Layer of Protection Analysis (LOPA) Worksheet

One sheet records one scenario, one cause-consequence pair. LOPA, as the CCPS glossary describes it, takes one such scenario at a time, estimates its risk from an initiating event frequency, the failure probabilities of the protection layers claimed and the consequence, and compares the estimate with risk criteria to see where more risk reduction or a more detailed study is needed. It is semi-quantitative, order-of-magnitude work, not a full quantified risk assessment. The scenario comes from a hazard study such as a HAZOP; this sheet does not replace it. No source opened for this form requires a LOPA: 29 CFR 1910.119(e), the US process hazard analysis paragraph, does not name it. **This form prints no typical value.** Every frequency, every probability of failure on demand (PFD), every modifier and the tolerable frequency is written by you, with its source and date. Numbers in the last column of section 5 are invented to show the arithmetic. The CCPS LOPA book and IEC 61511 are paid texts and are not reproduced.

1 Scenario

Scenario reference and linked PHA record (study, node, recommendation no.)	Facility or unit, revision and date	Prepared by (name, role)

Hazard scenario description and consequence: the cause, what goes wrong, the loss event and its consequence (one cause-consequence pair)

Severity category (your own scale, from your criteria document)	People, environment or asset affected, and the criteria document and revision

2 Initiating event, frequency, source and date

Initiating event: the first event that starts the sequence (what fails, errs or happens)

Initiating event frequency, per year (you enter it)	Source of the frequency (data set, plant history, calculation) and its date	Checked by

3 Enabling conditions and conditional modifiers (probabilities you enter)

Enabling conditions: a condition or operating phase that is not a failure, error or protection layer but must be present for the sequence to reach a loss event (for example, the unit is in a certain mode for part of the year).

No.	What must be true (describe the condition)	Probability, 0 to 1 (you enter it)	Source or basis, and date	Why it applies here and is not counted twice

Conditional modifiers: other probabilities applied when the consequence is expressed as an impact rather than a loss event, such as the CCPS glossary's examples of a hazardous atmosphere forming, ignition, explosion, personnel present, injury or fatality and equipment damage. Write only those that apply to this consequence, with the value you can support.

No.	What must be true (describe the condition)	Probability, 0 to 1 (you enter it)	Source or basis, and date	Why it applies here and is not counted twice

Terms as used on this sheet (CCPS glossary, paraphrased)

Term	Meaning
Safeguard	Any device, system or action that interrupts the chain of events after the initiating event or reduces the consequence. A safeguard is not automatically an independent protection layer.
Independent protection layer	A device, system or action able to stop the scenario reaching its consequence without being adversely affected by the initiating event or by any other layer on this scenario.
Probability of failure on demand	The probability that a system fails to perform its function when it is called on. Written by you for each layer, with source and date.
Enabling condition	A condition or operating phase that is not a failure, error or protection layer but must be present for the sequence to continue; a probability.
Conditional modifier	A further probability, such as ignition or someone being present, used when the consequence is stated as an impact.
Tolerable risk level	The highest level of risk regarded as tolerable in the circumstances. Here it is your criterion, written in section 6.

General template, not legal or certification advice. Adapt it to your own procedures and to the requirements that apply to you.
Free template by QHSEtech · CC BY 4.0: reuse and adapt it with credit and, where practicable, a link to qhsetech.com/templates/lopa-worksheet-template

4 Independent protection layers claimed

A protection layer is a device, system or action that stops the scenario from reaching the consequence. It counts as **independent** only if the initiating event and the action of every other layer on this scenario cannot adversely affect it (CCPS glossary). Not every safeguard in the PHA is an independent protection layer. A control loop that is the cause of the initiating event, a trip that shares the sensor, logic or final element of the alarm credited next to it, shared power or utilities, or the same operator, is not independent (HSE control-systems guidance, Great Britain). The CCPS glossary names seven attributes of an independent protection layer: independent, functional, integrity, reliable, validated-maintained-and-audited, access security and management of change; their criteria are in the CCPS book, text not reproduced. Write your reason in each box: an empty box means no credit.

No.	Protection layer claimed: device, system or action, and what it does for this scenario	PFD (you enter it)	Source of the PFD, and date	Independent: why (of the initiating event and of each other layer: sensor, logic, valve, power, people)	Effective and auditable: acts in time; how tested, maintained and evidenced; who can defeat it	Credit taken

4b Layers considered and not credited, and why

Safeguard or layer	Reason it is not credited (not independent, not effective in time, not tested, not auditable, other)	What would make it creditable

5 Calculation steps (you write each value and the result)

Worked example, invented: a vessel overpressures after loss of cooling. Two layers are credited (a high-pressure alarm with operator action, then a relief valve) and a third, an independent trip, is added to close the gap. Units are per year for frequencies and a number from 0 to 1 for probabilities. Write each factor in the product, not only the answer. The product of PFDs is valid only for layers that are independent of each other and of the initiating event.

Step	Quantity	Formula the form prints	Your value	Worked example (invented)
1	**Initiating event frequency, f_IE**	from section 2		*0.2 per year*
2	**Enabling conditions, P_en**	product of the enabling-condition probabilities in section 3 (use 1 if none)		*0.5*
3	**Credited layers, PFD_all**	product of the PFDs in section 4: PFD_1 x PFD_2 x ...		*0.2 x 0.05 = 0.01*
4	**Conditional modifiers, P_cm**	product of the conditional-modifier probabilities in section 3 (use 1 if none)		*0.3 x 0.25 = 0.075*
5	**Mitigated frequency, f_mit**	f_mit = f_IE x P_en x PFD_all x P_cm		*0.2 x 0.5 x 0.01 x 0.075 = 7.5E-5 per year*
6	**Tolerable frequency, f_tol**	from section 6, written by you		*1E-5 per year (invented)*
7	**Gap ratio, R**	R = f_mit / f_tol (above 1 means more reduction is needed)		*7.5E-5 / 1E-5 = 7.5*
8	**Required PFD of added layer(s), PFD_req**	PFD_req = f_tol / f_mit (use only when R is above 1)		*1E-5 / 7.5E-5 = 0.133, so 0.13 or lower*
9	**Check after the action**	f_new = f_mit x PFD_new, then compare with f_tol		*7.5E-5 x 0.1 = 7.5E-6, below 1E-5*

General template, not legal or certification advice. Adapt it to your own procedures and to the requirements that apply to you.
Free template by QHSEtech · CC BY 4.0: reuse and adapt it with credit and, where practicable, a link to qhsetech.com/templates/lopa-worksheet-template

6 Tolerable frequency, criterion and source (written by you)

The form supplies no tolerable frequency. Copy it from your own risk criteria and say where it came from. Whether a figure applies to a single scenario or to the total across all scenarios for the same people or asset is stated in your criteria document, not here.

Tolerable frequency, per year, for this consequence	Consequence endpoint it applies to (as your criteria define it)	Single scenario or total? (as your criteria say)

Criteria document, clause, revision and date	Approved by (name, role) and date

7 Gap and action

Result of step 7 (gap ratio R, in section 5)	Required reduction (PFD_req, step 8)	Further reduction considered where your law or procedure asks for it (for example ALARP)?
☐ R is 1 or below, no gap on this estimate ☐ R is above 1, gap		☐ Yes ☐ No ☐ Not applicable

Options considered, in order: remove or reduce the hazard, passive and active layers, procedures; the option chosen and why

Is a safety instrumented function proposed?	PFD or integrity target for it, and how it is set under your functional safety procedure (IEC 61511 text not reproduced)
☐ Yes ☐ No	

8 Recommendations, owner and due date

No.	Recommendation (and the section 4 or 5 line it closes)	Owner	Due	Status	Resolution recorded (date)

Findings are addressed promptly, the resolution is documented, a written schedule is kept and affected people are told (29 CFR 1910.119(e)(5), US). If a layer credited here is later bypassed, record it on a bypass record and manage the change.

9 Review trigger and sign-off

Review this scenario when

☐ a change is made (management of change) ☐ a credited layer fails a test or is bypassed ☐ an incident or near miss involves it
☐ the PHA is revalidated ☐ other

Next review date	Where this record and its sources are kept

Role	Name	Signature	Date
Operations Lead			
Process Engineer			
HSE Representative			
Maintenance Lead			
Site Manager (final approval)			

General template, not legal or certification advice. Adapt it to your own procedures and to the requirements that apply to you.
Free template by QHSEtech · CC BY 4.0: reuse and adapt it with credit and, where practicable, a link to qhsetech.com/templates/lopa-worksheet-template