RRF \leq 10$
SIL 1, EIL 1, CIL 1	$10^{-2} \leq PFD < 10^{-1}$	$10 < RRF \leq 100$
SIL 2, EIL 2, CIL 2	$10^{-3} \leq PFD < 10^{-2}$	$100 < RRF \leq 1\,000$
SIL 3, EIL 3, CIL 3	$10^{-4} \leq PFD < 10^{-3}$	$1\,000 < RRF \leq 10\,000$
SIL 4, EIL 4, CIL 4	$10^{-5} \leq PFD < 10^{-4}$	$10\,000 < RRF \leq 100\,000$

13.2. Spurious trips

a. If the spurious operation of a SIF can lead to hazardous consequences, the LOPA team should consider and document the impact of an unintended safe or spurious trip in a specific LOPA scenario. This impact may include safety and environmental impacts as well as equipment damage or financial loss.

For example, a SIF may require the opening of an emergency shutdown valve (ESD valve) which allows a high flow of emergency quench water into a process tower. At the same time the ESD valve is opened an emergency drain valve must be open to prevent overloading the tower. If the ESD valve opens spuriously during normal operation (but the drain valve does not open), there is potential for tower overfill and collapse.

b. If criteria for maximum allowable spurious trip rate has not been established by the facility, the LOPA team can suggest guidelines (e.g., once in 10 years).

This information is required by SIS design team to evaluate whether additional equipment is justified to reduce the spurious trip.

Refer to GP 30-76 for functional specification of SIS regarding this issue.

Annex A
(Informative)
Example of LOPA for SIL determination from PHA/HAZOP

Table A.1 - Information from HAZOP

Node 15	Amine Regenerator								
Drawing No.	101, 102								
Parameter	Pressure		Intention	To operate at 35 psig.					
GW	Deviation	Cause	Consequence	S	L	Risk	Safeguard	Recom-mendation	Remark
More	High Pressure	1. LV-2702 malfunction open.	Potential gas blowby to amine regenerator. Potential overpressure amine regenerator resulting in rupture. Potential fire and/or explosion.	H&S: D Env: F D&L: E	5 5 5	9 7 8	Operator training and procedure. PSV-2714 on amine regenerator set at 40 psig.		
		2. Manual bypass valve inadvertently open after maintenance.	Potential gas blowby to amine regenerator. Potential overpressure amine regenerator resulting in rupture. Potential fire and/or explosion	H&S: D Env: F D&L: E	5 5 5	9 7 8	Operator training and procedure. PSSR valve alignment checks Low level alarm LAL-801 on amine contactor. PSV-2714 on amine regenerator set at 40 psig		

Example of LOPA for SIL determination process using HAZOP in Table A.1 is described as follows:

a. Select hazardous scenario from HAZOP (Table A.1). This example has two initiating causes for the same hazard and has different IPLs applicable to each initiating cause.

b. Select TMEL as follows:

1. For safety (severity level D), TMEL is 1×10^{-5} /yr.
2. For environmental (severity level F), TMEL is 1×10^{-5} /yr.
3. For damage and loss (severity level E), TMEL is 1×10^{-3} /yr.

c. Identify initiating causes and quantify likelihood as follows:

1. Using Table 1, item "BPCS instrument loop failure", likelihood of the first initiating cause is 0,1/yr.

$$ICL_1 = 0,1/yr$$

2. Using Table 2, the second initiating cause is due to human intervention and the likelihood is assumed to be 0,1/yr.

ICL_2 = 0,1/yr

d. Identify independent layers of protection from existing safeguards without taking credit for SIS:

1. PSV-2714 on amine regenerator is IPL for both initiating causes. Using Table 12, item "Relief Valve", PFD for PSV is 0,01.

PFD for PSV = 0,01

2. The team verifies that the operator should be able to respond within 20 minutes after receipt of a low level alarm. Using Table 14, PFD for human response is 0,1. Since low level alarm uses the same level transmitter as LV-2702, credit should not be given to the first initiating cause.

PFD for human action = 0,1

3. Operator training and procedures are not considered IPLs.

e. Identify and quantify frequency modifiers

1. Time at risk factor: This is a continuous operation. (P_T = 1,0)

2. Occupancy as follows:

a) For the first initiating cause, people are present in the hazard zone half of the time. (P_p = 0,5).

b) For the second initiating cause, people are present in the hazard zone during this event since human intervention is the initiating cause. (P_p = 1,0).

c) Ignition probability: This event creates a very large vapour cloud and there are numerous ignition sources around the release location - therefore, P_I = 1,0.

f. Calculate intermediate event likelihood as follows:

1. First initiating cause:

a) For safety:

(ICL) 0,1 * (PFD for PSV) 0,01 * (P_T) 1,0 * (P_p) 0,5 * (P_I) 1,0 = $5,0 \times 10^{-4}$.

b) For environment:

(ICL) 0,1 * (PFD for PSV) 0,01 = $1,0 \times 10^{-3}$.

c) For damage and loss:

(ICL) 0,1 * (PFD for PSV) 0,01 = $1,0 \times 10^{-3}$.

2. Second initiating cause:

a) For safety:

(ICL) 0,1 * (PFD for PSV) 0,01 * (PFD for HA) 0,1 * (P_T) 1,0 * (P_p) 1,0 * (P_I) 1,0 = $1,0 \times 10^{-4}$.

b) For environment:

(ICL) 0,1 * (PFD for PSV) 0,01 * (PFD for HA) 0,1 = $1,0 \times 10^{-4}$.

c) For damage and loss:

(ICL) 0,1 * (PFD for PSV) 0,01 * (PFD for HA) 0,1 = $1,0 \times 10^{-4}$.

g. Compare sum of IELs with TMEL

1. For safety: $(5{,}0 \times 10^{-4} + 1{,}0 \times 10^{-4}) > 1 \times 10^{-5}$
2. For environment: $(1{,}0 \times 10^{-3} + 1{,}0 \times 10^{-4}) > 1 \times 10^{-3}$
3. For damage and loss: $(1{,}0 \times 10^{-3} + 1{,}0 \times 10^{-4}) > 1 \times 10^{-5}$

h. Because the sum of the IELs > TMEL, the PFD_{SIF} should be calculated to determine the appropriate SIL, EIL, CIL.

For safety,

$$PFD_{SIF} = \frac{1 \times 10^{-5}}{\left(5{,}0 \times 10^{-4} + 1{,}0 \times 10^{-4}\right)} = 0{,}017$$

For environmental,

$$PFD_{SIF} = \frac{1 \times 10^{-3}}{\left(1{,}0 \times 10^{-3} + 1{,}0 \times 10^{-4}\right)} = 0{,}91$$

For damage and loss,

$$PFD_{SIF} = \frac{1 \times 10^{-3}}{\left(1{,}0 \times 10^{-3} + 1{,}0 \times 10^{-4}\right)} = 0{,}91$$

i. Evaluation of SIS integrity level: the lowest PFD_{SIF} is 0,017 which requires a SIL 1.

j. Table A.2 shows the LOPA logsheet for this scenario.

Table A.2 - LOPA logsheet

Likelihood values are events per year; other numerical values are probabilities of failure on demand average.

Ref	1	2	3	4	5			6	7	8	9	10	11
					Protection layers (PLs)								
	Impact event description	Severity level	Initiating cause	Initiation likelihood	General process design	BPCS	Alarms, etc.	Additional mitigation, restricted access	Additional mitigation dikes (bunds), pressure relief	Intermediate event likelihood	PFD_{avg}	Target mitigated event likelihood	Notes
1	Over pressure of amine regenerator and potential 3 to 9 fatalities (Safety impact)	D	LV-2702 malfunction	0,1	--	--	--	Occupancy 0,5	PSV 0,01	5E-4	0,017 (SIL 1)	1E-5	
			Operator error	0,1	--	--	0,1	--	PSV 0,01	1E-4			
1	Over pressure of amine regenerator leading to localized damage to a non-sensitive environment (Environmental impact)	F	LV-2702 malfunction	0,1	--	--	--	--	PSV 0,01	1E-3	0,91 (EIL 0)	1E-3	
			Operator error	0,1	--	--	0,1	--	PSV 0,01	1E-4			
1	Over pressure of amine regenerator leading to damage and lost production ($5M to $100M) (Damage and loss impact)	E	LV-2702 malfunction	0,1	--	--	--	--	PSV 0,01	1E-3	0,91 (CIL 0)	1E-3	
			Operator error	0,1	--	--	0,1	--	PSV 0,01	1E-4			

Bibliography

BP

[1] Awaiting Number, *Group Recommended Operating Practice on Selection of hazard evaluation and risk assessment techniques.*

[2] GP 48-01, *HSSE Review of Projects (PHSSER).*

[3] GP 44-70, *Overpressure Protection Systems.*

[4] GP 44-80, *Relief Disposal Systems.*

[5] GP 48-02, *Hazard and Operability (HAZOP) Studies.*

[6] GP 48-04, *Inherently Safer Design (ISD).*

[7] GP 48-50, *Major Accident Risk (MAR) Process.*

American Institute of Chemical Engineers (AIChE)

[8] CCPS Concept Book, *Layer of Protection Analysis: Simplified Process Risk Assessment*, Center for Chemical Process Safety (CCPS), 2001.

[9] CCPS Guidelines, *Guidelines for Process Equipment Reliability Data*, (CCPS), 1989.

[10] CCPS Guidelines, *Guidelines for Safe and Reliable Instrumented Protective Systems*, (CCPS), 2007.

British Standards Institution (BSI)

[11] BS 7910, *Guide to methods for assessing the acceptability of flaws in metallic structures.*

Det Norske Veritas (DNV, Norway)

[12] OREDA *Offshore Reliability Data Handbook (OREDA)*, 1984, 1992, 1997, and 2002.

Energy Institute (EI)

[13] IP Research Report, *Ignition Probability Review, Model Development and Look-up Correlations*, IP, HSE, UKOOA, ISBN 978 0 85293 454 8, published by the Energy Institute.

International Electrochemical Commission (IEC)

[14] IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements.*

[15] IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements.*

[16] IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations.*

[17] IEC 61508-5, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels.*

[18] IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.*

[19] IEC 61508-7, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures.*

[20] IEC 61511-1, *Functional safety - Safety instrumented systems for the process industry sector - Parts 1: Framework, definitions, system, hardware and software requirements.*

[21] IEC 61511-2, *Functional safety - Safety instrumented systems for the process industry sector - Part 2: General requirements - Rating specifications for low voltage adjustable frequency a.c. power drive systems.*

[22] IEC 61511-3, *Functional safety - Safety instrumented systems for the process industry sector - Part 3: EMC requirements product standard.*

Institute of Electrical and Electronics Engineers (IEEE)

[23] Kumamoto, H., Henley, E.J., *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 1996.

IIT Research

[24] *Non-operating Reliability Databook*, 1987.

Instrument, Systems, and Automation Society (ISA)

[25] ISA TR84.00.02, *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques - Parts 1 to 5.*

Publications

[26] Smith, David, *Reliability, Maintainability and Risk*, David J. Smith PhD, ISBN 0 7506 5168 7, 5th ed., published by Butterworth Heinemann.

[27] Smith, D.J., *Reliability and Maintainability in Perspective*, 2nd and 3rd editions, Macmillan, London, 1985.