23
Analytical Methods in Process Safety Management and System Safety Engineering – Layers of Protection Analysis

Paul Baybutt

23.1
Introduction

Various analytical methods are used to support different aspects of process safety management, and layers of protection analysis (LOPA) has rapidly become one of the most important. LOPA is an analytical technique used to assess the risk of hazard scenarios for processes (CCPS, 2001). Commonly, it is used with process hazard analysis (PHA) to refine the qualitative risk rankings usually provided for hazard scenarios in order to produce more objective risk estimates in which greater confidence can be placed when making decisions on process modifications to reduce risk. However, LOPA is not a hazard identification method.

As with other forms of risk analysis, risk-informed decisions are made in LOPA by comparing risk estimates with risk tolerance criteria, sometimes called process safety target levels, to determine if there is a risk gap and a need to reduce the existing level of risk to meet the risk tolerance criteria.

LOPA is used to help resolve the need to implement PHA recommendations for risk reduction. Increasingly, it is also used to determine the safety integrity levels (SILs) required for safety instrumented functions (SIFs) to assist in compliance with industry standards for safety instrumented systems (SISs) such as IEC 61511/ISA 84 Parts 1–3 (ANSI/ISA 2004a–c). Other methods are also used, such as risk matrices and risk graphs, but LOPA has become a preferred method for many companies.

LOPA can be used in many other situations involving risk-informed decisions (Table 23.1).

Handbook of Loss Prevention Engineering, First Edition. Edited by J. M. Haight.

Table 23.1 Applications of LOPA.

Application	Purpose
Process hazard analysis	Evaluate the adequacy of existing safeguards Determine performance requirements for protection layers Resolve disagreements on PHA recommendations Resolve inconsistencies in PHA studies, for example, where there is team variability Analyze existing process safeguards to determine implicit risk tolerance criteria
Safety instrumented systems (IEC 61511/ISA 84)	Determine the safety integrity levels (SILs) required for safety instrumented functions (SIFs) in a safety instrumented system (SIS)
Quantitative risk analysis (QRA)	Screen hazard scenarios for further study using QRA
Design	Compare the risks of alternative designs to decide on the preferred design
Capital improvements	Use cost–benefit analysis with risk estimates to compare and prioritize alternative risk-reduction measures
Management of change	Compare the risks of the process with and without the change to decide if it should be implemented
Facility siting	Determine if the risks of scenarios that could impact occupied buildings and places where people are located are tolerable
Mechanical integrity	Identify safety-critical equipment
Operator roles	Identify safety-critical actions, for example, operator action to close a valve in response to an alarm Highlight the importance of particular process variables, alarms and actions in operator training and operating procedures
Incident investigation	Identify incident causes and safeguards that could have prevented the incident
Emergency response planning	Provide input to emergency planners to tailor response plans to actual scenarios better
Bypassing a safety system	Determine whether a critical safety system can be bypassed or taken out of service for a short, known time duration (e.g., for testing and/or repair) and determine what additional safeguards would be required in the interim
Overpressure protection	Determine the risk of the credible worst-case event used as the design basis for sizing pressure relief devices
Emergency isolation valves	Evaluate the need or provide justification for isolation systems
Other situations involving risk-informed decisions	Can be used in many cases

23.2 Overview of LOPA

23.2.1 Nature of LOPA

LOPA is a simplified form of risk assessment. It assists in identifying and determining the adequacy of *protection layers* for hazard scenarios (Figure 23.1). The goal of LOPA is to determine if there is sufficient protection, that is, if the risk can be tolerated. Process safety is best first addressed by an inherently safe process design. Protection layers are ued to address remaining risk. The term protection layer is used to mean a grouping of equipment and/or administrative and procedural controls that functions in concert with other layers to control process risk, for example, the barrier layer, or an individual protection measure, for example, a dike (bund).

LOPA is used to evaluate the risks of individual hazard scenarios. Each hazard scenario is a set of specific, unplanned events or sequence of events that has an undesirable consequence resulting from the realization of a hazard (see Chapter 21).

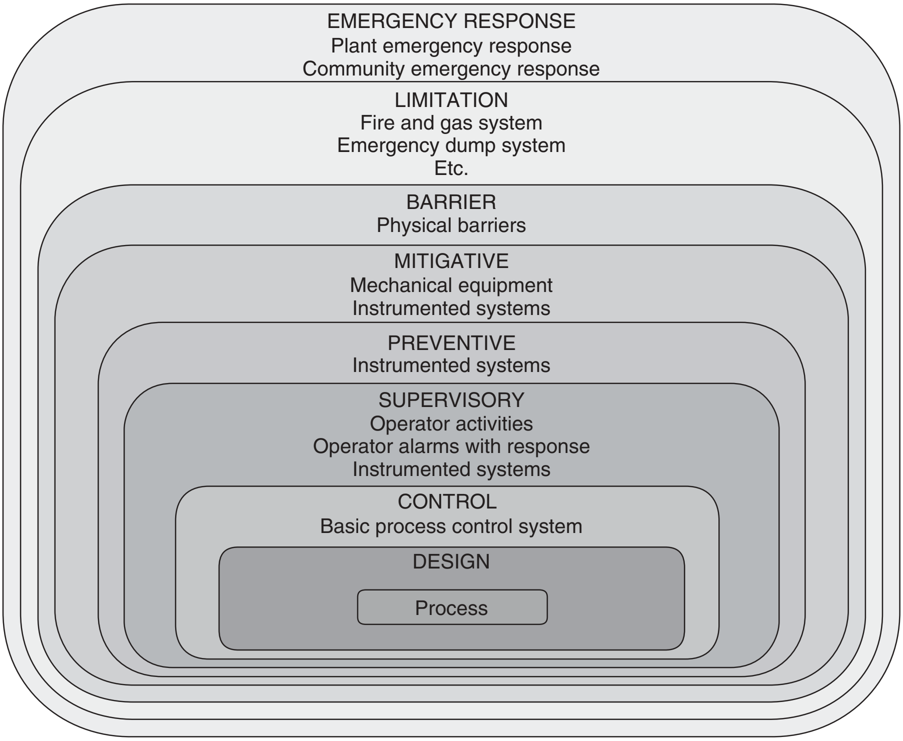


Figure 23.1 Protection layers for a process.

23.2.2
Hazard Scenarios

A hazard scenario begins with an initiating event which is the minimum combination of failures necessary to start the propagation of the hazard scenario. It may be an equipment failure, human failure, external event, or a combination thereof.

Human and automated control actions and safeguards typically respond to the initiating event. Safeguards are safety systems that protect against the hazard scenario, that is, they are *protection layers*. Process safeguards that prevent scenarios from occurring are called *prevention* layers. They act pre-release, for example, inhibitor addition. Safeguards that lessen the severity of the scenario consequences are called *mitigation* layers. They act post-release, for example, a deluge system. Safeguards that protect people are called *safety* protection layers, safeguards that protect the environment are called *environmental* protection layers, and those that protect property are called *property* protection layers.

Consequences are the direct impact of the hazard scenario in terms of its effects on receptors such as people, the environment, property or equipment, the process, the company, and so on. *Receptors* are the entities that are subject to harm. *Enablers* are events or conditions that must be present or active for the scenario to proceed, for example, an alarm that is bypassed. They do not by themselves initiate hazard scenarios, rather they make them possible. There are some special types of enablers. *At-risk factors* account for the time period in which a process is at risk, for example, a runaway of a batch reaction can only occur when the reaction is being conducted. *Incident outcome* enablers are used to represent different possible consequences, for example, fire or explosion. *Release condition* enablers are used to account for different release conditions or circumstances, for example, release duration and wind direction. *Conditional modifiers* (*conditionals* for short) affect the scenario consequence, for example, the probability that a flammable or explosive material will be ignited; the probability that a person will be present to be exposed to a hazard (sometimes called the *occupancy factor*); and the probability that harm will occur if an individual is exposed (sometimes called the *vulnerability*). Some enablers are similar and double counting must be avoided, otherwise scenario risks will be underestimated. Examples of enablers are provided in Table 23.2.

A situation that enables a scenario but always exists is called a *given*, for example, the location of a fixed and continuous ignition source, such as a boiler house, downwind of a release point. Givens are not addressed as enablers in LOPA as they are part of the scenario, that is, their probability of occurrence is 1. Other enablers may be probabilistic in nature, that is, their probabilities may be less than 1, depending on the circumstances, for example, hot work in a process as an ignition source. Further examples of givens are the omission of safety features from the process design and the locations of stationary equipment in the process.

Enablers may apply to any scenario element, that is, the initiating event, intermediate events, or consequences. There may be more than one enabler for each of the elements of a scenario and enablers for more than one element (Table 23.3).

Table 23.2 Examples of enablers.

Regular
Alarms disabled
Safeties/interlocks bypassed
Inhibit conditions overridden
Procedures not followed
Equipment in a failed or disabled state
Preventive maintenance (PM) not performed
Failure of inerting
Extreme ambient conditions
At-risk factors
Fraction of time a piece of equipment is operated
Fraction of time a process is in a particular mode
Fraction of time a process spends in a particular step
Fraction of time a particular event is possible
Fraction of time people are at risk, for example, time-of-day effects, day-of-week effects, indoors versus outdoors location
Incident outcomes
Vessel rupture
Fire versus explosion
Type of fire, e.g.: → Pool → Flash → Jet
Type of explosion, e.g.: → Confined → Unconfined → Boiling Liquid Expanding Vapor Explosion (BLEVE)
Release conditions and circumstances
Release characteristics, e.g.: → Hole size → Location → Elevation → Orientation → Duration → Delayed ignition

(continued overleaf)

Table 23.2 *(continued)*

Conditional modifiers
Weather conditions, e.g.: →Wind direction →Wind speed →Atmospheric stability class →Precipitation

Conditional modifiers
P^{ignition} – probability that a flammable/explosive material will be ignited P^{present} – probability that a person will be present to be exposed to a hazard, that is, the fraction of time personnel are in the area $\mathrm{P}^{\text{injury}}$ – probability that harm will occur if an individual is exposed Probability of sheltering Probability of escape Probability of evacuation

Table 23.3 Examples of enablers for scenario elements.

Type of element	Scenario element	Enablers
Initiating event	Pump seal leak	Lack of PM on pump Pump mis-operation
Intermediate events	Flammable gas release resulting in a fire	Flammable gas detectors inoperative Presence of ignition source
Consequence	Potential fatality	Presence of operator in the area

The effect of enablers is to increase or decrease the frequency of the hazard scenario. For example, lack of preventive maintenance (PM) on a pump will increase the failure rate for the pump while the presence of an operator in the area of a potential hazardous material release for less than 100% of the time will decrease the likelihood of harm to the individual.

23.2.3 LOPA Characteristics

LOPA reduces subjectivity in the decision-making process by using rules and well-defined criteria to guide the analysis. This produces more defensible decisions than PHA. LOPA helps to focus limited resources on the most critical safeguards and identify safeguards that should be emphasized during employee training, daily operations, and maintenance activities. LOPA does *not* suggest which safeguards to add or which design to choose to reduce risk to tolerable levels. However, it does assist in deciding between alternatives. Without LOPA, there can be a tendency to keep adding safeguards in the belief that the more that are added, the safer is the process. However, this can be a false assumption. Eventually, safeguards will be added that are unnecessary. They reduce the focus on the safeguards that are critical to achieving tolerable risk (TR) and add complexity that may result in new, and possibly unidentified, hazard scenarios.

Usually, LOPA helps to improve the details of the scenarios analyzed, and other scenarios or issues missed in PHA may be revealed. LOPA can be used at any stage in the process life-cycle beginning with early design when process changes can be made more easily. LOPA is a step towards quantification of scenario risk but involves much less effort than quantitative risk analysis (QRA) owing to the simplifying assumptions used. The simplifications are intended to be conservative so that QRA would show lower risk for a scenario than LOPA.

23.2.4 Timing of LOPA

Early LOPA studies were performed after a PHA was completed. Often, the LOPA team members discovered that PHA scenarios needed to be revised and the PHA team had to be reconvened to do so. Even when the LOPA team was the same as the PHA team, re-discussion of scenarios was needed, reducing the study efficiency.

LOPA builds on the information developed in PHA and can be performed as part of the PHA. Generally, this approach saves time because the analysts do not have to re-visit the scenarios. Typically, LOPA is now applied immediately after a PHA has identified hazard scenarios. However, LOPA is best separated from the brainstorming of scenarios since it can distract the team from this vital task.

23.3 Scenario Risk

23.3.1 Meaning of Risk

The risk, R, of a hazard scenario is a function of the scenario consequence severity, S, and its likelihood of occurrence, L. The consequence severity is the degree of impact of the hazard scenario and the likelihood of occurrence is how often a scenario is expected to occur. Commonly, R is defined as the product of S and L, that is, $R = S \times L$ (CCPS, 2000). The severity, S, and likelihood, L, may be expressed qualitatively or quantitatively.

23.3.2 LOPA Approaches

LOPA approaches differ according to how severity and likelihood are evaluated. The simplest approach is to use qualitative estimates for both severity and likelihood. However, such an approach is equivalent essentially to risk ranking in PHA. Since the goal of LOPA is to provide increased confidence over PHA risk estimates, some degree of quantification is desirable. Unfortunately, quantification of the consequence severity is challenging. The calculations are difficult to simplify and they require substantial effort and expertise. Consequently, consequence quantification is not commonly used in LOPA, although some practitioners employ estimates of release quantities to improve on the simple severity estimates used in PHA. On the other hand, simplified quantification of scenario likelihood is feasible if reasonable approximations are employed. Thus, the most common LOPA approach uses qualitative consequence severity estimates and quantitative likelihood estimates. Usually, only order-of-magnitude estimates are used. This approach requires much less effort than the detailed modeling and calculations used in QRA.

23.3.3 Risk Calculation

The risk of a scenario consequence severity is expressed as a frequency, that is, a *rate* of occurrence, usually, per year. It is calculated by taking the frequency of the initiating event and combining it with the probabilities of the other events in the scenario. Probabilities are dimensionless numbers. In the context of LOPA, they represent the number of times an event is expected to occur out of the total number of possible occurrences. Typically, such probabilities are described as Probabilities of Failure on Demand (PFDs) since they are used to represent the probability that a protection system will fail to perform a specified function on demand, that is, the scenario continues toward the undesired consequence despite the presence of the protection system. Thus, PFDs quantify the effectiveness of protection systems. The demand occurs whenever the process reaches a condition where the protection system is called on to function. The lower the value of the PFD, the greater is the confidence it will operate correctly and interrupt the chain of events in the scenario, and the larger will be the reduction in frequency of the undesirable consequence.

In LOPA, PFDs are usually expressed to no more than two significant figures since LOPA uses orders of magnitude estimates for risk but allowance needs to be made for rounding errors. Sometimes, protection system failure data are expressed in other ways, for example, as safety availability (SA) (i.e., the probability of success) and as a risk reduction factor (RRF). $SA = 1 - PFD$ and $RRF = 1/PFD$. Thus, if the PFD is 0.01, the SA is 0.99 and the RRF is 100.

Typically, LOPA is used to analyze the scenario in which all protection layers fail (Baybutt, 2012b). This can be seen in Figure 23.2 as the path in the event tree that follows the downward branches. The frequencies of scenarios in Figure 23.2 can be calculated by multiplying the initiating event frequency by the probabilities of the other events in the path of the scenario, provided that all the events are independent of one another. LOPA depends on this assumption. Therefore, any safeguard that is credited as a protection layer in LOPA must be an independent protection layer (IPL), that is, its action should not depend on any other aspect of the scenario, such as the initiating event, or the action or failure of any other protection layer associated with the scenario. In practice, additional criteria must be met to qualify

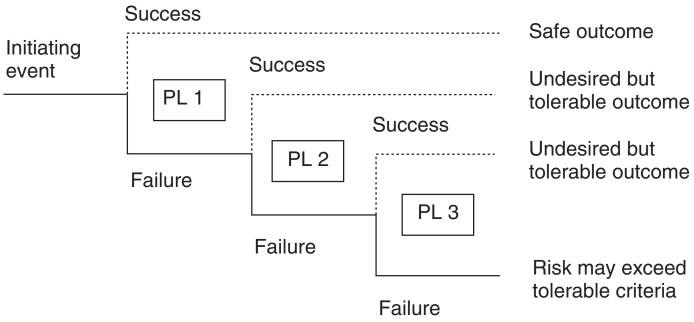

Initiating event
Success
Safe outcome
PL 1
Success
Undesired but tolerable outcome
Failure
PL 2
Success
Undesired but tolerable outcome
Failure
PL 3
Risk may exceed tolerable criteria
Failure

Figure 23.2 Event tree showing the hazard scenario typically analyzed in LOPA.

safeguards as IPLs (see Section 23.7.5). Consequently, not all safeguards are IPLs, but all IPLs are safeguards. LOPA takes credit only for IPLs.

23.3.4 Use of Risk Estimates

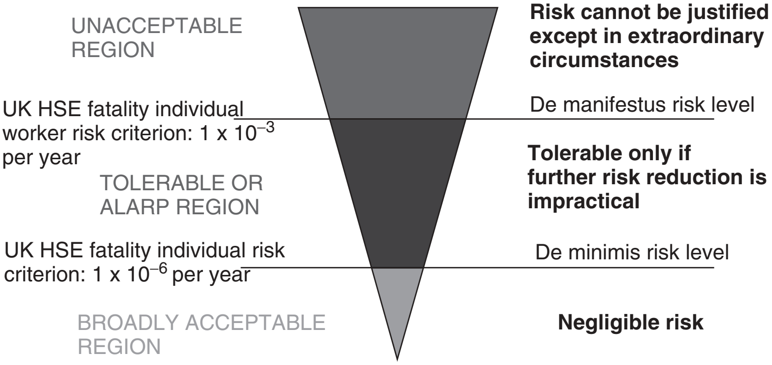
Scenario risk estimates are compared with risk tolerance criteria to determine if additional risk reduction is required to reach a tolerable level. The difference between the estimated risk (ER) and the TR is called the *risk gap*. Once the gap has been determined, the primary objective of LOPA has been met. However, at some point, the means to reduce the risk to tolerable levels must be determined. Some companies incorporate that effort into the LOPA study and develop recommendations for risk reduction to eliminate risk gaps.

23.4 Risk Tolerance Criteria

Usually, it is not possible to eliminate all risk from an activity unless the activity itself is eliminated. Consequently, criteria are needed to specify levels of risk that can be tolerated. Risk tolerance criteria are standards used for comparison with the ER to determine its acceptability and assist in decisions on whether further efforts to reduce risk are warranted. No level of risk is viewed as truly acceptable by some people, so usually the term *tolerable* is employed. The *residual* risk is the risk that remains after controls have been implemented. It must be tolerable for continuance of an activity.

23.4.1 ALARP Principle

The ALARP (as low as reasonably practicable) principle has been defined by the UK Health and Safety Executive (HSE) (HSE, 2001) to depict the concept that efforts to reduce risk should be continued until the incremental sacrifice in doing so is grossly disproportionate to the value of the incremental risk reduction achieved


UNACCEPTABLE REGION
Risk cannot be justified except in extraordinary circumstances
UK HSE fatality individual worker risk criterion: 1 x 10⁻³ per year
De manifestus risk level
TOLERABLE OR ALARP REGION
Tolerable only if further risk reduction is impractical
UK HSE fatality individual risk criterion: 1 x 10⁻⁶ per year
De minimis risk level
BROADLY ACCEPTABLE REGION
Negligible risk

Note: UK HSE criteria are per person for all hazards for a facility.

Figure 23.3 The ALARP principle.

(Figure 23.3). Incremental sacrifice is defined in terms of time, effort, cost, or other expenditure of resources (HSE, 2011). Usually, each incremental reduction in risk will require a greater expenditure of resources.

Three general levels of risk are shown in Figure 23.3. Negligible risks are so low as not to be of concern. This is sometimes called *de minimis* risk. Tolerable risks are considered acceptable if the benefit is seen to outweigh the impact. Unacceptable risks cannot be justified, except under extraordinary circumstances. The triangle represents the decreasing risk and the diminishing proportional benefit as risk is reduced.

The ALARP principle can be used to define two sets of risk tolerance criteria: a minimum requirement and a target value. Between the two sets of criteria, the range of risks is tolerable. The residual risk should fall either in the broadly acceptable region, or near the bottom of the tolerable region. This approach allows higher levels of safety to be provided where it is feasible. Risk tolerance criteria suggested by the HSE are shown in Figure 23.3 at the two dividing lines between the three risk regions.

The ALARP principle originated within a legal and regulatory framework. Increasingly, it is used by regulators and companies around the world as it provides a sensible basis for managing risks. The ALARP principle is now called so far as is reasonably practicable (SFAIRP) in the UK, with some legal distinctions from ALARP (Health and Safety at Work etc. Act 1974).

23.4.2
Form of Risk Tolerance Criteria

Risk tolerance criteria may be qualitative or quantitative in nature but must correspond to the form of the risk estimates used in LOPA. They may be depicted explicitly, for example, using defined numerical criteria, or they may be displayed implicitly, for example, in a risk matrix.

Table 23.4 Example of a risk matrix showing tolerable risk criteria[b].

Frequency of mitigated scenario consequence/year	Consequence severity level[a]				
	1	2	3	4	5
$1–10^{-1}$	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}
$10^{-1} - 10^{-2}$	TR	10^{-1}	10^{-2}	10^{-3}	10^{-4}
$10^{-2} - 10^{-3}$	TR	TR	10^{-1}	10^{-2}	10^{-3}
$10^{-3} - 10^{-4}$	TR	TR	TR	10^{-1}	10^{-2}
$< 10^{-4}$	TR	TR	TR	TR	10^{-1}

[a] Note: This matrix shows how much risk reduction is needed.
[b] TR = tolerable risk.

The simplest risk tolerance criteria are for hazard scenarios. They can be shown using risk matrices (see Table 23.4) or specified as the maximum TR for a particular scenario consequence severity, for example, a single fatality risk of 1×10^{-5} per year. More complex risk tolerance criteria may be needed that set limits for summations of the risk of multiple scenarios, for example, those that contribute to a specific hazardous event of those that result in the same consequence for a process or facility. Such criteria represent maximum tolerable cumulative risks. Scenario risk criteria are easier to understand but cumulative risk criteria are more representative of the total risk and their use ensures that decisions are not based exclusively on individual scenarios which can result in inappropriate risk reduction decisions.

23.4.3 Types of Risk Tolerance Criteria

Different types of risk measures can be constructed depending on how individual scenario risk estimates are combined to produce overall risk estimates. The types of risk measures calculated must match the type of risk tolerance criteria used. Risk to people can be characterized using two different types of risk measure (CCPS, 2000, 2009):

- risk to an individual (called *individual risk*)
- risk to groups of people (called *societal risk, communal risk*, or *group risk*).

Individual risk provides a measure of the risk to an individual in the vicinity of one or more hazards, that is, in the zones affected by the hazard scenarios for the process. Individual risk tolerance criteria specify a limit to the risk to which an individual should be exposed, usually as the maximum frequency at which an individual may experience a given level of harm from the realization of hazards.

Societal risk provides a measure of the risk to a group of people and societal risk tolerance criteria specify a limit to the risk to which a group of people should be exposed, typically in the form of the relationship between the maximum frequency at which various numbers of people in a given population may experience a given level of harm from the realization of hazards.

Societal risk provides a measure of the overall risk to a population but only individual risk provides information about the distribution of risk within the population. Individual risk criteria help prevent any one individual from being exposed to an inequitable share of risk but provide no indication of the number of people impacted by hazard scenarios. Some hazard scenarios have the potential to affect multiple people and, consequently, they are of considerable concern for process safety. Therefore, societal risk measures are used to represent this aspect of risk to people.

A facility may meet individual risk tolerance criteria but not societal risk criteria, or vice versa. For example, individual risk may be low but societal risk high if there is a large population of people exposed to the risk. Conversely, societal risk for facility personnel may be low but individual risk may be high for personnel in a process unit at the facility that contains a large amount of hazardous material. Such situations would not be acceptable. Both individual and societal risk can be calculated for on-site personnel (employees and contractors) and off-site personnel (members of the public). Societal risk for on-site personnel has been addressed infrequently, although logically it should be included in risk-informed decision-making. Decisions on reducing risks in a facility using LOPA should address both societal and individual risks (Baybutt, 2012a).

Depending on the scope and objectives of the LOPA study, risk tolerance criteria may be needed for:

- different types of receptors, for example:
  - people
  - environment
  - property
- different classes of a receptor, for example:
  - employees versus the public
  - on-site property versus off-site property
- different hazardous events, for example:
  - fire
  - explosion
  - toxic material release
  - runaway reaction
- different levels of harm, for example:
  - multiple versus single fatalities, fatalities versus injuries
  - environmental remediation versus cleanup.

Fatalities and injuries are typically used as measures of harm for people and financial impacts are often used for other types of receptors. At a minimum, it is suggested that risk tolerance criteria be established for people and the environment. Employees and the public should be addressed separately.

23.4.4 Determining Tolerable Risk

Levels of TR are determined by the risk levels that are accepted in a given context based on:

- current values of society
- national and international standards and regulations
- corporate policies
- input from concerned parties, such as:
  - communities
  - local government jurisdictions
  - insurance companies
- good engineering practices.

Thus, societal, legal, regulatory, business, and engineering considerations must be addressed in formulating risk tolerance criteria. These can be unique to each company. Additional factors to consider in setting risk criteria include the following:

- comparisons with other companies
- industry and company historical accident statistics
- comparisons with the risks of everyday activities
- ability to achieve
- cost to achieve.

Criteria should be calibrated and validated against established consensus values as reflected in historical precedents and decisions regarding the tolerance of major hazard risks. Examples of risk tolerance criteria for safety, environmental, and financial impacts, are provided in Tables 23.5, 23.6, and 23.7, respectively, for various consequence severity levels.

23.4.5 Use of Risk Tolerance Criteria

Once risk tolerance criteria have been set and risk estimates have been made, a simple comparison of them determines if risk reduction measures are needed.

Table 23.5 Example of risk tolerance criteria for safety impacts.

Level	Meaning	Tolerable frequency/year
1	Potential for 100 or more fatalities	1×10^{-6}
2	Potential for 10 or more fatalities	1×10^{-5}
3	Potential for 1 or more fatalities	1×10^{-4}
4	One or more hospitalization injuries	1×10^{-3}
5	One or more recordable injuries	1×10^{-2}
6	One or more first aid cases	1×10^{-1}

Table 23.6 Example of risk tolerance criteria for environmental impacts.

Level	Meaning	Tolerable frequency/year
1	Damage that can be remediated within 5 years	1×10^{-6}
2	Damage that can be remediated within 3 years	1×10^{-5}
3	Damage that can be remediated within 1 year	1×10^{-4}
4	Damage that can be remediated within months	1×10^{-3}
5	Damage that can be remediated within weeks	1×10^{-2}
6	Damage that can be remediated within days	1×10^{-1}

Table 23.7 Example of risk tolerance criteria for financial impacts.

Level	Meaning (US$)	Tolerable frequency/year
1	500M–5B	1×10^{-5}
2	50M–500M	1×10^{-4}
3	5M–50M	1×10^{-3}
4	500k–5M	1×10^{-2}
5	50k–500k	1×10^{-1}
6	<50k	1

If the ER is less than the risk tolerance criterion, the situation is judged to be of sufficiently low risk, that is, there is sufficient protection so that no further protection is needed. If the ER exceeds the risk tolerance criterion, the scenario is judged to require stronger protection or additional protection, that is, design changes are needed to make the process safer.

Care must be excerised to use appropriate risk tolerance criteria for the application (Baybutt, 2012d).

23.5 Stages and Steps in LOPA

LOPA entails several stages and steps:

- initiating a project
- preparing for LOPA:
  - deciding on a LOPA approach
  - deciding on TR criteria
  - selecting hazard scenarios for analysis
  - determining which scenario elements will be addressed
  - deciding on criteria for qualifying safeguards as IPLs
  - obtaining and using failure data
- preparing for a study:
  - defining the purpose, scope, and objectives (PSO)
  - selecting a team

  - collecting information and data needed
  - estimating the effort required and scheduling study sessions
  - briefing/training team members
  - arranging required facilities
  - addressing other items
- conducting a study:
  - conducting the first session
  - recording scenario information
  - assigning initiating event frequencies
  - addressing enablers
  - assigning enabler probabilities/multipliers
  - identifying existing IPLs
  - assigning IPL PFDs
  - documenting IPLs
  - estimating scenario consequence severity and frequency
  - evaluating scenario risk
  - assessing compliance with TR criteria
  - developing recommendations for any needed risk reduction
  - addressing quality assurance
  - revalidating previous studies
  - preparing a report
  - following up.

Some companies have developed written procedures to govern their LOPA studies, in which case LOPA facilitators must familiarize themselves with the procedures. If company procedures are not available, facilitators will need to develop their own guidelines. Procedures are important as they help to ensure that:

- LOPA performance and documentation complies with industry standards and company requirements
- LOPA studies are conducted consistently for different processes
- appropriate teams are selected
- responsibilities are established
- a consistent format is used to facilitate the use of LOPA studies by others
- schedules are established to ensure timely completion
- departures from established practices are avoided.

Companies should establish a system to manage the performance of LOPA studies. Such a system needs to cover training of teams, team selection, scheduling sessions, tracking recommendations, and so on. Each of the stages and steps in conducting LOPA is described in the following sections.

23.6
Initiating a Project

A LOPA project begins when a responsible manager determines that a study is needed. The responsible manager must:

- determine that a study is required
- ensure it is performed when required
- specify the level of detail required
- appoint a study leader
- assist in the identification and assignment of team members and ensure their availability
- provide or arrange for necessary resources
- ensure the study is planned and performed
- monitor the study and provide support
- resolve issues as the study progresses
- ensure that the study is completed and documented
- receive and act on the results of the study
- ensure any needed liaison with the process owner occurs.

The project must be clearly defined by the responsible manager, including the facility, processes, and chemicals to be addressed. This information is provided to the team leader.

23.7 Preparing for LOPA

The issues addressed in this section are commonly covered by LOPA procedures. In such cases, the responsibility of LOPA facilitators is to understand the issues and implement the procedures.

23.7.1 Deciding on a LOPA Approach

There are many variants of LOPA. The key decision is whether the scenario severities and likelihoods will be evaluated qualitatively or quantitatively as discussed in Section 23.3.2. Other decisions relate to how:

- safeguards will be qualified as IPLs (see Section 23.7.5)
- enablers will be addressed (see Section 23.7.4)
- consequences will be expressed.

Consequences can be expressed in various forms (Table 23.8). Releases and impacts are the most common forms used. Whichever form is used must be consistent with the form and type of the risk tolerance criteria used (see Sections 23.4.2 and 23.4.3). Use of releases as endpoints avoids estimating the numbers of injuries/fatalities, and so on, which can give the overt appearance that injuries/fatalities, and so on, are tolerable. It also avoids the difficulty and uncertainty of determining the numbers of people who may be harmed and how severe the harm might be. However, analysts usually better understand consequence severities in terms of impacts rather than releases. In either approach, usually, the consequence severity is assigned to one of several categories. Risk tolerance criteria must correlate with these categories.

Table 23.8 Consequence endpoints for hazard scenarios.

Endpoint	Measures
Release of hazardous material	Quantity released, physical characteristics of material
Dispersion of hazardous material	Dispersion distance/area for specific concentrations
Physical effects	Size of fire, explosion, toxic exposure, energy release
Impacts or losses from physical effects	Number of injuries/fatalities, financial impacts, environmental decontamination costs, and so on

The consequence types that will be included in the study must be specified (e.g., impacts on people, the environment). This issue is addressed as part of the definition of the scope of the LOPA study (see Section 23.8.1).

23.7.2 Deciding on Tolerable Risk Criteria

TR criteria must be expressed in the same form as the risk estimates calculated in LOPA as a comparison must be made between them. TR criteria should be set before beginning a LOPA study. Further details on the specification of criteria are provided in Section 23.4.

23.7.3 Selecting Hazard Scenarios for Analysis

Hazard scenarios may be taken from various sources, including:

- preliminary hazard analyses
- design hazard reviews
- existing PHAs
- management of change (MOC) PHAs
- revalidation PHAs
- new PHAs
- incident investigations
- emergency response plans
- cause and effect matrices.

Usually, criteria are employed to select scenarios for analysis, for example:

- scenario risk, for example, those above PHA Risk Level 4
- type of consequence, for example, impacts on people
- consequence level, for example, all PHA Category 5
- scenarios involving a SIF (when determining the required SIL for a SIF).

An example of a decision scheme is provided in Figure 23.4. Some companies will not use LOPA for scenarios that have the highest consequence levels (e.g., 5 or 10, or more fatalities) and use QRA approaches instead.

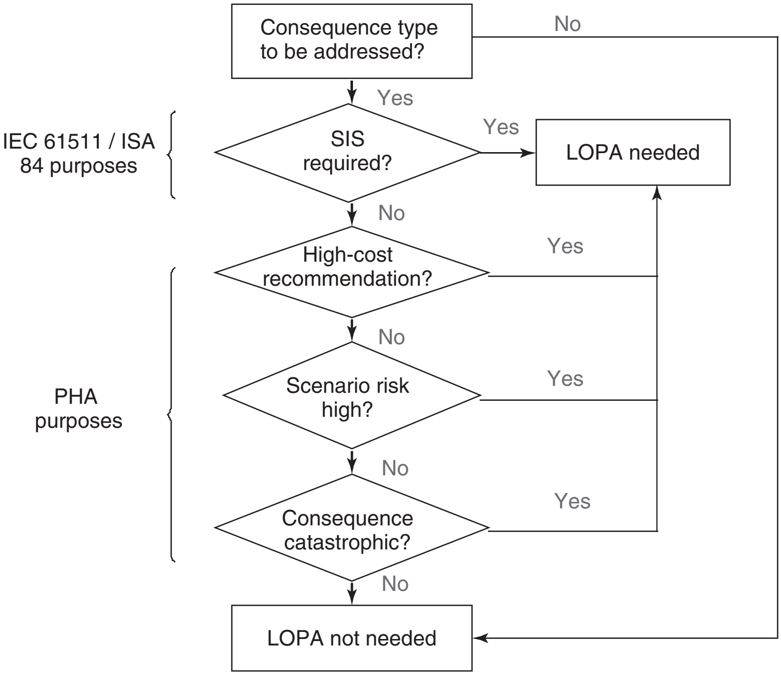

Consequence type to be addressed?
No
Yes
IEC 61511 / ISA 84 purposes
SIS required?
Yes
LOPA needed
No
High-cost recommendation?
Yes
No
PHA purposes
Scenario risk high?
Yes
No
Consequence catastrophic?
Yes
No
LOPA not needed

Figure 23.4 Example of a decision scheme for using LOPA.

For IPLs that mitigate the consequence, practitioners should consider evaluating the mitigated consequence as a separate scenario. The scenario in which a mitigation safeguard fails has the worst-case *consequence* but for the scenario in which it operates successfully, while the mitigated consequence is less, the frequency is usually higher and, therefore, the risk may be higher. In such cases, this scenario variant will set the requirement for the required risk reduction.

Many PHAs provide insufficient detail to be able to perform LOPA studies properly using their results. LOPA teams experience difficulties when PHA studies are performed without regard to the information needed for LOPA. The LOPA team must develop any needed information that is missing from the PHA. Not only does this work require additional time and effort but it also detracts from performing LOPA. Furthermore, the LOPA results may be inaccurate as the LOPA team may not develop hazard scenarios correctly. Guidelines to address this matter have been provided (Baybutt, 2012c).

23.7.4
Determining Which Scenario Elements Will Be Addressed

Some companies choose not to consider enablers that *reduce* the scenario frequency (including conditional modifiers) owing to the complexity that results and the potential for underestimation of scenario frequency. However, rules can be used to address underestimating scenario frequency that results from including enablers that reduce the scenario likelihood, for example, a rule that no more than three such enablers can be claimed for any scenario and a restriction that the maximum risk reduction from all such enablers for any scenario be limited to no more than 1×10^{-2}.

23.7.5
Deciding on Criteria for Qualifying Safeguards as IPLs

The heart of LOPA is deciding which safeguards qualify as IPLs. Criteria must be specified to make this determination. Historically, three key criteria have been used (CCPS, 2001):

- *Effectiveness*:
  - The safeguard protects against the undesired consequence of the scenario when it functions as designed.
- *Independence*:
  - Safeguard effectiveness must be independent of:
    - The occurrence or consequences, of the initiating event.
    - Failure of any component of an IPL already credited for the scenario.
    - Conditions that caused another IPL to fail.
    - Any other element of the scenario.
- *Auditability*:
  - The safeguard is designed to enable periodic validation that:
    - It is effective in preventing the consequences if it functions as designed.
    - It achieves the specified PFD.
    - Design, installation, functional testing, and maintenance systems for the safeguard are in place and working.

More recently, additional criteria have been proposed (Table 23.9). Further criteria are also possible, such as specificity, meaning the safeguard is designed to prevent or mitigate a scenario from proceeding to a specific consequence.

The key criterion is that of independence. If $P(\mathrm{A})$ represents the probability of event A, for independent failures:

$$P(\mathrm{A\ and\ B}) = P(\mathrm{A}) \times P(\mathrm{B}) \tag{23.1}$$

LOPA depends on this assumption (see Figure 23.2). For dependent failures:

$$P(\mathrm{A\ and\ B}) = P(\mathrm{A}) \times P(\mathrm{B}|\mathrm{A}) \tag{23.2}$$

where $P(\mathrm{B}|\mathrm{A})$ is the conditional probability of B given the occurrence of A. Thus, for dependent failures, their joint probability of occurrence cannot be determined simply by multiplying together the probabilities of the independent events. The result would not only be incorrect but would also underestimate the probability of the events occurring together, that is, a non-conservative result would be produced.

Table 23.9 CCPS attributes for independent protection layers (CCPS, 2007).

Attribute	Meaning
Independence	Performance of a protection layer is not affected by the initiating event, its consequences or the failure of other protection layers used to reduce the risk of the scenario
Functionality	Protection layer must be capable of operating according to its design during actual service conditions for all process operating modes where the hazard scenario can occur and responding effectively within the time required by stopping propagation of the initiating event even in the presence of other protection layer failures
Integrity or dependability	Risk reduction claimed for a protection layer is achievable given its design and management
Reliability	Probability that the protection layer operates according to its specification for a specified period of time under all relevant conditions
Auditability	Ability to inspect information, documents, and procedures, which demonstrate the adequacy of and adherence to the design, inspection, maintenance, testing, and operation practices used to achieve the other core attributes
Access security	Use of administrative controls and physical means to reduce the probability for unintentional or unauthorized changes to protection layers or systems that impact them
Management of change	Formal process to help ensure that changes made to the process and its protection layers do not negatively or inadvertently compromise the other core attributes

23.7.6 Obtaining and Using Failure Data

Various failure data are needed for LOPA, including:

- initiating event frequencies
- enabler multipliers and probabilities
- IPL PFDs.

23.7.6.1 Data Sources

Essentially, there are two primary sources of data:

- published data
- process data.

Published data appear in the literature or are available from other sources, for example, other plants or companies. Often they are called *generic* data since they do not apply to a specific process. Companies must find data applicable to their processes. This can be a challenge but it is the approach followed currently by many companies.

Process data are for a company's own processes and necessarily must be collected over an extended period of time in order to provide statistically significant values. Often they are called *plant-specific* data since they apply to specific processes. Clearly, they are preferred over generic data since they represent the actual operating environment, regime, and so on. Unfortunately, most companies either do not have such data or do not have sufficient data to be statistically meaningful. Consequently, generic data are commonly used. However, companies are establishing data collection programs to support their LOPA studies and plant-specific data increasingly should replace generic data.

Some common sources of generic data are:

- Center for Chemical Process Safety (CCPS), *http://www.aiche.org/ccps/*:
  - Guidelines for Process Equipment Reliability Data, 1989.
  - Guidelines for Improving Plant Reliability Data Collection and Analysis, 1998.
  - Guidelines for Chemical Process Quantitative Risk Analysis, 2000.
  - Process Equipment Reliability Database (PERD).
- Institute of Electrical and Electronic Engineers (IEEE), *http://www.ieee.org*:
  - Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations, 1983.
  - Standard Reliability Data for Pumps and Drivers, Valve Actuators, and Valves, 1986.
- OREDA, *http://www.oreda.com*:
  - Offshore Reliability Data, Handbook, 5th Edition, 2009.
- UK HSE, *http://www.hse.gov.uk*
  - Failure rate and event data for use within 2012 risk assessments.

In the absence of generic or process data, reliability modeling and expert opinion are sometimes used.

Vendor and laboratory data are unlikely to be applicable. Typically, they produce optimistic estimates since, for best-achievable performance, they are based on testing in clean, well-maintained laboratory environments that do not reflect actual process operating environments, which are invariably much harsher and produce higher failure rates than those obtained in a laboratory. In some cases, vendor data may be based on returns, but many components are thrown away rather than returned, and thus underestimates of failure rates result. Also, vendors may not be willing to provide data.

LOPA is intended to provide only an order of magnitude estimate for scenario risk. Therefore, individual failure data do not have to be highly accurate, which is fortunate given the current need to rely on generic data. However, conservative estimates should be used while being careful not to produce an overly conservative result. Equipment-specific data (i.e., manufacturer, make, model, and serial number) are not needed to obtain useful results.

23.7.6.2 **Standardized Data**

Companies should establish a standardized set of failure data for their plants and processes. Such a database can be constructed from generic data sources and any available company data to produce a tailored database. To the extent possible, data values should be applicable to the company's processes and be conservative estimates. Guidance on the applicability of the data should be provided considering such factors as specifications, equipment design and quality, service environments, the range of operating parameters, specific chemicals handled, operator and mechanic training, and inspection and testing requirements. Users of such data must give careful consideration to their true applicability given the scenario assumptions. Otherwise, unrealistic scenario risk estimates will result that produce poor decisions. LOPA analysts should be allowed to use more conservative values if they believe them to be appropriate. However, they should not use less conservative values without providing written justification. CCPS has documented recommended values for initiating event frequencies and IPL PFDs as a function of proof test method and frequency and other considerations (CCPS, 2010).

23.7.6.3 **Use of Data**

LOPA assumes that failure rates are constant, but that is not always true due to burn-in and burn-out of equipment. Equipment failure rates are typically higher immediately after installation and as equipment ages (a plot of average failure rate against time is known as a bathtub curve owing to its shape). For most equipment, the longest period of operation involves an approximately constant average failure rate so that is a reasonable assumption unless equipment is new or old.

Failure data are usually point values taken from distributions or ranges. They should be taken from the same part of the data range to provide a consistent degree of conservatism, for example, an upper bound that is at the same percentile of the distribution.

Human error rates are frequently underestimated by LOPA analysts. There is always a tendency to assume, optimistically, that people will perform at their highest level and save the day. Although this is certainly possible, error rates at the other end of distribution should be used for conservatism. Factors that influance humon error rates should be addressed (Baybutt, 2002)

Some failure data may combine data for multiple events such as initiating events, enablers, and/or conditional modifiers. Such confounded data can result in unreasonably low scenario frequencies if event failure data are inadvertently included more than once. Analysts must know what failures are included in the data used and avoid multiple counting.

For high-demand mode scenarios, the standard LOPA calculation does not apply and would result in unreasonably high scenario frequencies. High-demand mode occurs when the initiating event frequency (IPL demand rate or challenge frequency) is higher than the test frequency for the IPL, typically by a factor of 2, for example, an IPL is tested once per year and there are more than two demands per year. The standard calculation does not apply because the high number of demands on an IPL will detect its failure before its regular test. Alternative calculations must be used (CCPS, 2001).

When risk tolerance criteria are not met, analysts may be tempted to adjust failure rate data downwards, claiming that the adjustments are reducing conservatism in the data. This is poor practice since humans have shown time and again that they can readily talk themselves into whatever may be expedient.

23.8 Preparing for a Study

Various steps must be taken prior to study initiation. Thorough preparation is vital for a smooth-running and high-quality study.

23.8.1 Defining the Purpose, Scope, and Objectives

A vital aspect of study preparation is defining the PSO for the study. The PSO statement helps to ensure that the LOPA study is focused and complete and avoid the inclusion of extraneous items and digressions during the study sessions.

The purpose is why the study is performed. It must be defined as it affects the way in which the study is conducted, for example, the scenarios to be included and the types of consequences to be addressed. It helps to ensure that the study outcome is consistent with the intention for the study. Scope specifies what is included in the study and it may also specify what is *not* included. Items to address in the scope statement include the scenarios to be analyzed and any exclusions or assumptions. Objectives define what is to be considered, specifically, the types of consequences.

Management is responsible for the PSO statement. However, the statement is often drafted by the LOPA team leader for review and approval by management. The PSO statement may vary from one study to another, although commonalities for processes at the same facility will be likely.

The PSO statement is used to help ensure that team members fully understand the study goals as expressed by management. It is also used during the performance of the LOPA study to keep the team on track, ensure appropriate study content, ensure that the study is complete, and help avoid team members raising issues that are not relevant. It may be modified during the performance of a study, for example, if team members identify missing items. In such cases, management approval should be obtained for any changes made to it.

23.8.2 Selecting a Team

Usually, a LOPA study is performed by a team of people in order to provide the expertise needed to complete the study. The responsible manager and/or the team leader select the team members advised and approved by the other. Team members collectively should possess the knowledge and skills to analyze the hazard scenarios selected. They should have a sense of ownership and responsibility for the study to ensure their commitment and motivation. Typical participants are:

- facilitator/scribe
- process engineer
- operator
- safety engineer
- design/project engineer
- maintenance engineer
- electrical/instrumentation/control systems engineer
- risk/reliability analyst.

Commonly, a number of the participants will also be members of the PHA team. Team members should have personal attributes that result in positive team dynamics, which are important for an effective and efficient study. Of course, the availability of personnel must also be taken into account. Team member qualifications, including education and experience, should be documented as part of the LOPA records.

23.8.3 Collecting Information and Data Needed

Information and data needed for a LOPA study include:

- piping and instrumentation drawings (P&IDs) and other process drawings
- operating and other procedures
- hazard scenarios
- equipment design data, for example, relief systems, vessels
- cause and effect diagrams
- failure data.

The results of any available consequence analysis studies may also be useful. Needed information and data should be collected in advance of a study as some of the information may require a significant amount of time to develop, update, or assemble.

The validity of the LOPA study depends on the quality of the information on which it is based, so it is important to confirm that the information is accurate, complete, and clear.

23.8.4 Estimating the Effort Required and Scheduling Study Sessions

The effort required depends on the number of scenarios analyzed and their complexity. Typically, each scenario may require 5–25 min for analysis. Usually, 10–25% of the scenarios identified in the PHA are analyzed, although some companies analyze all PHA scenarios.

23.8.5 Briefing/Training Team Members

Team members should be briefed on the LOPA procedure that will be followed and reviews should be provided of the study PSO, the process and its hazards, and available information to support the study.

Novice teams will benefit from a short training session on LOPA. Practice in LOPA will be beneficial for the study. This briefing can be conducted shortly before the LOPA study begins or as part of the first session.

23.8.6 Arranging Required Facilities

A meeting room is required to conduct the study sessions. Ideally, it should be away from the facility, for example, at a neighborhood hotel, to provide fewer distractions and disturbances. However, an on-site meeting room provides access to the facility, proximity to reference materials, and availability of office equipment. Sufficient wall and table space is needed to display drawings and documents and team members must be able to enter, exit, and move around the room without obstructions.

A means is required to record the LOPA study. Typically, computer software is used. Therefore, a computer and computer projector are needed. The latter is used so that all team members can see entries as they are being made in the LOPA worksheet. A white board or flip chart should also be provided for impromptu use.

The room environment and lighting must be controllable and suitable. Temperature, humidity, ventilation, air quality, noise, and so on, should not interfere with the study. Variable lighting is needed to optimize viewing of the LOPA worksheet by computer projection and the reading of documents. Window blinds are needed to control sunlight. Of course, office supplies and refreshments should be provided.

Video or web conferencing for LOPA sessions is not recommended. Efficiencies and synergistic benefits of in-person meetings are lost and facilitation is harder. Personal interactions of team members are very important. However, video or web conferencing may be acceptable in some cases, for example, when team members are separated geographically, when team members know each other well, or when consulting with a subject matter expert.

23.8.7 Addressing Other Items

The team leader should prepare a project plan for the study to help ensure an efficient and effective study. Typically, the plan will include such items as:

- reference to LOPA procedures to be used
- PSO of the study
- names and roles of team members

- list of reference information to be used
- schedule (dates and times) and locations of PHA sessions.

The plan should be reviewed with the responsible manager, who should approve it and provide authorization to proceed with the LOPA study. The team leader and the responsible manager must agree on the authority of the team leader before the LOPA study begins, for example, the freedom to postpone a LOPA session if team members are absent or if needed information is not available.

The team leader should formally notify team members, and their supervisors, or managers, of their selection for participation in a study and their role and responsibilities. The intent is to ensure their availability and attendance. Team leaders should also provide an information package to team members so they can prepare for participation in the study. The package should contain such information as the study PSO and the dates, times and locations of sessions. The team leader may prepare session aids such as checklists to assist team members during LOPA sessions as well as configure recording software for the study.

23.9 Conducting a Study

23.9.1 Conducting the First Session

A number of important orientation issues should be addressed in the first session of a study. The team is briefed on the study and informed of what to expect in the LOPA sessions. The process of establishing the group as a functional team should begin as quickly as possible. Items to address include:

- team member introductions
- LOPA orientation
- explanation of LOPA procedure
- review of study PSO
- process overview briefing
- review of process hazards
- review of available study data
- review of guidelines for behavior by team members and rules to govern how the LOPA study will be conducted
- explanation of how recommendations will be handled
- viewing of the process.

The foundation should be laid for a constructive study. The team should be informed that it is normal for LOPA studies to find areas of needed improvement, even when processes are designed and operated by the most highly regarded people, and that no-one should feel threatened by critique of the process design, operation, and so on.

Participants should be asked to help ensure that the LOPA is performed on the process as it is actually constructed and operated. Thus, operators must be willing to describe operating practices that are actually followed rather than assuming that written procedures are always followed. Similarly, participants must flag any inaccuracies they observe in process drawings or other information used in the study. There is little point in performing a LOPA study assuming that procedures are followed and documentation is correct if that is not the case. The LOPA study performed may be of high technical quality but it would not correspond to any existing process and the time and effort invested would be wasted.

A practice LOPA session may be conducted, especially with inexperienced teams. Such a session can help teach LOPA to the participants.

Team members may have questions on topics covered during the first session. They must be answered to their satisfaction to ensure that the entire team has an understanding of LOPA and the process and is ready to begin the study.

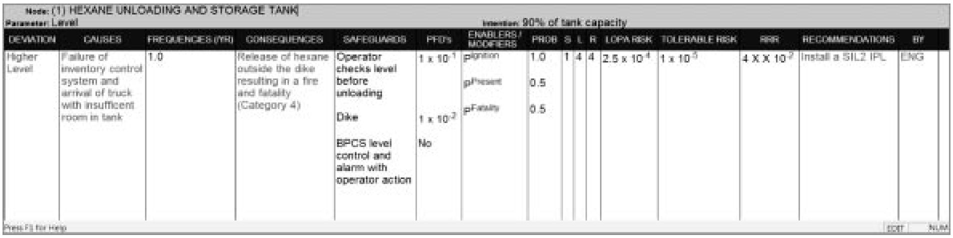
A checklist can help ensure that each LOPA session proceeds smoothly. Items to address include:

- checking that facilities are OK prior to the session start time
- recording session participants
- reminding participants of expected behavior and rules for how the study will be conducted
- addressing any issues identified by QC reviews
- briefly reviewing the study PSO
- briefly reviewing where the study left off at the end of the previous session.

23.9.2 Recording Scenario Information

23.9.2.1 Study Worksheets

LOPA study results can be recorded in a PHA worksheet (Figure 23.5) or in a separate LOPA worksheet (Figure 23.6). The advantages of using a PHA worksheet are that the LOPA information appears together with the PHA scenario and a single



Node: (1) HEXANE UNLOADING AND STORAGE TANK

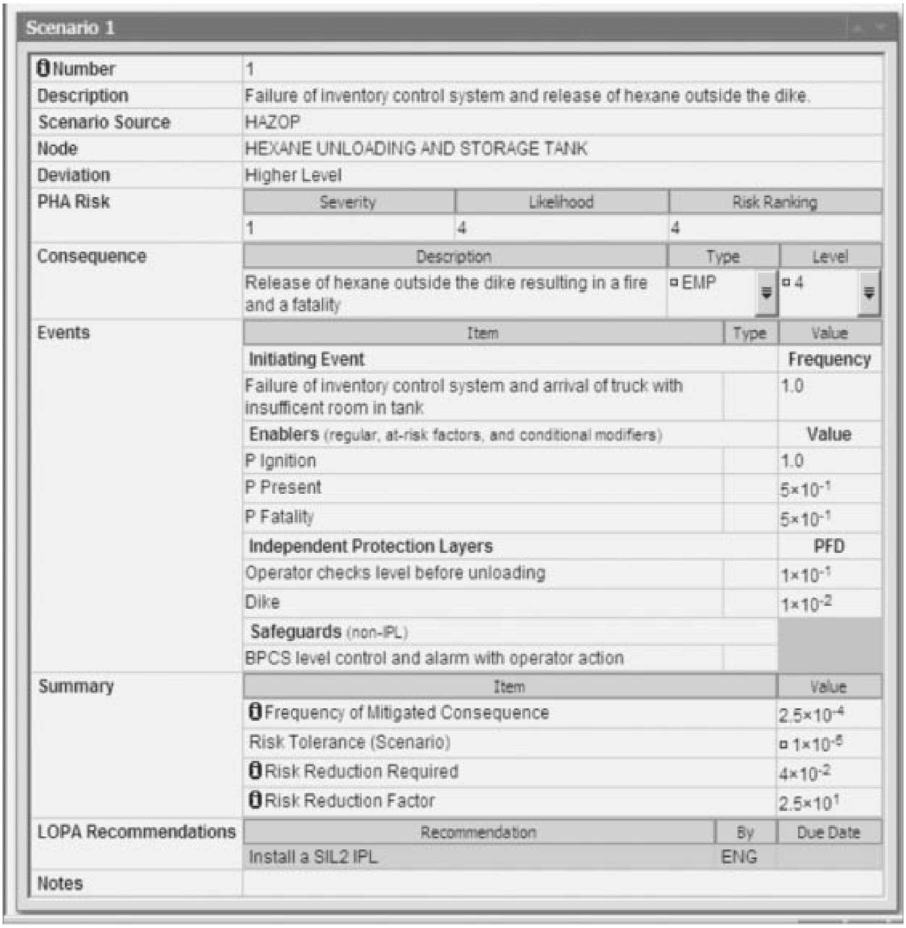
Parameter: Level

Intention: 90% of tank capacity

DEVIATION	CAUSES	FREQUENCIES (/YR)	CONSEQUENCES	SAFEGUARDS	PFD's	ENABLERS / MODIFIERS	PROB	S	L	R	LOPA RISK	TOLERABLE RISK	RRR	RECOMMENDATIONS	BY
Higher Level	Failure of inventory control system and arrival of truck with insufficent room in tank	1.0	Release of hexane outside the dike resulting in a fire and fatality (Category 4)	Operator checks level before unloading Dike BPCS level control and alarm with operator action	1 x 10^{-1} 1 x 10^{-2} No	$p^{Ignition}$ $p^{Present}$ $p^{Fatality}$	1.0 0.5 0.5	1	4	4	2.5 x 10^{-4}	1 x 10^{-5}	4 X X 10^{-2}	Install a SIL2 IPL	ENG

Screen capture from PHAWorks®.

Figure 23.5 Example of LOPA in a PHA worksheet.



Scenario 1

Number	1		
Description	Failure of inventory control system and release of hexane outside the dike.		
Scenario Source	HAZOP		
Node	HEXANE UNLOADING AND STORAGE TANK		
Deviation	Higher Level		
PHA Risk	Severity	Likelihood	Risk Ranking
	1	4	4
Consequence	Description	Type	Level
	Release of hexane outside the dike resulting in a fire and a fatality	□ EMP	□ 4
Events	Item	Type	Value
	Initiating Event		**Frequency**
	Failure of inventory control system and arrival of truck with insuffcent room in tank		1.0
	Enablers (regular, at-risk factors, and conditional modifiers)		**Value**
	P Ignition		1.0
	P Present		5×10^{-1}
	P Fatality		5×10^{-1}
	Independent Protection Layers		**PFD**
	Operator checks level before unloading		1×10^{-1}
	Dike		1×10^{-2}
	Safeguards (non-IPL)		
	BPCS level control and alarm with operator action		
Summary	Item		Value
	Frequency of Mitigated Consequence		2.5×10^{-4}
	Risk Tolerance (Scenario)		□ 1×10^{-5}
	Risk Reduction Required		4×10^{-2}
	Risk Reduction Factor		2.5×10^{1}
LOPA Recommendations	Recommendation	By	Due Date
	Install a SIL2 IPL	ENG	
Notes			

Screen capture from LOPAWorks®.

Figure 23.6 Example of a LOPA worksheet.

worksheet is used. However, the PHA worksheet is made more complex and more worksheet columns must be displayed.

The advantages of using a separate LOPA worksheet are as follows:

- provides a more logical organization of LOPA data
- avoids cluttering the PHA worksheet with information that is not needed for PHA
- simplifies the treatment of references within the PHA worksheet
- makes global safeguards easier to manage
- analyzes only scenarios of interest
- avoids "holes" in the PHA worksheet where LOPA is not performed

- focuses attention on the scenario under analysis
- avoids potential regulatory and legal liabilities created when those PHA scenarios analyzed using LOPA have detailed information but others do not
- LOPA and PHA are two separate types of studies involving different types of thought processes and, therefore, it is not a good idea to integrate the studies fully
- avoids the compromises needed to integrate it into a PHA worksheet
- the analysis is more easily understood
- LOPA studies may need to include scenarios from multiple PHAs
- Mirrors the CCPS format (CCPS, 2001).

On balance, a separate worksheet is preferred. Each scenario is recorded in its own worksheet which provides various fields to define the scenario. A number is usually assigned to each scenario.

LOPA worksheets are used in various ways:

- review by the team leader and team members
- reference by team members during the study
- quality control review
- generation of actions on risk reduction
- review by interested parties on completion of the study, for example, regulators
- revalidation of LOPA studies.

23.9.2.2 **Format and Content of LOPA Worksheets**

Key information displayed in the LOPA worksheet that is transferred from the PHA study for each hazard scenario includes the initiating event, hazardous event, consequence, including description, type, and level, safeguards present, and enablers (if identified). Additional useful information may be incorporated from the PHA, including the PHA risk ranking, node, or system/subsystem information, and PHA recommendations. The risk tolerance criteria that are to be used should also be entered. Further information may be included in the LOPA worksheet, including:

- scenario description
- scenario reference number
- group number
- category
- date of analysis
- revision number
- revision date
- reason for revision
- facility
- process
- process mode
- reason for LOPA
- screening criteria used
- scenario source
- analysts
- drawings
- procedures
- documents
- remarks
- comments
- reviewers
- approvals
- data source(s)
- Notes.

The Notes field is used for various purposes, including:

- references to supporting information
- comments on the results
- assumptions
- justifications.

The format and content of LOPA worksheets may vary. Some worksheets may contain:

- scenario consequences of multiple types, for example, impacts on people, property, and the environment
- analysis of scenarios involving both failure and successful operation of mitigation IPLs
- multiple causes for the same consequence
- summation of frequencies for scenarios with the same consequences
- confirmation check boxes, for example, IPL qualification criteria, human action IPL criteria.

23.9.2.3 Use of LOPA Worksheets

Scenarios are selected from studies that precede LOPA using screening criteria (see Section 23.7.3). Initiating events, safeguards, and consequences are defined by these prior studies. They must be reviewed to ensure they are appropriate. Enablers may not have been recorded in prior studies but can contribute significantly to risk reduction and may need to be identified as part of the LOPA study.

LOPA worksheets can be populated with scenario information before the analysis begins to speed up the study. However, the LOPA facilitator should not complete any of the analysis as it should be performed by the team; otherwise team members will be tempted to endorse what has been done and not think critically about the analysis.

After scenario information has been recorded in a LOPA worksheet, analysts enter the following information:

- initiating event frequency
- enabler probabilities/multipliers
- IPLs and their PFDs.

Various tools can be used to document LOPA studies, including:

- paper worksheets
- computer software.
  - word processor tables/spreadsheets
  - PHA software (e.g., PHAWorks®, *http://www.primatech.com*)
  - custom software (e.g., LOPAWorks®, *http://www.primatech.com*).

Software improves the efficiency and effectiveness of recording studies and helps to avoid the need for team review, comments, and editing of paper worksheets. In addition to LOPA worksheets, a report is also prepared to ensure the LOPA study is properly documented (see Section 23.9.15).

23.9.3 Assigning Initiating Event Frequencies

Frequencies of initiating events are usually taken from a standard database developed by a company (see Section 23.7.6) and entered into the worksheet. Any deviations from standard values should be documented and justified.

23.9.4 Addressing Enablers

Historically, enablers have not been identified often in PHA worksheets. Sometimes, they are now included if LOPA is to be performed. However, most often LOPA teams will need to identify enablers for scenarios if they are to be included in the analysis.

Enablers are factored into LOPA using their probabilities or multipliers to modify the scenario frequency, either by adjusting the initiating event frequency or, alternatively, by adjusting the probability of the affected events in the scenario. In the latter case, the enabler is usually annotated with a description of the adjustment made, for example, PM on relief valves is not performed as often as specified (relief valve PFD adjusted upwards).

Care must be exercised to avoid counting enablers twice. They may have been incorporated into the consequence estimate, for example, the probability of the operator being present may have been used to adjust the consequence. Double counting will underestimate the scenario risk. Similarly, adjustment for at-risk factors may have been made in the initiating event frequency. For example, a pump may be used for 4 h each day and failure rate data are collected for the pump over time. It is not appropriate to adjust this failure rate for time-at-risk as the failure rate is already the appropriate rate for this periodic operation of the pump.

If an enabler will definitely occur, for example, a safety system is permanently bypassed by the operators, its probability is 1. No credit is taken for needing the enabler to occur. It is considered to be part of the scenario description, that is, it is a *given*.

For conditional modifiers, the probability of ignition, P^{ignition}, applies only to fire and explosion scenarios, of course. The probability of personnel being in the affected area, P^{present}, and the probability of harm from exposure, P^{injury}, apply in principle to all scenarios. During some modes of operation, such as startup, operators may always be present and thus $P^{\text{present}} = 1$. During the build-up to a hazardous event, more people may be present investigating the symptoms and, therefore, it is likely that $P^{\text{present}} = 1$ when the release occurs. Human presence may be correlated with the cause of a hazardous event and it is possible that $P^{\text{present}} = 1$ if the person contributes to the initiating event, for example, for a release caused by an operator opening a bleed valve. The initiating events, P^{ignition}, and P^{present} may be linked. For example, a crane operator may drop a load on the process, causing a release. Metal-on-metal sparking or the crane engine provides an ignition

Table 23.10 Factors that influence P^{ignition}, P^{present}, and P^{injury} and ways of controlling them.

Influencing factor	**Means of control**
P^{ignition}	
Initiating event for the scenario	Hazardous area classifications
→If it produces or provides a source of ignition	Ventilation
Physical properties of the flammable material, for example:	Procedures
→Flash point	Equipment design
→Flammable and explosive limits	Containment of releases
→Auto-ignition temperature	
→Physical state (gas, vapor, and liquid)	
→Volatility	
Chemical properties of the released material, for example reactivity	
Layout, for example:	
→Proximity and location of ignition sources	
→Hazardous area classifications	
Environmental factors that impact dispersion, for example, wind direction	
P^{present}	
Mode of operation	Barriers
Initiating event	Access control
Attended/unattended operation	Exclusion areas
	Procedures
P^{injury}	
Type of event, for example, pool fire versus flash fire	Hazardous area entry control
Duration and magnitude of the exposure	Release detection and alarms
Escape route	Escape plans
Ability to escape	Protective equipment
Skill/knowledge/training	Refuges
Physical ability	Training
Availability/use of PPE	

source. Thus $P^{\text{ignition}} = 1$ and $P^{\text{present}} = 1$ as a result of the nature of the initiating event.

Factors that influence P^{ignition}, P^{present}, and P^{injury} and ways of controlling them are provided in Table 23.10.

23.9.5 Assigning Enabler Probabilities/Multipliers

Typically, companies develop standardized values for common enablers. Whenever non-standard values are used, or enablers are encountered that are not in the company database, justification must be provided for the values.

23.9.6 Identifying Existing IPLs

The identification of IPLs can be performed as part of PHA or, subsequently, as part of LOPA. Probably, their identification during LOPA is preferred as the discussion that is required is valuable in helping the LOPA team understand the scenario and perform the analysis.

Usually, all safeguards that protect a scenario are listed in the LOPA worksheet. Qualification criteria are then applied to each safeguard to determine if it is an IPL (see Section 23.7.5). Commonly, guidelines are used to help teams determine if each qualification criterion is met. For example, checklists have been developed to determine if safeguards meet the effectiveness criterion and for conditions under which human actions may be qualified as IPLs (CCPS, 2001).

In judging the independence of IPLs, the potential for common-cause failures (CCFs) must be considered. CCFs are a specific type of dependent failure where simultaneous (or near-simultaneous) multiple failures result from a single shared cause. Causes of failure can be common between the initiating event and one or more IPLs or between different IPLs. Credit should be taken for only one of the IPLs where they are affected by CCF. Where safeguards are dependent, and only one of them can be credited as an IPL, the one with the highest PFD may be selected to be conservative. For example, in the case of a process that is protected by an emergency vent (PFD = 0.01) and a relief valve (PFD = 0.001) that do not operate independently, credit may be taken for the emergency vent. Alternatively, credit could be taken for the safeguard that receives the first demand.

Some LOPA worksheets use check boxes to show that qualification criteria have been met. Careful consideration should be given to the qualification criteria for each candidate IPL. A rush to judgment must be avoided. This process takes more time than is required for deciding what credit to take for each safeguard in PHA.

Common practice is to list IPLs in the LOPA worksheet in the chronological sequence of the incident. Preventive safeguards (if any) will be the first ones to be challenged. Mitigative safeguards will be activated only after the first layer(s) of protection (if any) have been challenged.

It is good practice to show in the LOPA worksheet all safeguards that were not qualified as IPLs, with the justification for their exclusion, so the basis for the analysis will be clear to reviewers. This practice clarifies which candidate IPLs were considered and helps to avoid reviewers believing that IPLs were missed. IPLs may be classified according to what they protect, for example, safety, environment, assets, business interruption, and so on.

There are various types of protection layers:

- process design
- basic process control system
- supervisory
- preventive

- mitigative
- barriers
- limitation
- emergency response
- vendor-installed.

Table 23.11 identifies the meaning and characteristics of these protection layers and describes their strength as IPLs. Some safeguards that are not normally considered as IPLs are shown in Table 23.12.

IPL equipment should be included in the company's mechanical integrity (MI) program and be subject to inspection and proof tests at defined intervals. IPLs that depend on actions by people should be covered by written operating procedures, and personnel should meet competency requirements and be trained and tested on the procedures.

23.9.7 Assigning IPL PFDs

Typically, companies develop a database of standard values for use in their LOPA studies. The values used should be applicable for the specific process. For example, higher values should be considered for IPLs installed in severe conditions, such as relief valves or sensors in fouling, polymeric, or corrosive service. The design of an IPL should be evaluated against the details of the scenario to ensure that an appropriate PFD is used. Also, the PFD of an IPL is usually related to its test frequency. The longer the period between testing, the higher is the PFD. The PFD used must be consistent with the actual test frequency. Particular care is required when an IPL will be challenged at a frequency that is high in relation to its effective test frequency, human action PFDs are outside industry norms, or frequent testing is required to achieve the claimed PFD.

The justification for the IPL PFDs used should be documented. For example, they may be taken from corporate standards or industry norms.

IEC 61511/ISA 84 requires that SIF PFDs be verified by calculation. In some cases, the PFDs of non-SIS IPLs may also be calculated to help justify the numbers used, for example, for BPCS (basic process control system) control loops or safety control loops involving alarms and actions by people.

23.9.8 Documenting IPLs

The design and technical basis for IPLs, plus other pertinent information, should be documented. This can be a regulatory or standards requirement. Documentation is also needed to facilitate audits of IPLs and to provide information for training and operating procedures. Specific documentation should be provided according to the type of IPL.

Table 23.11 Characteristics of protection layers as IPLs.

Protection layer	**Meaning**	**Characteristics**	**IPL candidate**
Process design	Physical design and chemistry of a process are the origins of process risk	Reduce or eliminate risk during design through choices of technology, equipment, operating parameters, and so on, using inherently safer design (ISD) approaches	Can consider as IPLs or view ISDs as eliminating scenarios
Basic process control system	Maintains the process within normal operating limits	Process may be controlled by operator actions or automated systems or a combination thereof Designed to achieve business goals rather than safety goals	Relatively weak IPL. Maximum credit often limited to a PFD of not less than 1 × 10^{-1}
Supervisory	Operator activities	Daily inspections, observations, independent verifications, and actions required by procedures	Routine operator actions may not be credited as IPLs by some companies
	Operator alarms with response	Requires correct functioning of both equipment and people	Operator action in response to alarms may be credited as an IPL if certain conditions are met
	Instrumented systems may call for operator action or take action automatically	Instrumented supervisory functions can be implemented in a dedicated system, the BPCS or a SIS	May be credited as IPLs subject to conditions being met for the qualification of any operator actions involved All IPLs involving human actions are relatively weak owing to typically high human failure probabilities
Preventive	Implements safety instrumented systems (SISs)	Separate and independent from the BPCS	Strong IPLs when properly designed and maintained
Mitigative	Mechanical equipment	Pressure relief device, emergency isolation valve, pressure regulator, and so on Acts in response to a specified process condition and takes a specific mitigative action. Actions are predictable and equipment failure modes are well understood	All are candidate IPLs. PFDs can vary over a wide range. Need to qualify them using specific rules or guidelines
	Instrumented protective systems	High-integrity pressure protective systems, reactor kill systems, life safety systems	Strong IPLs when properly designed and maintained

(*continued overleaf*)

Table 23.11 (*continued*).

Protection layer	Meaning	Characteristics	IPL candidate
Barriers	Physical barriers such as dikes (bunds), blast walls, and dual-walled piping	Passive systems. High probability they will function as intended	Strong IPLs provided they are designed, constructed, inspected, and maintained in accordance with good engineering practices
Limitation	Fire and gas systems. Emergency dump systems. Water/steam curtains. Emergency shutdown (ESD) systems	Respond to loss of containment to lessen the effects, minimize the potential for the incident to propagate, bring the incident under control faster, contain and possibly dispose of the released materials, and isolate the source of hazardous materials	May not be considered IPLs since a hazardous event has occurred, their effectiveness is uncertain, and their availability and effectiveness may be affected by events in the scenario If credit is taken for them, it may be limited to a risk reduction factor of 10 and require justification
Emergency response	Plant and community response. HAZMAT team, plant fire brigade, public fire department, manual deluge systems, shelter in place, facility, and community evacuations	Communication equipment and alarms that trigger the response may be affected by the incident. Must be tested frequently	Not normally considered as IPLs. Responses occur after the initial release and there are too many variables affecting their overall effectiveness to qualify them as IPLs
Vendor-installed safeguards	Vibration switches, limit switches, over-speed protection, and so on	Safeguards and interlock systems provided with equipment	May be considered as IPLs depending on their design, historical performance, and degree of integration with the BPCS and/or SIS

Table 23.12 Safeguards not normally considered to be IPLs.

Safeguard	Comments
Training and certification	May influence the PFD for operator action
Routine procedures	May influence the PFD for operator action
Testing and inspection	Affects the PFD for certain IPLs
Maintenance	Affects the PFD for certain IPLs
Communications	Affects the PFD for certain IPLs
Signs	Signs may be unclear, obscured, ignored, and so on. May affect the PFD for certain IPLs

23.9.9 Estimating Scenario Consequence Severity and Frequency

The consequence severity for each hazard scenario is usually estimated qualitatively. The severity level estimated in the PHA risk ranking process may be used, or that estimate may be refined by using release quantity estimates to assign the severity to a category (see Section 23.7.1). Typically, the scenario frequency is calculated by multiplying the initiating event frequency for the scenario by the probabilities of the other events in the scenario, including IPL failures and enablers.

It should be recognized that when very low scenario frequencies are calculated (say 1×10^{-6} or below) before any additional reduction measures have been considered, it is possible that the analysis is in error. Various causes are possible, including:

- Initiating event frequency may be too low.
- Too much credit may have been taken for enablers.
- Too many IPLs may have been credited. CCF becomes more likely when there are more than three or four IPLs.
- IPL PFDs may be too low.
- CCFs may not have been addressed.
- Something may have been missed.

23.9.10 Evaluating Scenario Risk

The scenario risk is determined by combining the scenario consequence severity and likelihood. As the severity is usually expressed as a qualitative category or level and the likelihood as a number, the risk is represented by the severity–likelihood couplet rather than a single number. Thus, a scenario may have a severity level of 2 with a frequency of occurrence of 1×10^{-4} per year. This represents the LOPA risk of the scenario.

23.9.11 Assessing Compliance with Tolerable Risk Criteria

The estimated scenario risk is compared with risk tolerable criteria. Typically, the risk reduction required (RRR) is calculated by taking the ratio of the tolerance risk (TR), to the estimated risk (ER), that is, RRR $=$ TR/ER. If the risk gap is 10^{-3} or more, some companies will not rely on LOPA. Instead, more sophisticated methods are used such as QRA.

23.9.12 Developing Recommendations for Any Needed Risk Reduction

When a risk gap is found, possible actions to meet the risk tolerance criteria include the installation of additional or strengthened IPLs. LOPA analysts may or may not be requested to identify such recommendations. The effort can add significantly to the study time.

If recommendations are made, they must be resolved by management, who will need to review the recommendations and either implement or reject them with appropriate justification and documentation. A tracking system is needed to manage this process and the implementation of action items.

Whenever a recommendation for risk reduction is made, either by the LOPA team or subsequently by others, it is important that the impact of the recommendation be assessed using LOPA.

23.9.13 Addressing Quality Assurance

Various assumptions and judgments may be made during a LOPA study. It can be useful to perform an independent review of the study before it is considered to be complete. The LOPA team will need to respond to any review comments.

Other quality control actions should be taken during study preparation and the performance of the study. Usually, checklists of key issues are employed by team leaders, team members, third-party reviewers, and management. The ability of the team to achieve high-quality results can be compromised by inattention to quality.

23.9.14 Revalidating Previous Studies

Government regulations and industry standards require that PHAs be revalidated periodically, typically at least every 5 years. Revalidation involves updating the PHA to account for changes that have been made to the process. Usually, LOPA is directly connected to PHA. Therefore, it is good practice also to revalidate LOPA studies.

23.9.15 Preparing a Report

LOPA worksheets alone are not adequate to document a LOPA study. A comprehensive written report should be produced. The report must be clear, accurate, and complete as it will be used by people who were not part of the study team, for example, to follow up on study recommendations. It provides a permanent record of the study and proof that the study was conducted. It is prepared after the study is completed. The report is also needed for auditing, periodic revalidation, MOC reviews, and reference by stakeholders.

Typical report contents include:

- summary of the study results
- list of recommendations made
- process description
- study PSO

- description of the LOPA approach used
- how the study was conducted
- who participated
- assumptions made
- references to failure data used
- LOPA worksheets for scenarios analyzed
- copies of reference materials used during the study.

Some practitioners include these items in the PHA report rather than preparing a separate LOPA report.

The report must be structured to meet the needs of various audiences including management, technical reviewers, and regulators. It should be prepared as soon as possible after the study is completed when information is fresh and the report is easier to produce. Management should be provided with the results in a timely fashion so that they can act promptly. It is good practice to retain the report and records on the disposition of its recommendations for the life of the process.

LOPA reports are sensitive documents. They should be safeguarded from access or theft for malicious intent and damage/destruction while providing access to meet regulatory requirements, and for valid uses such as LOPA revalidations and auditing.

23.9.16 Following Up

Various actions are needed on completion of a LOPA study, including:

- addressing risk reduction needed
- verifying that IPLs do not introduce additional hazards
- verifying IPL adequacy
- modifying the PSM (process safety management) program
- Auditing IPLs.

23.9.16.1 Addressing Risk Reduction Needed

The following actions are needed:

- developing recommendations for risk reduction
- categorizing and prioritizing recommendations
- resolving recommendations
- managing action items, that is, recommendations that will be implemented
- communicating LOPA results to affected parties.

A full set of recommendations must be produced for consideration by management.

Recommendations may need to be developed for situations where the LOPA team did not make a recommendation, or when making recommendations was not included as part of the study. Additional and alternative recommendations to those developed by the LOPA team can be considered. A group of engineers normally performs this task. The LOPA Team Leader may participate to explain the LOPA results. Once a full set of recommendations has been developed, they must be resolved by management, that is, decisions must be taken on which should be implemented. This review is the responsibility of management but it may involve various technical disciplines.

LOPA results should be presented in a form suitable for decision-making. Recommendations should be categorized and prioritized. Categorization helps to make sense of the PHA results and prioritization helps to decide the order of implementation. Recommendations should be categorized based on the PSO of the study, for example, by consequence type. Categorization helps in organizing the recommendations and assists in planning follow-up activities. Various factors may be considered in prioritizing recommendations, including risk reduction, cost, feasibility, and so on. The key criterion is risk reduction.

A management system is needed to facilitate implementation of recommendations and to ensure that:

- recommendations are addressed promptly
- recommendations are resolved in a timely manner
- resolutions are documented
- differences of opinion between management and the LOPA team are addressed
- actions to be taken are documented
- written schedules are developed for the completion of actions
- responsibilities for actions are assigned
- needed resources are provided
- actions are communicated to people whose work assignments are in the process and who may be affected
- commitments are obtained from affected employees
- management oversight and follow-up occur
- actions are completed as soon as possible
- actions are implemented in the way intended by the LOPA team
- completion of actions is verified
- completion of actions is documented.

Periodic audits can help to ensure that recommendations have been resolved and action items have been implemented in a timely manner.

The results of LOPA studies should be communicated to affected employees, including operators, mechanics, contractors, and so on. Access to LOPA reports alone is not sufficient; proactive communication is needed. Communication should be tailored to the audience and information that is relevant to the job should be presented. For example, operators may be informed of new alarms that will be installed.

Proper management and follow-up of study recommendations is needed to comply with industry standards and to ensure that LOPA study findings and recommendations are not overlooked.

23.9.16.2 Verifying That IPLs Do Not Introduce Additional Hazards

Recommended IPLs, individually or in combination, may introduce hazards to the process or modify existing hazards. Such new or modified hazards must be identified and managed using the company's MOC program or by using PHA methods.

23.9.16.3 Verifying IPL Adequacy

IPLs are critical safeguards. As a precaution, reliability modeling can be used to confirm the PFDs claimed for them. For IPLs that are SIFs, the IEC 61511/ISA 84 standard requires verification of their SILs by calculation. Strong PM programs are important in achieving low IPL PFDs.

23.9.16.4 Modifying the PSM Program

IPLs should be added to a facility's safety-critical equipment list so that they will be addressed in the facility's MI program or the facility's safety-critical action list so they will be addressed in the facility's procedures and training.

IPLs will be effective only if associated procedures and training are adequate and followed, for example, PM procedures. In order to respond appropriately to alarms, operators must understand what should be done, why it should be done, and how it should be done. Refresher training is vital and must address facility modifications resulting from LOPA studies.

23.9.16.5 Auditing IPLs

Processes should be audited periodically to confirm that IPLs are still in place with the assigned PFDs. This may require functional testing, inspections, and replacement or PM of IPLs at a specified frequency. The results of tests, inspections, and so on, should be recorded, including any corrective actions taken. Audit results should be made available to LOPA teams so they can determine the validity of IPL PFDs used.

23.10 Limitations, Cautions, and Pitfalls

Some limitations and cautions for LOPA are provided in Table 23.13.

Mis-application of LOPA results in over-conservative or non-conservative risk estimates. Over-conservative estimates result in unnecessary IPLs, additional life-cycle costs, and more spurious trips. Non-conservative risk estimates result in an under-protected process and unacceptable risk.

Some pitfalls in LOPA and their consequences are:

- Scenarios are poorly defined:
  - Risk is underestimated or overestimated.
- Scenarios do not represent actual operations, for example, an operator relies on a SIF to terminate transfer to a tank instead of monitoring the level using the BPCS:
  - Risk is underestimated.

Table 23.13 Limitations and cautions for LOPA.

LOPA risk estimates are only approximations of the risk for a scenario
LOPA is a simplified approach and should not be applied to all scenarios from a PHA
LOPA is overkill for simple risk-informed decisions and is overly simplistic for complex decisions
LOPA may be inappropriate for very high consequence severity scenarios for which risk tolerance is low. They may require QRA approaches
Risk comparisons of scenarios are valid only if they are based on the same risk tolerance criteria and the same LOPA approach is used
LOPA requires more effort to reach a risk-informed decision than purely qualitative methods such as PHA
LOPA is not used for analyzing risks associated with escape and evacuation

- Spurious trip scenarios with safety consequences are not addressed:
  - Risk is underestimated.
- IPL qualification criteria are not applied correctly:
  - Inappropriate credit is taken for safeguards as IPLs.
  - CCFs are not recognized.
  - Risk is underestimated.
- High-demand situations are treated incorrectly:
  - Risk is overestimated.
- Time at risk is not addressed, for example, for modes of process operation:
  - Risk is overestimated.
- LOPA failure data are not validated, documented, and audited:
  - Results are incorrect.
- IPLs are not maintained to meet the PFD values that were assumed in the LOPA study:
  - Risk is underestimated.
- New IPLs may change existing hazard scenarios or introduce new ones:
  - Impact on the entire process must be considered otherwise risk may be increased.

Keys to avoiding pitfalls include:

- good scenario definitions
- solid LOPA training
- good LOPA guidelines
- strong peer review
- good supporting programs.

The formality of LOPA should not cause analysts to abandon common sense. Input data, assumptions, and results must be reasonable.

Acknowledgments

The copyright of all figures and tables in this chapter is held by Primatech Inc. or Professional Training Services Inc. The figures and tables are used with permission.

References

ANSI/ISA (American National Standards Institute/International Society of Automation) (2004a) 84.00.01-2004 Part 1 (IEC 61511-1 Mod). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*, ANSI, Washington, DC.

ANSI/ISA (American National Standards Institute/International Society of Automation (2004b) 84.00.01-2004 Part 2 (IEC 61511-2 Mod). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod)*, ANSI, Washington, DC.

ANSI/ISA (American National Standards Institute/International Society of Automation (2004c) 84.00.01-2004 Part 3 (IEC 61511-3 Mod). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of the Required Safety Integrity Levels – Informative*, ANSI, Washington, DC.

Baybutt, P. (2002) Layen of Protection Analysis for Humon Factors, *Process Saf. Prog.*, **21**(2), 119–129.

Baybutt, P. (2012a) Risk Tolerance Criteria for Layen of Protection Analysis, *Process Saf. Prog.*, **31**(2), 118–121.

Baybutt, P. (2012b) Using Layen of Protection Analysis to Evoluate Fire and Gas Systems, *Process Saf. Prog.*, **31**(3), 255–260.

Baybutt, P. (2012c) Conducting Process Hazard Analysis to Foulitate Leyan of Production Analysis, *Process Saf. Prog.* **31**(3), 282–286.

Baybutt, P. (2012d) Using Risk Tolerance Criteria to Determine Safety Integrity Levels for Safety Instrumented Functions, *Process Saf. Prog.* **25**(6), 1000–1009.

CCPS (Center for Chemical Process Safety) (2000) *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd edn, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2001) *Layer of Protection Analysis: Simplified Process Risk Assessment*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2007) *Guidelines for Safe and Reliable Instrumented Protective Systems*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2009) *Guidelines for Developing Quantitative Safety Risk Criteria*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2010) *Guidelines for Initiating Events and Independent Protection Layers for LOPA*, American Institute of Chemical Engineers, New York.

HSE (Health and Safety Executive) (2001) *Reducing Risks, Protecting People, HSE's Decision-Making Process*, HSE Books, Sudbury.

HSE (Health and Safety Executive) (2011) HSE Principles for Cost Benefit Analysis (CBA) in Support of ALARP Decisions, *http://www.hse.gov.uk/risk/theory/alarpcba.htm*. (last accessed 22 June 2012)

National Archives (1974) Health and Safety at Work etc. Act 1974, *http://www.legislation.gov.uk/ukpga/1974/37/contents* (last accessed 22 June 2012).