F.2 Impact event

Using Figure F.1, each impact event description (consequence) determined from the HAZOP study is entered in column 1.

F.3 Severity level

Severity levels of Minor (M), Serious (S), or Extensive (E) are next selected for the impact event according to Table F.2 and entered into column 2 of Figure F.1.

Table F.1 – HAZOP developed data for LOPA

LOPA required information	HAZOP developed information
Impact event	Consequence
Severity level	Consequence severity
Initiating cause	Cause
Initiating likelihood	Cause frequency
Protection layers	Existing safeguards
Required additional mitigation	Recommended new safeguards

Table F.1 – HAZOP developed data for LOPA

#	1	2	3	4		5		6	7	8	9	10	11
					PROTECTION LAYERS								
	Impact event description F.2 F.13.2	Severity level F.3 F.13.2	Initiating cause F.4 F.13.3	Initiation likelihood per year F.5 F.13.4	General process design F.13.5	BPCS F.13.6	Alarms, etc. F.13.7	Additional mitigation, restricted access,F.7 F.13.8	IPL additional mitigation dikes, pressure relief F.7 F.13.9	Inter-mediate event likelihood per year F.9 F.13.10	SIF integrity level F.10 F.13.11	Mitigated event likelihood per year F.11 F.13.11	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0,1	0,1	0,1	0,1	0,1	PRV 0,01	10^{-7}	10^{-2}	10^{-9}	High pressure causes column rupture
2	Fire from distillation column rupture	S	Steam control loop failure	0,1	0,1		0,1	0,1	PRV 0,01	10^{-6}	10^{-2}	10^{-8}	Same as above
N													

IEC

Key

Severity Level E = Extensive; S = Serious; M = Minor

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

Figure F.1 – Layer of protection analysis (LOPA) report

NOTE If independent protection layers have not been properly selected frequency and probability of failure on demand cannot be multiplied as shown in Figure F.1. See Annex J.

Table F.2 – Impact event severity levels

Severity level	Consequence
Minor (M)	Impact initially limited to local area of event with potential for broader consequence, if corrective action not taken.
Serious (S)	Impact event could cause serious injury or fatality on site or off site.
Extensive (E)	Impact event that is five or more times severe than a serious event.

F.4 Initiating cause

All of the initiating causes of the impact event are listed in column 3 of Figure F.1. Impact events may have many Initiating causes, and it is important to list all of them.

F.5 Initiation likelihood

Likelihood values of the initiating causes occurring, in events per year, are entered into column 4 of Figure F.1. Table F.3 shows typical initiating cause likelihoods. The experience of the team is very important in determining the initiating cause likelihood.

Values in Table F.3 are not to be used for specific assessments (see Note 1).

Table F.3 – Initiation likelihood

Low	A failure or series of failures with a very low probability of occurrence within the expected lifetime of the plant. EXAMPLES – Three or more simultaneous instrument, or human failures – Spontaneous failure of single tanks or process vessels	$f < 10^{-4}$, /year
Medium	A failure or series of failures with a low probability of occurrence within the expected lifetime of the plant. EXAMPLES – Dual instrument or valve failures – Combination of instrument failures and operator errors – Single failures of small process lines or fittings	$10^{-4} < f < 10^{-2}$, /year
High	A failure can reasonably be expected to occur within the expected lifetime of the plant. EXAMPLES – Process leaks – Single instrument or valve failures – Human errors that could result in material releases	$10^{-2} < f < 100$, /year
NOTE 1 This table is illustrative. These values cannot be taken as generic frequencies and cannot be used in specific assessments. NOTE 2 "*f*" = Initiating event frequency (initiating event likelihood).		

F.6 Protection layers

Figure 2 in Clause 1 shows the multiple protection layers (PLs) that are normally provided in the process industry. Each protection layer consists of a grouping of equipment and/or administrative controls that function in concert with the other layers. Protection layers that perform their function with a high degree of reliability may qualify as independent protection layers (IPL) (see Clause F.8).

Process design to reduce the likelihood of an impact event from occurring, when an initiating cause occurs, is listed first in column 5 of Figure F.1. An example of this would be a jacketed pipe or vessel. The jacket would prevent the release of process material if the integrity of the primary pipe or vessel is compromised.

The next item in column 5 of Figure F.1 is the basic process control system (BPCS). If a control loop in the BPCS prevents the impacted event from occurring when the initiating cause occurs, credit based on its PFD_{avg} (average probability of failure on demand) is claimed.

The last item in column 5 of Figure F.1 takes credit for alarms that alert the operator and utilize operator intervention. Typical protection layer PFD_{avg} values are listed in Table F.4.

Values in Table F.4 are not to be used for specific assessments (see Note).

Table F.4 – Typical protection layers (prevention and mitigation) PFD_{avg}

Protection layer	PFD_{avg}
Control loop	$1,0 \times 10^{-1}$
Human performance (trained, no stress)	$1,0 \times 10^{-1}$ to $1,0 \times 10^{-2}$
Human performance (under stress)	0,5 to 1,0
Operator response to alarms	$1,0 \times 10^{-1}$
Vessel pressure rating above maximum challenge from internal and external pressure sources	10^{-4} or better, if vessel integrity is maintained (that is, corrosion is understood, inspections and maintenance is performed on schedule)

NOTE The figures in Table F.4 are illustrative of the range of values that could appear in assessments. These values cannot be taken as generic probabilities and used in specific assessments. Human error probabilities can be appropriately assessed on a case by case basis.

F.7 Additional mitigation

Mitigation layers are normally mechanical, structural, or procedural. Examples would be:

– pressure relief devices;
– dikes (bunds); and
– restricted access.

Mitigation layers may reduce the severity of the impact event but not prevent it from occurring. Examples would be:

– deluge systems for fire or fume release;

– fume alarms; and
– evacuation procedures.

The LOPA team should determine the appropriate PFD_{avg} for all mitigation layers and list them in column 6 of Figure F.1.

F.8 Independent protection layers (IPL)

Protection layers that meet the criteria for IPL are listed in column 7 of Figure F.1.

The criteria to qualify a protection layer (PL) as an IPL are:

– the protection provided reduces the identified risk by a large amount, that is, a minimum of a 10-fold reduction;
– the protective function is provided with a high degree of availability (0,9 or greater);
– it has the following important characteristics:
  a) Specificity: An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (for example, a runaway reaction, release of toxic material, a loss of containment, or a fire). Multiple causes may lead to the same hazardous event; and, therefore, multiple event scenarios may initiate action of one IPL;
  b) Independence: An IPL is independent of the other protection layers associated with the identified danger;
  c) Dependability: It can be counted on to do what it was designed to do. Both random and systematic failures modes are addressed in the design;
  d) Auditability: It is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety system is necessary.

Only those protection layers that meet the tests of availability, specificity, independence, dependability, and auditability are classified as independent protection layers (IPL).

F.9 Intermediate event likelihood

The intermediate event likelihood is calculated by multiplying the initiating likelihood (column 4 of Figure F.1) by the PFD_{avg} of the protection layers and mitigating layers (columns 5, 6 and 7 of Figure F.1). The calculated number is in units of events per year and is entered into column 8 of Figure F.1.

If the intermediate event likelihood is less than process safety target level for events of this severity level, additional PLs are not required. Further risk reduction should, however, be applied if economically appropriate.

If the intermediate event likelihood is greater than your corporate criteria for events of this severity level, additional mitigation is required. Inherently safer methods and solutions should be considered before additional protection layers in the form of SIS are applied. If inherently safe design changes can be made, Figure F.1 is updated and the intermediate event likelihood recalculated to determine if it is below corporate criteria.

If the above attempts to reduce the intermediate likelihood below corporate risk criteria fail, a SIS is required.

F.10 SIF integrity level

If a new SIF is needed, the required integrity level can be calculated by dividing the corporate criteria for this severity level of event by the intermediate event likelihood. A PFD_{avg} for the SIF below this number is selected as a maximum for the SIS and entered into column 9.

F.11 Mitigated event likelihood

The mitigated event likelihood is now calculated by multiplying columns 8 and 9 and entering the result in column 10. This is continued until the team has calculated a mitigated event likelihood for each impact event that can be identified.

F.12 Total risk

The last step is to add up all the mitigated event likelihood for serious and extensive impact events that present the same hazard. For example, the mitigated event likelihood for all serious and extensive events that cause fire would be added and used in formulas like the following:

– risk of fatality due to fire = (mitigated event likelihood of all flammable material release) × (probability of ignition) × (probability of a person in the area) × (probability of fatal injury in the fire).

Serious and extensive impact events that would cause a toxic release would be added and used in formulas like the following:

– risk of fatality due to toxic release = (mitigated event likelihood of all toxic releases) × (probability of a person in the area) × (probability of fatal injury in the release).

The expertise of the risk analyst specialist and the knowledge of the team are important in adjusting the factors in the formulas to conditions and work practices of the plant and affected community.

The total risk to the corporation from this process can now be determined by totalling the results obtained from applying the formulas.

If this meets or is less than the corporate criteria for the population affected, the LOPA is complete. However, since the affected population may be subject to risks from other existing units or new projects, it is wise to provide additional mitigation and risk reduction if it can be accomplished economically.

F.13 Example

F.13.1 General

The following is an example of the LOPA methodology that addresses one impact event identified in the HAZOP study.

F.13.2 Impact event and severity level

The HAZOP study identified high pressure in a batch polymerization reactor as a deviation. The stainless steel reactor is connected in series to a packed steel fibre reinforced plastic column and a stainless steel condenser. Rupture of the fibre reinforced plastic column would release flammable vapour that would present the possibility for fire if an ignition source is present. Using Table F.2,

severity level serious is selected by the LOPA team since the impact event could cause a serious injury or fatality on site. The impact event and its severity are entered into columns 1 and 2 of Figure F.1, respectively.

F.13.3 Initiating cause

The HAZOP study listed two initiating causes for high pressure: loss of cooling water to the condenser and failure of the reactor steam control loop. The two initiating causes are entered into column 3 of Figure F.1.

F.13.4 Initiating likelihood

Plant operations have experienced loss in cooling water once in 15 years in this area. The team selects once every 10 years as a conservative estimate of cooling water loss. 0,1 events per year is entered into column 4 of Figure F.1. It is wise to carry this initiating cause all the way through to conclusion before addressing the other initiating cause (failure of the reactor steam control loop).

F.13.5 General process design

The process area was designed with an explosion proof electrical classification and the area has a process safety management plan in effect. One element of the plan is a management of change procedure for replacement of electrical equipment in the area. The LOPA team estimates that the risk of an ignition source being present is reduced by a factor of 10 due to the management of change procedures. Therefore a value of 0,1 so it is entered into column 5 of Figure F.1 under process design.

F.13.6 BPCS

High pressure in the reactor is accompanied by high temperature in the reactor. The BPCS has a control loop that adjusts steam input to the reactor jacket based on temperature in the reactor. The BPCS would shut off steam to the reactor jacket if the reactor temperature is above set-point. Since shutting off steam is sufficient to prevent high pressure, the BPCS is a protection layer. The BPCS is a very reliable DCS and the production personnel have never experienced a failure that would disable the temperature control loop. The LOPA team decides that a PFD_{avg} of 0,1 is appropriate and enters 0,1 in column 5 of Figure F.1 under BPCS (0,1 is the minimum allowable for the BPCS).

F.13.7 Alarms

There is a transmitter on cooling water flow to the condenser, and it is wired to a different BPCS input and controller than the temperature control loop. Low cooling water flow to the condenser is alarmed and utilizes operator intervention to shut off the steam. The alarm can be counted as a protection layer since it is located in a different BPCS controller than the temperature control loop. The LOPA team agrees that 0,1 PFD_{avg} is appropriate since an operator is always present in the control room and enters 0,1 in column 5 of Figure F.1 under alarms.

F.13.8 Additional mitigation

Access to the operating area is restricted during process operation. Maintenance is only performed during periods of equipment shutdown and lockout. The process safety management plan requires all non-operating personnel to sign into the area and notify the process operator. Because of the enforced restricted access procedures, the LOPA teams estimate that the risk of personnel in the area is reduced by a factor of 10. Therefore 0,1 is entered into column 6 of Figure F.1 under additional mitigation and risk reduction.

F.13.9 Independent protection layer(s) (IPL)

The reactor is equipped with a relief valve that has been properly sized to handle the volume of gas that would be generated during over temperature and pressure caused by cooling water loss. After consideration of the material inventory and composition, the contribution of the relief valve in terms of risk reduction was assessed. Since the relief valve is set below the design pressure of the fibre glass column and there is no possible human failure that could isolate the column from the relief valve during periods of operation, the relief valve is considered a protection layer. The relief valve is removed and tested once a year and never in 15 years of operation has any plugging been observed in the relief valve or connecting piping. Since the relief valve meets the criteria for a IPL, it is listed in column 7 of Figure F.1 and assigned a PFD_{avg} of 0,01 based on previously discussed operating experience and published industry data.

F.13.10 Intermediate event likelihood

The columns in row 1 of Figure F.1 are now multiplied together and the product is entered in column 8 of Figure F.1 under intermediate event likelihood. The product obtained for this example is 10^{-7}.

F.13.11 SIS

The mitigation and risk reduction obtained by the protection layers are sufficient to meet corporate criteria, but additional mitigation can be obtained for a minimum cost since a pressure transmitter exists on the vessel and is alarmed in the BPCS. The LOPA team decides to add a SIF that consists of a current switch and a relay to de-energize a solenoid valve connected to a block valve in the reactor jacket steam supply line. The SIF is designed to the lower range of SIL 1, with a PFD_{avg} of 0,01. 0,01 is entered into column 9 of figure F.1 under SIF Integrity Level.

The mitigated event likelihood is now calculated by multiplying column 8 by column 9 and putting the result (1×10^{-9}) in column 10 of Figure F.1.

F.13.12 Next SIF

The LOPA team now considers the second initiating cause (failure of reactor steam control loop). Table F.3 is used to determine the likelihood of control valve failure and 0,1 is entered into column 4 of Figure F.1 under initiation likelihood.

The protection layers obtained from process design, alarms, additional mitigation and the SIS still exist if a failure of the steam control loop occurs. The only protection layer lost is the BPCS. The LOPA team calculates the intermediate likelihood (1×10^{-6}) and the mitigated event likelihood (1×10^{-8}). The values are entered into columns 8 and 10 of Figure F.1 respectively.

The LOPA team would continue this analysis until all the deviations identified in the HAZOP study have been addressed.

The last step would be to add the mitigated event likelihood for the serious and extensive events that present the same hazard.

In this example, if only the one impact event was identified for the total process, the number would be $1,1 \times 10^{-8}$. Since the probability of ignition was accounted for under process design (0,1) and the probability of a person in the area under additional mitigation (0,1) the equation for risk of fatality due to fire reduces to:

Risk of fatality due to fire = (Mitigated event likelihood of all flammable material releases) × (Probability of fatal injury due to fire) = 0,5.

or

Risk of fatality due to fire = $(1,1 \times 10^{-8}) \times (0,5) = 5,5 \times 10^{-9}$

This number is below the corporate criteria for this hazard and further risk reduction is not considered economically justified, so the work of the LOPA team is complete.

Annex G
(informative)

Layer of protection analysis using a risk matrix

G.1 Overview

Annex G describes a hazard and risk assessment method that uses layer of protection analysis (LOPA) to identify the safety functions that reduce the frequency of loss of primary containment (LOPC) events to a tolerable level. The method encourages the implementation of proactive safeguards that prevent the LOPC, but allows the consideration of consequence mitigation systems as necessary. When consequence mitigation systems are implemented, the method requires the explicit examination of the outcome resulting from the mitigation system deployment. Since the method does not determine the frequency of harm posed by the LOPC, this method does not consider post-release conditions, such as the probability of ignition or occupancy. This simplifies the method and focuses the assessment team on reducing LOPC events through inherently safer design and proactive layers of protection.

This method uses a risk matrix to communicate the risk criteria to the assessment team. The risk matrix has been calibrated to account for the consequence severity potentially posed by the LOPC event. The criteria include consideration for safety, environmental, and economic loss potential.

The method examines hazardous events identified using any hazard identification technique appropriate for the process lifecycle step. At a minimum, the hazard identification should describe the hazardous events that were assessed and should identify the initiating cause(s) and the safeguard(s) that prevent or mitigate the event(s).

The risk assessment is performed using LOPA where the process risk is determined and compared to a tolerable risk as defined by a semi-quantitative risk matrix. When the process risk is above tolerable, safety functions are identified and allocated to independent protection layers (IPLs) as shown in Figure G.1 (adapted from CCPS, 2007). Some IPLs are proactive and act to prevent the hazardous event from occurring. Others are reactive and act to reduce the harm caused by the hazardous event.

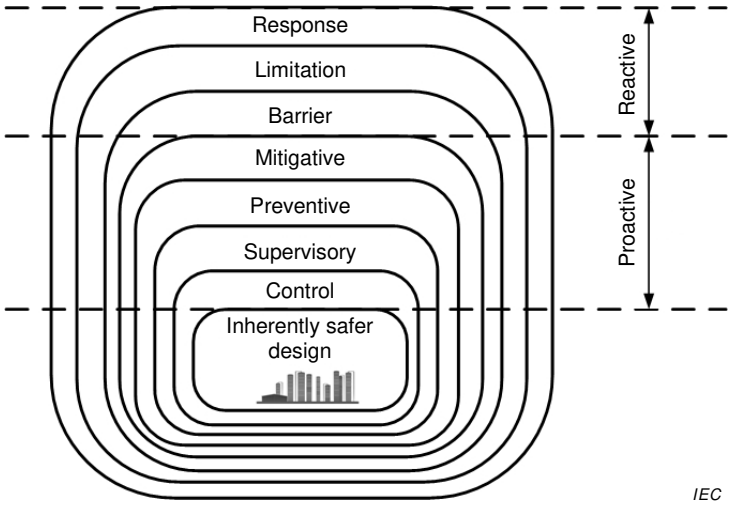

Figure G.1 – Layer of protection graphic highlighting proactive and reactive IPL

This method encourages the selection of proactive IPL, which reduce the frequency of the hazardous event (e.g., loss of containment or equipment damage). The use of any protection layer requires the additional consideration of the secondary consequence that results from their successful operation. This is particularly true of mitigative layer IPLs – see step 7 below.

When the study is completed, the identified safety functions have been allocated risk reduction in accordance with guidelines that are established for each type of IPL and associated function. When risk reduction is allocated to a SIS, this risk reduction yields a SIL in accordance with IEC 61511-1:2016 Table 4.

This method does not consider the duration of the operating mode when analysing sequenced, batch, start-up or maintenance risk. In this method, the risk of each operating mode should be reduced to the tolerable frequency regardless of the amount of time the process is in a particular operating mode.

The tolerable frequency for a hazardous event is determined by assessing the worse credible scenario consequence in terms of the health and safety impact to plant personnel and the public, environmental impact, and economic impact (property and business losses). The team is expected to qualitatively estimate the worst credible consequence regardless of likelihood and identify IPLs to reduce the event risk. Again, since this method seeks to reduce the hazardous event frequency (e.g., loss of primary containment or equipment damage), this method does not consider the use of conditional modifiers for occupancy, ignition or fatality, which are typically used to assess the frequency of specific types of harm caused by the event.

NOTE 1 This method leverages the availability of the team and information to assess economic impact of loss of containment events. The implementation of any recommendations for economic-related events is determined by business approval processes.

NOTE 2 The frequency, probability and risk reduction values used are for illustration only and are not to be used as generic values for specific assessments.

Annex G is not intended to be a definitive account of the method but is intended to illustrate the general principles. It is based on a method described in more detail in the following references:

Layer of Protection Analysis-Simplified – Process risk assessment, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7.