SKF 4163 : Safety in Process Plant Design

Risk Assessment: Layer of Protection Analysis (LOPA)

Mohammad Fadil Bin Abdul Wahab

Faculty of Petroleum and Renewable Energy Engineering

Norzita Ngadi

Faculty of Chemical Engineering

Layer of Protection Analysis (LOPA)

A simpler version of QRA and provide conservative results.

Based on the effectiveness of protection layers to lower the the frequency of
undesired consequences.

The objective is to provide sufficient layers to the process to reduce the risk
to an acceptable level.

Example of Protection Layers

Protection Layers	Type of Device
Inherent safety in process design	Passive
Basic process control system (BPCS)	Active
Critical Alarms and Human intervention	Active/Human action
Safety intrumented functions (SIFs), e.g. Interlock	Active
Physical protection such as relief devices	Active
Post-release physical protection such as dikes	Passive
Plant Emergency Response	Human action
Community Emergency Response	Human action

BPCS

The Basic Process Control System (BPCS) is responsible for normal operation of the plant.

Normally use in the first layer of protection against unsafe conditions.

If the BPCS fails to maintain control, alarms will notify operations that human intervention is needed to reestablish control within the specified limits.

If the operator is unsuccessful then other layers of protection, e.g. pressure safety valves and Safety Instrumented System need to be in place to bring the process to a safe state and mitigate any hazards.

Safety Intrumented Functions

Also known as Safety Intrumented Systems

An additional safety layer designed to achieve specific Safety Integrity Levels (SILs) according to standard in IEC 61508 and IEC 61511

Major Steps in LOPA

1. Identifying a single consequence
2. Identifying an accident scenario/cause associated with the consequence
3. Identifying the initiating event and estimating its frequency
4. Identifying the protection layers for the consequence and estimate the probability failure on demand (PFD) for each layers

cont . **Major Steps in LOPA**

5. Estimate a mitigated consequence frequency (f_i^C) through combination of initiating event frequency (f_i^I) with probabilities of failure on demand of the independent protection layers (PFD_{ij})

$$f_i^C = f_i^I x \prod_{j=1}^{i} PFD_{ij}$$

where i refers event, j refers to layer

6. Estimate the risk by plotting the consequence versus the mitigated consequence frequency (f_i^C)
7. Evaluating the risk for acceptability*

*If unacceptable, additional layers of protection are required

Common Example of Consequence

Loss of containment of hazardous material

Leak from vessel
Ruptured pipeline
Gasket failure
Release from relief valve

The consequences are estimated through

1. Semi-quantitative approach with no reference to human harm
   The quantity of release is determined from source model
   The consequence is characterized with a category

2. Qualitative estimates with human harm
3. Quantitative estimates with human harm

Failure Frequency

Failure frequencies for common initiating events (f_i^I) are shown in Table 11-3

Adjustment of failure frequencies,

For non-continuous usage, e.g. a reactor is used only one month during entire year, the reactor failure frequency is divided by 12.

For equipment with preventive maintenance program, e.g. a control system is given preventive maintenance 4 times each year, so its failure frequency is divided by 4

Probabilities of failure on demand (PFD) for Independent Protection Layers (IPLs) are shown in Table 11-4 and Table 11-5.

The IPL functions independently of the components of other IPLs that are used for the same scenario.

The IPL is auditable, its PFD can be validated to include review, testing and documentation

LOTO

"Lockout/Tagout" refers to specific practices and procedures to safeguard employees from the unexpected energization or startup of machinery and equipment, or the release of hazardous energy during service or maintenance activities.

This requires that a designated individual turns off and disconnects the machinery or equipment from its energy source(s) before performing service or maintenance.

The authorized employee(s) either lock or tag the energy-isolating device(s) to prevent the release of hazardous energy and take steps to verify that the energy has been isolated effectively.

Reference

- Crowl, Daniels A. and Louvar, Joseph F., Chemical Process Safety: Fundamentals with Applications, Prentice Hall, 1990, New Jersey, USA.